LOCAL RINGS

MASAYOSHI NAGATA

Kyoto University, Kyoto, Japan

INTERSCIENCE PUBLISHERS
a division of John Wiley & Sons, New York • London

INTERSCIENCE TRACTS
IN PURE AND APPLIED MATHEMATICS

Editors: L. BERS • R. COURANT • J. J. STOKER

Number 13

LOCAL RINGS

By Masayoshi Nagata

INTERSCIENCE PUBLISHERS
a division of John Wiley & Sons, New York • London

INTERSCIENCE TRACTS
IN PURE AND APPLIED MATHEMATICS

Editors: L. BERS • R. COURANT • J. J. STOKER

1. D. Montgomery and L. Zippin—**Topological Transformation Groups**
2. Fritz John—**Plane Waves and Spherical Means Applied to Partial Differential Equations**
3. E. Artin—**Geometric Algebra**
4. R. D. Richtmyer—**Difference Methods for Initial-Value Problems**
5. Serge Lang—**Introduction to Algebraic Geometry**
6. Herbert Busemann—**Convex Surfaces**
7. Serge Lang—**Abelian Varieties**
8. S. M. Ulam—**A Collection of Mathematical Problems**
9. I. M. Gel'fand—**Lectures on Linear Algebra**
10. Nathan Jacobson—**Lie Algebras**
11. Serge Lang—**Diophantine Geometry**
12. Walter Rudin—**Fourier Analysis on Groups**
13. Masayoshi Nagata—**Local Rings**

Additional volumes in preparation

BRARY OF CONGRESS CATALOG CARD NUMBER 62-17459

PRINTED IN THE UNITED STATES OF AMERICA

PREFACE

The theory of local rings is important in both algebraic geometry and the theory of commutative rings, and has been intensively developed in the past decade by many authors. But, to the best of the writer's knowledge, only two books, by Samuel [2] and Akizuki and Nagata [1] have been published on the subject. The former is rather out of date and the latter was written in Japanese.

The writer aimed, therefore, on one hand to give in the present book a systematic exposition of an up-to-date theory of local rings. The writer aimed on the other hand to develop further the theory of local rings. Among the new methods and new results given in the present book, the following four should be noted:

(1) A principle, which is called the principle of idealization, and by which modules become ideals, is applied manywhere in this book.

(2) The primary decomposition of a homogeneous ideal has been treated by a different method from that of inhomogeneous ideals. But, proving a lemma (our (8,3)), we give a unified treatment which is an adaption of the one for the inhomogeneous case. The primary decomposition of a Noetherian graded submodule follows from that of ideals by virtue of the principle of idealization.

(3) We give in Chapter II a new theory of the exact tensor product.

(4) We give in Chapter IV a new theory of syzygies, which takes the place of homological methods employed in the theory of local rings. Thus we shall never use homological algebra in the present book. Furthermore, it should be emphasized here that our theory is simpler than the one given by homological algebra even for readers who know the subject.

The writer wishes to express his thanks to his colleague Dr. Hideyuki Matsumura for a critical reading of the manuscript.

Kyoto, July, 1960 MASAYOSHI NAGATA

PREREQUISITES

Only the following are assumed to be known:

(1) Elements of set theory including Zorn's lemma which asserts that an inductive set has a maximal member.

(2) A knowledge of algebra which is common to Van der Waerden [1] and Zariski-Samuel [1] (Van der Waerden [1], Chapters 3–8; Zariski-Samuel [1], Chapters I–III), and the definitions of Galois extensions and Galois groups including infinite field extensions.

(3) Elementary properties of tensor products (see, for instance, Bourbaki [1], §1, §2.)

(4) Elementary knowledge of the notions of open sets, neighborhoods, closed sets, T_0-spaces, and metric spaces.

Our use of inclusion symbol:
$A \subseteq B$ (or $B \supseteq A$) means that A is a subset of B.
$A \subset B$ (or $B \supset A$) means that A is properly contained in B, namely, that $A \subseteq B$ and $A \neq B$.

CONTENTS

Chapter V
Theory of Complete Local Rings and Its Application

Chapter VI
Geometric Local Rings

Chapter VII
Henselian Rings and Weierstrass Rings

Appendix

INTRODUCTION

The history of the theory of local rings begins with Krull's paper [9]. Here he defined a "Stellenring" as a Noetherian ring with only one maximal ideal (a Noetherian ring is a commutative ring with units which satisfies the maximum condition for ideals). The name Stellenring was chosen because such rings are often associated with points on algebraic and analytic varieties. Chevalley [1] renamed them "local rings" since a ring associated with a point on a variety gives local properties of the variety.

To illustrate this geometric aspect of local rings let us consider an affine n-dimensional space A_n over the complex field C. Let $x_1, \cdots, x_n$ be a set of coordinates for A_n and P a point in A_n. If R_P is the set of rational functions in $x_1, \cdots, x_n$ which are regular at P, then R_P is a Noetherian ring in which $\mathfrak{m}_P = \{f \mid f \in R_P, f(P) = 0\}$ is the only maximal ideal. Thus R_P is a local ring associated with a point P of A_n. An irreducible variety V going through P defines a prime ideal of R_P, $\mathfrak{P} = \{f \mid f \in R_P, f(V) = 0\}$ and *vice versa* a prime ideal of R_P defines a variety through P. Further the ring $R_P/\mathfrak{P}$ is again a local ring which we call the local ring of P on V. Thus a ring-theoretic and sheaf-theoretic study of the set of local rings of points on V might be expected to yield properties of V. This can be adapted to algebraic varieties over other defining fields, abstract varieties, and also to analytic varieties if R_P is replaced by the set of analytic (holomorphic) functions of P.

Many geometric theorems can be derived from local ring theorems, others may be rephrased in purely ring-theoretic terms, e.g., (1) the irreducibility of the product of two irreducible varieties [algebraic case our (39,9), analytic case our (47,5)], (2) the normality of the product of two normal varieties [algebraic case our (42,10), analytic case our (47,10)], (3) the fact that the set of points of a variety whose multiplicities are greater than a given number forms a subvariety which may be reducible [our (40,3)], and (4) the so-called Jacobian criterion for simple points [our (46,3)].

As we have sketched above, the theory of local rings is important for its geometric applications. These local rings which occur in geometry are the principle study of this book. Most of nice properties of these local rings are derived from the fact that they are pseudo-geometric rings which are homomorphic images of Macaulay rings. The single exception to this aim is §33 where we depart from these

rings to investigate an application of the theory of local rings to the general theory of Noetherian rings.

The first three chapters of this book are devoted to basic results for general commutative rings (Chapter I) and to the development of two important tools which are used throughout. These are the completion of rings with respect to a simple topology (Chapter II) and the notion of multiplicity (Chapter III). The fact that the completed rings have a nice relationship to the original ring is itself a major reason for the usefulness of the theory of local rings. The notion of multiplicity plays a large role in ideal theory and in algebraic geometry. In Chapter II we have also studied semi-local rings, not because they are a generalization of local rings but from theoretical necessity. For instance, a ring which is a finite integral extension of a local integral domain or more generally a ring which is a finite module over a local ring is not in general a local ring but rather a semi-local ring. Geometrically, this is accounted for by the fact that if V' is a finite covering variety of a variety V then to each point P of V there corresponds a finite number of points of V', but in general more than one.

As noted in the preface, Chapter IV gives a theory of syzygies which is Hilbert's notable contribution to the theory of invariants. Except a few elementary results from Chapter I, this chapter can be read without reference to the preceding ones.

Chapter V is devoted to the theory and application of complete local rings. This is of particular importance for applications and leads to our theory of pseudo-geometric rings.

Next in Chapter VI we take up the subject of pseudo-geometric rings which, as we have noted, is our main object of study.

Chapter VII is devoted to the general theory of convergent power series rings.

A few words on our general approach are in order. If our only concern had been the construction of a theory of local rings which appear in algebraic geometry, then other methods might have been used. For instance, some of the necessary ring-theoretic results in Chapter IV can be derived without the use of syzygies and the existence of subfields sometimes makes for easier treatment. But these known methods cannot be applied even to localities over the ring of rational integers, which should certainly be included for their geometric interest. Thus Chapters IV and V (except §33) are important for the theory of local rings. It might be thought that we are indulging in unnecessary gen-

erality, but, as far as this writer knows, any restricted treatment which still manages to include localities over rings of integers does not yield substantial simplifications. Some results have proofs which use elementary ideas but which are nevertheless quite difficult. For instance, the validity of the chain condition for prime ideals in a locality over a Dedekind domain can be proved directly, (see Nagata [13]), but the proof is not easy and our generalized treatment in §34 is simpler.

Numerous exercises are included in the book but the reader should not be discouraged if he cannot do all of them. Except for a very few easy problems the results are not used in the text except perhaps for other exercises. Thus the reader need not solve all the problems in order to understand the text. Nevertheless it is advisable to attempt all the problems in order to get a better understanding of the general theory of local rings.

CHAPTER I

General Commutative Rings

1. Rings, ideals, and modules

A ring will always mean a commutative ring with a unit.

When R is a ring and $x_1, \ldots, x_n$ are either indeterminates or elements of a ring containing R, then the ring $R[x_1, \ldots, x_n]$ is well defined. This ring may be denoted simply by $R[x]$ if there will be no confusion.

When R is a ring, an R-module M is such that $1m = m$ for any $m \in M$ (1 being the identity of R). When M is an R-module, a submodule of M will mean R-submodules, unless otherwise stated explicitly. A homomorphism (or an isomorphism) from an R-module M into another R-module N means an R-homomorphism (or an R-isomorphism). A homomorphism ϕ from M into N is said to be *surjective* if $\phi(M) = N$.

Adapting the definition of zero divisors and nilpotent elements, we define: An element a of a ring R is called a *zero divisor* with respect to a given R-module M if there is a non-zero element m of M such that $am = 0$; a is said to be *nilpotent* with respect to M if $a^r M = 0$ for some natural number r; and a is said to be an *annihilator* of M if $aM = 0$.

The intersection of submodules is again a submodule. We say that the intersection $N_1 \cap \cdots \cap N_r$ is *irredundant* if $\bigcap_{i \neq j} N_i \neq \bigcap_i N_i$ for any $j = 1, 2, \ldots, r$.

In the following, let R be a ring, M an R-module and let N, N_λ be submodules of M.

The *sum* of submodules N_λ is the submodule generated by the N_λ, and is denoted by $\sum N_\lambda$. The sum of $N_1, \ldots, N_r$ may be denoted by $N_1 + \cdots + N_r$. Note that $N_1 + \cdots + N_r$ is set-theoretically $\{n_1 + \cdots + n_r \mid n_i \in N_i\}$.

A subset $\{u_\lambda\}$ of N which generates N is called a *basis* for N. A

basis consisting of a finite number of elements is called a *finite basis*. N is called a *finite module* if N has a finite basis. A basis for N is said to be a *minimal basis* for N if any proper subset of the basis is not a basis for N. Note that the submodule of a module generated by the empty set consists of zero.

If $\mathfrak{a}$ is an ideal of R, we define the *product* $\mathfrak{a}N$ to be the submodule of N generated by $\{an \mid a \in \mathfrak{a}, n \in N\}$, this last set itself may not be a module.

Note that if x is an element of R, then $xN = \{xn \mid n \in N\}$ is an R-module.

We call the following well-known theorem the *isomorphism theorem*: $(N_1 + N_2)/N_1$ is naturally isomorphic to $N_2/(N_1 \cap N_2)$.

Next we observe some facts about ideals. In the following, German letters denote ideals of R, and A, B, B_λ, C, D, E, denote subsets of R. $[\mathfrak{a}:B]_C$ denotes the set of elements c of C such that $cB \subseteq \mathfrak{a}$; this set is obviously an ideal if C is an ideal. $[\mathfrak{a}:B]_R$ is denoted simply by $\mathfrak{a}:B$. The following equalities can be verified easily:

$$
\begin{aligned}
[\mathfrak{a}:B]_C &= (\mathfrak{a}:B) \cap C \\
[[\mathfrak{a}:B]_{\mathfrak{b}}:C]_E &= E \cap [\mathfrak{a}:BC]_{\mathfrak{b}:E} \qquad (1.1) \\
[(\bigcap \mathfrak{a}_\lambda):B]_D &= \bigcap [(\mathfrak{a}_\lambda:B)]_D \\
[\mathfrak{a}:(\sum B_\lambda R)]_D &= \bigcap [\mathfrak{a}:B_\lambda]_D
\end{aligned}
$$

We generalize the above to the case of modules, using the following principle, which we call the *principle of idealization*: When an R-module M is given, let R^* be the direct sum $R \oplus M$ as modules. In R^*, we introduce multiplication defined by $(r + m)(r' + m') = rr' + rm' + r'm$, and R^* becomes a ring containing R and M, in which M is an ideal and $M^2 = 0$. Furthermore, submodules of M are nothing but ideals of R^* contained in M; the structure of M as an R-module is substantially the same as that of M as an R^*-module because $R^*/M = R$ and $M^2 = 0$.

Now, for submodules N, N' of M, we defined $N:N'$ to be $\{x \mid x \in R, xN' \subseteq N\}$; if A is a subset of R, then $N:A$, which may better be denoted by $[N:A]_M$, is defined to be $\{m \mid m \in M, \mathfrak{a}m \subseteq N\}$. Then, in $R^* = R \oplus M$ as above, our $N:N'$ is nothing but $[N:N']_R$ and our $N:A$ is nothing but $[N:A]_M$. Therefore (1.1) can be generalized to the case of modules in the following forms:

$$
\begin{aligned}
&(N:A):B = N:AB, && (N:A):N' = N:AN' \\
(1.2)\qquad &(\bigcap N_\lambda):A = \bigcap (N_\lambda:A), && (\bigcap N_\lambda):N = \bigcap (N_\lambda:N) \\
&N:(\sum A_\lambda) = \bigcap (N:A_\lambda), && N:(\sum N_\lambda) = \bigcap (N:N_\lambda)
\end{aligned}
$$

We go back to ideals: Assume that $\mathfrak{a} + \mathfrak{b} = \mathfrak{a} + \mathfrak{c} = R$. Then $R = R^2 = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{bc} \subseteq R$, hence we have $\mathfrak{a} + \mathfrak{bc} = R$. On the other hand, since $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ in general, we have, by our assumption that $\mathfrak{a} + \mathfrak{b} = R$, that $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Furthermore, the isomorphism theorem shows that $R/\mathfrak{ab} = (\mathfrak{a} + \mathfrak{b}) / (\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{b})) + (\mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b})) = ((\mathfrak{a} + \mathfrak{b})/\mathfrak{b}) + ((\mathfrak{a} + \mathfrak{b})/\mathfrak{a}) = R/\mathfrak{b} + R/\mathfrak{a}$; this sum is a direct sum because, in $R/\mathfrak{ab}$, $(\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{b})) \cap (\mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b})) = 0$. Thus we have:

(1.3) *If* $\mathfrak{a} + \mathfrak{b} = R$, $\mathfrak{a} + \mathfrak{c} = R$, *then* $\mathfrak{a} + \mathfrak{bc} = R$ (*hence* $\mathfrak{a} + \mathfrak{b}^2 = R$), $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$, $R/\mathfrak{ab} = R/\mathfrak{a} \oplus R/\mathfrak{b}$.

From this, we deduce:

(1.4) *If, for given ideals* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, *it holds that* $(\bigcap_{i \neq j} \mathfrak{a}_i) + \mathfrak{a}_j = R$ *for every* $j = 1, \ldots, n$, *then, for any power* $\mathfrak{a}_i'$ *of* $\mathfrak{a}_i$, *we have* (a) $(\bigcap_{i \neq j} \mathfrak{a}_i') + \mathfrak{a}_i' = R$ *for any* j, (b) $\prod \mathfrak{a}_i' = \bigcap \mathfrak{a}_i'$, *and* (c) $R/(\bigcap \mathfrak{a}_i') = R/\mathfrak{a}_1' \oplus \cdots \oplus R/\mathfrak{a}_n'$.

Proof: If $n = 2$, then a repeated application of $\mathfrak{a} + \mathfrak{b}^2 = R$ in (1.3) gives (a); and (b) and (c) follow from (a) and (1.3); the general case can be proved easily by induction on n.

Next we give an application of the isomorphism theorem:

(1.5) *Let M be a module over a ring R. Let N be a submodule of M and let m be an element of M. Then $(N + mR)/N$ is isomorphic to $R/(N:mR)$.*

Proof: $(N + mR)/N = mR/(mR \cap N)$ by the isomorphism theorem. Let ϕ be the homomorphism from $R/(N:mR)$ onto $mR/(mR \cap N)$ such that $\phi(x \text{ modulo } N:mR) = (mx \text{ modulo } mR \cap N)$. $\phi(x \text{ modulo } N:mR) = 0$ implies that $mx \in mR \cap N$, whence $mx \in N$ and $x \in N:mR$, and therefore $(x \text{ modulo } N:mR) = 0$. Thus ϕ is an isomorphism, and the assertion is proved.

Similarly we have:

(1.6) *With M, N, and R as above, if $a \in R$, then $(N + aM)/N$ is isomorphic to $M/(N:aR)$.*

We add here some definitions and remarks concerning tensor products. Let R be a ring and let R' be a ring which is an R-module. Then for an R-module M, $M \otimes_R R'$, which is usually denoted simply

by $M \otimes R'$, is naturally an R'-module, though it is still an R-module. We treat $M \otimes R'$ as an R'-module, unless the contrary is explicitly stated. Let ϕ be a homomorphism from an R-module M into an R-module N. Then there is a uniquely determined homomorphism ϕ^* from $M \otimes R'$ into $N \otimes R'$ such that $\phi^*(m \otimes r') = \phi(m) \otimes r'$. This ϕ^* is denoted by $\phi \otimes R'$. It is obvious that:

(1.7) *If ϕ is surjective, then so is $\phi \otimes R'$.*

We say that $\otimes R'$, or more exactly $\otimes_R R'$, is *exact* if for any identity map ϕ from a finite R-module M into a finite R-module N such that $M \subseteq N$, the tensor product $\phi \otimes R'$ is an isomorphism. (This definition can be adapted to the case where R' is just an R-module.)

In closing this section, we define the length of a module. If an R-module M has a composition series $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$, then the length n is independent of the choice of the composition series by the well known Jordan-Hoelder-Schreier theorem. The length n is called the *length* of the R-module M and is denoted by $\text{length}_R M$ or simply by length M.

EXERCISE: Let R be a ring. A sequence of R-modules N_i accompanied by homomorphisms d_i, which is denoted by $N_0 \xleftarrow{d_1} N_1 \xleftarrow{d_2} N_2 \xleftarrow{d_3} \cdots \cdots \xleftarrow{d_{r-1}} N_{r-1} \xleftarrow{d_r} N_r$, is called *exact* if the kernel of d_{i-1} is the image of d_i for $i = 2, \ldots, r$. Prove that, in such a case, if $\otimes R'$ is exact, then $N_0 \otimes R' \xleftarrow{d_1 \otimes R'} N_1 \otimes R' \xleftarrow{d_2 \otimes R'} \cdots \xleftarrow{d_r \otimes R'} N_r \otimes R'$ is exact.

2. Prime ideals and primary ideals

We observe first that the following conditions for an ideal $\mathfrak{p}$ of a ring R ($\mathfrak{p} \neq R$) are equivalent to each other: (1) $\mathfrak{p}$ is a prime ideal of R. (2) If $ab \in \mathfrak{p}$ ($a, b \in R$), then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. (3) If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R such that $\mathfrak{ab} \subseteq \mathfrak{p}$, then either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$. (4) If $\mathfrak{p} \subset \mathfrak{a}$ and $\mathfrak{p} \subset \mathfrak{b}$, then $\mathfrak{ab} \not\subseteq \mathfrak{p}$.

Though the ring R itself satisfies the above conditions, *we exclude it from the set of prime ideals.*

Let S be a multiplicatively closed subset of a ring R. An ideal $\mathfrak{p}$ of R is called a *maximal ideal with respect to* S if $\mathfrak{p}$ does not meet S and if every ideal of R properly containing $\mathfrak{p}$ meets S.

(2.1) THEOREM: *Let S be a multiplicatively closed subset of a ring R. If an ideal $\mathfrak{a}$ of R does not meet S, then there is a maximal ideal $\mathfrak{p}$ with respect to S such that $\mathfrak{p}$ contains $\mathfrak{a}$. Such a $\mathfrak{p}$ is necessarily prime.*

Proof: Let F be the set of ideals $\mathfrak{b}$ containing $\mathfrak{a}$ such that $S \cap \mathfrak{b} =$ empty. Then F is an inductive set (the order being given by the in-

clusion relation). Hence, Zorn's lemma implies the existence of $\mathfrak{p}$. If $\mathfrak{p} \subset \mathfrak{b}$, $\mathfrak{p} \subset \mathfrak{c}$, then $\mathfrak{b}$ and $\mathfrak{c}$ meet S. Hence $\mathfrak{bc}$ meets S and therefore $\mathfrak{bc} \nsubseteq \mathfrak{p}$. This implies that $\mathfrak{p}$ is prime and the theorem is proved.

We say that an ideal $\mathfrak{m}$ is a *maximal ideal* if it is a maximal ideal with respect to $\{1\}$.

By this definition, we have the following corollary to (2.1):

(2.2) *If $\mathfrak{a}$ is an ideal of R and if $\mathfrak{a} \neq R$, then there is a maximal ideal $\mathfrak{m}$ of R which contains $\mathfrak{a}$. Hence, if $\mathfrak{a}$ is a non-unit of R, then there exists a maximal ideal of R which contains $\mathfrak{a}$. A maximal ideal is a prime ideal.*

Furthermore, since a field is characterized as a ring which has no ideals except the zero ideal and the ring itself, we see that an ideal $\mathfrak{m}$ of a ring R is maximal if and only if $R/\mathfrak{m}$ is a field.

For an ideal $\mathfrak{a}$ of a ring R, the intersection of all prime ideals containing $\mathfrak{a}$ is called the *radical* of $\mathfrak{a}$. The radical of the zero ideal is called the *radical* of R. An ideal $\mathfrak{a}$ is called *semi-prime* if the radical of $\mathfrak{a}$ coincides with $\mathfrak{a}$ itself.

(2.3) THEOREM: *The radical of an ideal $\mathfrak{a}$ of a ring R is the set of all elements of R which are nilpotent modulo $\mathfrak{a}$.*

Proof: Assume that $x^n \in \mathfrak{a}$ ($x \in R$) for a natural number n. Then every prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ contains x^n, hence $x \in \mathfrak{p}$, which implies that x is in the radical of $\mathfrak{a}$. Conversely, assume that $x^n \notin \mathfrak{a}$ for any natural number n. Then the set S of powers of x is a multiplicatively closed set which does not meet $\mathfrak{a}$. Therefore (2.1) implies that there is a prime ideal $\mathfrak{p}$ of R containing $\mathfrak{a}$ but not containing x. Hence we see that x is not in the radical of $\mathfrak{a}$. Thus the proof is complete.

(2.4) COROLLARY: *An ideal $\mathfrak{a}$ of a ring R is semi-prime if and only if $R/\mathfrak{a}$ has no nilpotent element except* 0.

Let $\mathfrak{a}$ be an ideal of a ring R. A prime ideal $\mathfrak{p}$ of R is called a *minimal prime divisor* of $\mathfrak{a}$ if it is minimal among prime ideals containing $\mathfrak{a}$.

(2.5) THEOREM: *If an ideal $\mathfrak{a}$ of a ring R is contained in a prime ideal $\mathfrak{p}$, $\mathfrak{p}$ contains a minimal prime divisor of $\mathfrak{a}$.*

Proof: In the set of prime ideals containing $\mathfrak{a}$ and contained in $\mathfrak{p}$, we introduce ordering which is opposite to the inclusion relation. Then we see that the set becomes an inductive set, and we prove the assertion by Zorn's lemma.

(2.6) COROLLARY: *The radical of an ideal $\mathfrak{a}$ is the intersection of all minimal prime divisors of $\mathfrak{a}$.*

(2.7) *If* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *are prime ideals of a ring* R *and if* $\mathfrak{a}$ *is an ideal of* R *which is not contained in any of the* $\mathfrak{p}_i$, *then there is an element* a *of* $\mathfrak{a}$ *which is not contained in any of the* $\mathfrak{p}_i$.

Proof: If one of the $\mathfrak{p}_i$, say $\mathfrak{p}_n$, is contained in some other $\mathfrak{p}_j$, then we may omit $\mathfrak{p}_n$. Therefore we may assume that there is no inclusion relation among the $\mathfrak{p}_i$. Then there is an element a_i of

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_n\mathfrak{a}$$

which is not in $\mathfrak{p}_i$, for each i. Then $a = \sum a_i$ is in $\mathfrak{a}$ and is in none of the $\mathfrak{p}_i$.

An ideal $\mathfrak{q}$ of a ring R ($\mathfrak{q} \neq R$) is called *primary* if every zero divisor of $R/\mathfrak{q}$ is nilpotent, or equivalently, if $ab \in \mathfrak{q}$, $a \notin \mathfrak{q}$($a, b \in R$) imply the nilpotency of b modulo $\mathfrak{q}$. This definition can be expressed as follows:

(2.8) *Let* $\mathfrak{p}$ *be the radical of* $\mathfrak{q}$, *then* $\mathfrak{q}$ *is primary if and only if* $ab \in \mathfrak{q}$, $b \notin \mathfrak{p}$ ($a, b \in R$) *imply* $a \in \mathfrak{q}$.

(2.9) *The radical* $\mathfrak{p}$ *of a primary ideal* $\mathfrak{q}$ *is prime, hence it is the unique minimal prime divisor of* $\mathfrak{q}$.

Proof: $ab \in \mathfrak{p}, a \notin \mathfrak{p}(a, b \in R)$ imply that $a^n b^n \in \mathfrak{q}$ for some natural number n and that $a^n \notin \mathfrak{p}$. Therefore, by (2.8), we have $b^n \in \mathfrak{q}$, hence $b \in \mathfrak{p}$, which proves that $\mathfrak{p}$ is a prime ideal. The last assertion is obvious.

If $\mathfrak{q}$ is a primary ideal with radical $\mathfrak{p}$, we say that $\mathfrak{q}$ is a *primary ideal belonging to* $\mathfrak{p}$ or that $\mathfrak{q}$ is *primary to* $\mathfrak{p}$, or that $\mathfrak{p}$ is *the prime divisor* of $\mathfrak{q}$ (the justification for "the" will be given in (7.6)).

(2.10) *If the radical* $\mathfrak{p}$ *of an ideal* $\mathfrak{a}$ *in a ring* R *is a maximal ideal, then* $\mathfrak{a}$ *is primary.*

Proof: $\mathfrak{p}/\mathfrak{a}$ is the unique prime ideal of $R/\mathfrak{a}$. Therefore, by virtue of (2.2), we see that an element of $R/\mathfrak{a}$ is either a unit or nilpotent, which proves the assertion.

(2.11) *If* $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *are primary ideals with the same prime divisor* $\mathfrak{p}$ *in a ring* R, *then the intersection* $\mathfrak{a}$ *of the* $\mathfrak{q}_i$ *is primary to* $\mathfrak{p}$.

Proof: Let x be an arbitrary element of $\mathfrak{p}$. Then $x^{m_i} \in \mathfrak{q}_i$ for some m_i (for each i), hence $x^m \in \mathfrak{a}$ with $m = \max m_i$, which shows that $\mathfrak{p}$ is contained in the radical of $\mathfrak{a}$. This implies that the radical of $\mathfrak{a}$ is $\mathfrak{p}$. Assume that $ab \in \mathfrak{a}$, $a \notin \mathfrak{p}(a, b \in R)$. Since the $\mathfrak{q}_i$ are primary to $\mathfrak{p}$, we have $b \in \mathfrak{q}_i$ for every i, hence $a \in \mathfrak{a}$, which implies that $\mathfrak{a}$ is a primary ideal belonging to $\mathfrak{p}$.

(2.12) *Let* ϕ *be a homomorphism from a ring* R *into a ring* R'. *If* $\mathfrak{q}'$

is a primary ideal with prime divisor $\mathfrak{p}'$ *in* R', *then* $\mathfrak{q} = \phi^{-1}(\mathfrak{q}')$ *is a primary ideal with prime divisor* $\mathfrak{p} = \phi^{-1}(\mathfrak{p}')$.

Proof: Let x be an element of R. x is nilpotent modulo $\mathfrak{q} \rightleftarrows x^n \in \mathfrak{q}$ for some $n \rightleftarrows \phi(x)^n \in \mathfrak{q}'$ for some $n \rightleftarrows \phi(x) \in \mathfrak{p}' \rightleftarrows x \in \mathfrak{p}$. Thus we see that $\mathfrak{p}$ is the radical of $\mathfrak{q}$. If $ab \in \mathfrak{q}$, $a \notin \mathfrak{p}$, then $\phi(a)\phi(b) \in \mathfrak{q}'$, $\phi(a) \notin \mathfrak{p}'$, hence $\phi(b) \in \mathfrak{q}'$, and therefore $b \in \mathfrak{q}$. Thus we see that $\mathfrak{q}$ is primary to $\mathfrak{p}$.

(2.13) *If* $\mathfrak{q}$ *is a primary ideal of a ring* R *with prime divisor* $\mathfrak{p}$ *and if* a *is an element of* R *which is not in* $\mathfrak{q}$, *then* $\mathfrak{q}:aR$ *is primary to* $\mathfrak{p}$.

Proof: Since $a \notin \mathfrak{q}$, we have $\mathfrak{q} \subseteq (\mathfrak{q}:a) \subseteq \mathfrak{p}$, and $\mathfrak{p}$ is the radical of $(\mathfrak{q}:a)$. Now $bc \in (\mathfrak{q}:a)$, $b \notin \mathfrak{p}$ imply $ca \in \mathfrak{q}$ because $bca \in \mathfrak{q}$. Hence $c \in \mathfrak{q}:a$, proving our assertion.

3. *Noetherian rings*

We say that a ring R is *Noetherian* if it satisfies the maximum condition for ideals, namely, any non-empty set of ideals of R has maximal members. We say that a module M over a ring R is *Noetherian* if it satisfies the maximum condition for (R-)submodules.

Observe that a ring R is a Noetherian R-module if and only if R is a Noetherian ring.

(3.1) THEOREM: *Let* M *be a module over a ring* R. *Then the following three conditions are equivalent to each other*:

(1) M *is Noetherian.*

(2) *If* $N_1, \ldots, N_n, \ldots$ *are submodules of* M *such that* $N_i \subseteq N_{i+1}$ *for any* $i = 1, 2, \ldots$, *then there is an* n *such that* $N_j = N_n$ *for any* $j \geq n$.

(3) *Every submodule of* M *is a finite module.*

Proof: Equivalence between (1) and (2): If there are N_i as in (2), but no such n, then the set of the N_j has no maximal member. This shows that (1) implies (2). Assume, conversely, that (2) is true and let F be any non-empty set of submodules of M. Let N_1 be any arbitrary member of F. When N_i is defined, we define N_{i+1} to be such that: (i) $N_{i+1} = N_i$ if N_i is maximal in F, (ii) N_{i+1} is a member of F such that $N_i \subset N_{i+1}$ if N_i is not maximal. Then, by the validity of (2) we see that some N_n must be maximal in F. Thus (2) implies (1).

Equivalence between (2) and (3): If an R-submodule N of M is not finite, then we see easily that (2) is not true. Thus (2) implies (3).

Conversely, assume that (3) is true and let N_i be as in (2). The union N of the N_i is a submodule of M, hence N is generated by a finite number of elements, say $x_1, \ldots, x_m$. Then they are in some N_i, say N_n, whence $N_n = N$, which implies that $N_j = N_n$ for any $j \geq n$. Thus the proof is complete.

(3.2) COROLLARY: *If an R-module M is Noetherian, then any (R-)homomorphic image of M and any submodules of M are Noetherian.*

(3.3) *Let $\mathfrak{a}$ be an ideal of a ring R and let b be an element of R. If both $\mathfrak{a} + bR$ and $\mathfrak{a}:bR$ have finite bases, then $\mathfrak{a}$ has a finite basis.*

Proof: Let a_i and $c_j (i = 1, \ldots, r; j = 1, \ldots, s)$ be such that $\mathfrak{a} + bR = \sum a_i R + bR$ and $\mathfrak{a}:bR = \sum c_j R$. We may assume that the a_i are in $\mathfrak{a}$. Let $\mathfrak{a}'$ be the ideal generated by the a_i and the bc_j. Then we have $\mathfrak{a}' \subseteq \mathfrak{a}$. Let a be an arbitrary element of $\mathfrak{a}$. Then, since $a \in \mathfrak{a}' + Rb$, $a \equiv rb$ (modulo $\mathfrak{a}'$) with an $r \in R$. Since $a \in \mathfrak{a}$, we have $rb \in \mathfrak{a}$, hence $r \in \mathfrak{a}:bR = \sum c_j R$. Therefore $rb \in \mathfrak{a}'$. Thus $a \in \mathfrak{a}'$, and we have $\mathfrak{a} = \mathfrak{a}'$ and the proof is complete.

(3.4) THEOREM: *A ring R is Noetherian if and only if every prime ideal of R has a finite basis.* (THEOREM OF COHEN)

Proof: The *only if* part is a consequence of (3.1). Assume that every prime ideal of R has a finite basis and that R is not Noetherian, which means, by virtue of (3.1), that there are ideals which have no finite basis. Let F be the set of ideals of R which have no finite basis. Then F is an inductive set; for, if $\{N_\lambda\}$ is a well-ordered subset of F and if the union N of all the N_λ has a finite basis, say $x_1, \ldots, x_r$, then they are in some N_j and we have $N_j = N$, which contradicts the assumption that N_j has no finite basis, hence we have $N \in F$. Therefore there is a maximal member $\mathfrak{a}$ in F. By our assumption, $\mathfrak{a}$ is not a prime ideal, hence there are elements a, b of R which are not in $\mathfrak{a}$ such that $ab \in \mathfrak{a}$. Then both $\mathfrak{a} + bR$ and $\mathfrak{a}:bR$ contain $\mathfrak{a}$ properly, hence they have finite bases by the maximality of $\mathfrak{a}$ in F. Therefore, by (3.3), we see that $\mathfrak{a}$ has a finite basis, which contradicts the fact that $\mathfrak{a} \in F$. Thus F must be empty, and R is Noetherian.

(3.5) THEOREM: *A finite module M over a Noetherian ring R is a Noetherian module.*

Proof: We prove the assertion by induction on the number of generators of M. If M is generated by the empty set, then $M = 0$ and the assertion is obvious. Assume now that $M = Rx_1 + \cdots + Rx_r$ and that $M' = \sum_2^r Rx_i$ is Noetherian. Let N be an arbitrary R-sub-

module of M. Let $\mathfrak{a}$ be the set of elements a of R such that $ax_1 \in N + M'$, i.e., $\mathfrak{a} = (N + M') : Rx_1$. Then $\mathfrak{a}$ is an ideal of R; hence $\mathfrak{a}$ has a finite basis, say $a_1, \ldots, a_m$. Let d_i be, for each $i = 1, \cdots, m$, such that $d_i \in N$ and such that $d_i - a_i x_1 \in M'$, and let N' be the submodule $\sum Rd_i$ of N. Then $N = N' + (N \cap M')$. Since M' is Noetherian by our assumption, $N \cap M'$ has a finite basis, hence N has a finite basis. Therefore M is Noetherian.

(3.6) THEOREM: *If a ring R' is generated by a finite number of elements over a Noetherian ring R, then R' is Noetherian.* (HILBERT BASIS THEOREM)

Proof: Using an induction argument on the number of generators, we may treat only the case where $R' = R[x]$ with a single element x of R'. Let $\mathfrak{a}'$ be an arbitrary ideal of R'. Let $\mathfrak{a}$ be the set of elements a of R such that there is an element a' of $\mathfrak{a}'$ of the form $a' = ax^s + c_1x^{s-1} + \cdots + c_s$ (for a suitable natural number s and elements c_i of R). Then $\mathfrak{a}$ is an ideal of R. Since R is Noetherian, $\mathfrak{a}$ has a finite basis, say $a_1, \ldots, a_m$. Let a_i' be, for each i, an element of $\mathfrak{a}'$ such that $a_i' - a_i x^s \in Rx^{s-1} + \cdots + Rx + R$ for some s. Considering elements of the form $a_i' x^\alpha$, we may assume that s is common to all a_i'. Let $\mathfrak{a}''$ be the ideal of R' generated by the a_i'. Then, by our choice of $\mathfrak{a}''$, we see that every element of $\mathfrak{a}'$ is congruent to an element of $Rx^{s-1} + \cdots + Rx + R$ modulo $\mathfrak{a}''$, namely,

$$\mathfrak{a}' = (\mathfrak{a}' \cap (\textstyle\sum_0^{s-1} Rx^i)) + \mathfrak{a}''.$$

Since $\sum_0^{s-1} Rx^i$ is a finite R-module, it is Noetherian. Hence $\mathfrak{a}' \cap (\sum_0^{s-1} Rx^i)$ has a finite basis. Therefore $\mathfrak{a}'$ has a finite basis, which proves that R' is Noetherian.

(3.7) THEOREM: *Let M be a finite module over a Noetherian ring R and let N, N' be (R-)submodules of M. Let $\mathfrak{a}$ be an ideal of R. Then there is a natural number r such that*

$$\mathfrak{a}^n N \cap N' = \mathfrak{a}^{n-r}(\mathfrak{a}^r N \cap N')$$

for natural numbers n which are greater than r. (LEMMA OF ARTIN-REES)

Proof: By the principle of idealization and by the fact that $R \oplus M$ becomes a Noetherian ring by virtue of (3.6) (Hilbert basis theorem), we may assume that M, N, N' are ideals of R. Let $a_1, \ldots, a_s$ be a basis for $\mathfrak{a}$ and let $x_1, \ldots, x_s$ be indeterminates. Let S_n be the set of

homogeneous forms $f(x_1, \ldots, x_s)$ of degree n in the x_i such that $f(a_1, \ldots, a_s) \in \mathfrak{a}^n N \cap N'$. Let S be the union of all the S_n and let $\mathfrak{A}$ be the ideal of $R[x]$ generated by S. Since $R[x]$ is Noetherian by the Hilbert basis theorem, $\mathfrak{A}$ is generated by a finite subset $f_1, \ldots, f_t$ of S. Let d_i be the degree of f_i and set $r = \max d_i$. For $n > r$, let a be an element of $\mathfrak{a}^n N \cap N'$. Since $a \in \mathfrak{a}^n$, there is an $f \in S_n$ such that $f(a_1, \ldots, a_s) = a$. Since $f \in S, f = \sum f_i g_i$ with $g_i \in R[x]$. Comparing the degrees, we may assume that g_i is a homogeneous form of degree $n - d_i$. Thus we have $a = f(a_1, \ldots, a_s) = \sum f_i(a_1, \ldots, a_s) \times g_i(a_1, \ldots, a_s) \in \sum \mathfrak{a}^{n-d_i}(\mathfrak{a}^{d_i} N \cap N') \subseteq \mathfrak{a}^{n-r}(\mathfrak{a}^r N \cap N')$. Thus we see that $\mathfrak{a}^n N \cap N' \subseteq \mathfrak{a}^{n-r}(\mathfrak{a}^r N \cap N')$. Since the converse inclusion is obvious, we have completed the proof.

(3.8) *Let $\mathfrak{a}$ be an ideal of a Noetherian ring R and let M be a finite R-module. Set $N = \bigcap_n \mathfrak{a}^n M$. Then $\mathfrak{a}N = N$.*

Proof: By (3.7) (the lemma of Artin-Rees), we have $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$ for $n > r$. Hence we have $N = \mathfrak{a}^{n-r} N$, which proves our assertion.

(3.9) *Let a_{ij} and $t_j (i, j = 1, \ldots, s)$ be elements of a ring R. If $\sum_j a_{ij} t_j = 0$ for $i = 1, \ldots, s$, then, denoting by d the determinant $|\, a_{ij} \,|$, we have $dt_j = 0$ for any j.*

Proof: Let d_{ij} be the cofactor of a_{ij} in the determinant $|\, a_{ij} \,|$. Then $\sum_i d_{ij} a_{ij} = d$, $\sum_i d_{ij} a_{ik} = 0$ $(j \neq k)$. Therefore

$$0 = \sum_i d_{ij} (\sum_k a_{ik} t_k) = dt_j .$$

(3.10) *Let M be a finite module over a ring R such that $\mathfrak{a}M = M$ for an ideal $\mathfrak{a}$ of R. If no element a of R such that $a - 1 \in \mathfrak{a}$ is a zero divisor with respect to M, then $M = 0$.*

Proof: Let $t_1, \ldots, t_s$ be elements of M such that $M = \sum Rt_i$. Then the relation $\mathfrak{a}M = M$ shows that there are elements $a_{ij} \in \mathfrak{a}$ such that $t_i = \sum a_{ij} t_j$ for every $i = 1, \ldots, s$. Let d be the determinant $|\, \delta_{ij} - a_{ij} \,|$ (δ_{ij} being the Kronecker δ). Then $d \equiv 1 \pmod{\mathfrak{a}}$, hence d is not a zero divisor with respect to M. On the other hand, $dt_i = 0$ by (3.9), which implies that $t_i = 0$ by our assumption. Thus $M = 0$.

(3.11) THEOREM: *Let M be a finite module over a Noetherian ring R and let $\mathfrak{a}$ be an ideal of R. Then $\bigcap_n \mathfrak{a}^n M = 0$ if and only if no element a of R such that $a - 1 \in \mathfrak{a}$ is a zero divisor with respect to M.* (INTERSECTION THEOREM OF KRULL)

Proof: Assume at first that such an element a is not a zero divisor with respect to M. Set $N = \bigcap_n \mathfrak{a}^n M$. Then $\mathfrak{a}N = N$ by (3.8). Since

M is Noetherian, N has a finite basis. Therefore the relation $\mathfrak{a}N = N$ shows that $N = 0$ by (3.10). Conversely, assume that there is a zero divisor a with respect to M such that $a - 1 \in \mathfrak{a}$. Let m be a non-zero element of M such that $am = 0$. Then we have $(1 - a)m = m$, hence $(1 - a)^n m = m$ for any natural number n. Therefore $m \in \mathfrak{a}^n M$ for any n, and $\bigcap_n \mathfrak{a}^n M \neq 0$.

(3.12) THEOREM: *Let M be a finite module over a Noetherian ring R, let $\mathfrak{a}$ be an ideal of R and let x be an element of R. Then there is an integer r such that $\mathfrak{a}^n M : xR \subseteq [0 : xR]_M + \mathfrak{a}^{n-r} M$ for $n > r$.*

Proof: $x(\mathfrak{a}^n M : xR) = \mathfrak{a}^n M \cap xM = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap xM) \subseteq x\mathfrak{a}^{n-r} M$ by (3.7) (the lemma of Artin-Rees). Therefore, if $y \in \mathfrak{a}^n M : xM$, then there is an element $y' \in \mathfrak{a}^{n-r} M$ such that $xy = xy'$, whence $y - y' \in [0 : xR]_M$, which proves the assertion.

(3.13) COROLLARY: *With the same notation as above, if N is a submodule of M, then there is an integer r such that $(N + \mathfrak{a}^n M) : xR \subseteq [N : xR]_M + \mathfrak{a}^{n-r} M$ for $n > r$.*

Proof: Applying (3.12) to $M' = M/N$, we prove the assertion.

(3.14) COROLLARY: *Let M, N, $\mathfrak{a}$, and R be the same as above and let x be an element of M. Then there is an integer r such that*

$$(N + \mathfrak{a}^n M) : xR \subseteq (N : xR) + \mathfrak{a}^{n-r} \quad \text{for} \quad n > r.$$

Proof: The proof of (3.12) can be applied to the case where $N = 0$ if we replace xM with xR, whence we prove the assertion in the same way as in (3.13).

(3.15) *If an ideal $\mathfrak{a}$ is generated by a finite number of nilpotent elements, then $\mathfrak{a}$ is nilpotent. Consequently, if $\mathfrak{a}'$ is the radical of an ideal $\mathfrak{a}$ in a Noetherian ring, then $\mathfrak{a}'$ is nilpotent modulo $\mathfrak{a}$.*

Proof: Let $a_1, \ldots, a_m$ be a basis for $\mathfrak{a}$ such that each of the a_i is nilpotent. Then there is a natural number n such that $a_i^n = 0$ for every i. If r is greater than $m(n - 1)$, then any monomial of degree r in the a_i has a formal factor a_i^n for at least one i, which shows that such a monomial must be zero, and $\mathfrak{a}^r = 0$. The last assertion follows from (3.1) and what we have proved.

We add here the following theorem and an application:

(3.16) THEOREM: *If a ring R has ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that $\bigcap_i \mathfrak{b}_i = 0$, and such that each $R/\mathfrak{b}_i$ is Noetherian, then R is Noetherian.*

Proof: Using induction on n, we may assume that $n = 2$. The sum $\mathfrak{b}_1 + \mathfrak{b}_2$ is a direct sum in that case. There are a finite number of ele-

ments b_i of $\mathfrak{b}_1$ such that $\mathfrak{b}_1 + \mathfrak{b}_2 = \sum b_i R + \mathfrak{b}_2$. From the properties of direct sums, we see that the b_i generate $\mathfrak{b}_1$. Thus $\mathfrak{b}_1$ has a finite basis; similarly $\mathfrak{b}_2$ has a finite basis. Let now $\mathfrak{p}$ be an arbitrary prime ideal of R. Then $\mathfrak{p}$ contains one $\mathfrak{b}_i$. Since $\mathfrak{b}_i$ and $\mathfrak{p}/\mathfrak{b}_i$ have finite bases, we see that $\mathfrak{p}$ has a finite basis, which proves the assertion by virtue of (3.4) (the theorem of Cohen).

(3.17) COROLLARY: *If M is a Noetherian module over a ring R, then $R/(0:M)$ is a Noetherian ring and M is a finite $R/(0:M)$-module.*

Proof: The finiteness of M is obvious by (3.1). Let $u_1, \ldots, u_n$ be a basis for M. Then Ru_i is Noetherian and is isomorphic to $R/(0:Ru_i)$. Hence $R/(0:Ru_i)$ is Noetherian for each i. Now, $0:M = \bigcap_i (0:Ru_i)$ by (1.2), and we have the proof by (3.16).

We note that we have made use of the following in the above proof:

(3.18) *The structure of the R-module M is the same as the structure of the $R/(0:M)$-module M.*

EXERCISES: *1.* Prove (3.7), (3.8), and (3.11) without assuming that the ring R is Noetherian but assuming that M is a Noetherian module.

2. Let $\mathfrak{a}$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ be ideals of a Noetherian ring R. Prove that there exists a natural number r such that $\bigcap_i \mathfrak{a}^n\mathfrak{b}_i = \mathfrak{a}^{n-r}(\bigcap_i \mathfrak{a}^r\mathfrak{b}_i)$ for $n > r$. (Hint: Consider the direct sum of m copies of R as an R-module.)

3. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a Noetherian integral domain R. Prove that there exists a natural number r such that $\mathfrak{a}^n:\mathfrak{b} = \mathfrak{a}^{n-r}(\mathfrak{a}^r:\mathfrak{b})$ for $n > r$.

4. Jacobson radicals

The intersection $\mathfrak{m}$ of all maximal ideals of a ring R is called the *Jacobson radical* of R. It is obvious, by virtue of (2.2), that if $a - 1 \in \mathfrak{m}$, then a is a unit in R.

(4.1) THEOREM: *Let $\mathfrak{m}$ be the Jacobson radical of a ring R and let M be a finite R-module. If N is a submodule of M such that $M = \mathfrak{m}M + N$, then $M = N$.* (LEMMA OF KRULL-AZUMAYA)

Proof: Set $M' = M/N$. Then M' is a finite module and $M' = \mathfrak{m}M'$. Hence, by (3.10), we have $M' = 0$, namely, $M = N$.

(4.2) THEOREM: *If $\mathfrak{m}$ is the Jacobson radical of a Noetherian ring R, and if M is a finite R-module, then $\bigcap_n \mathfrak{m}^n M = 0$; in particular,*

$$\bigcap_n \mathfrak{m}^n = 0.$$

This is an immediate consequence of (3.11).

(4.3) THEOREM: *Let a be an element of the Jacobson radical of a*

Noetherian ring R and assume that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R such that $\mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{a} \subseteq aR + \mathfrak{b}$. If $\mathfrak{a}:aR = \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$.

Proof: a modulo $\mathfrak{b}$ is in the Jacobson radical of $R/\mathfrak{b}$ and therefore we may assume that $\mathfrak{b} = 0$. Then $\mathfrak{a} \subseteq Ra$, which implies that $\mathfrak{a} = a(\mathfrak{a}:a) = a\mathfrak{a}$. Therefore we have $\mathfrak{a} = 0$ by (3.10), which proves our assertion.

5. *The definition of local rings*

Local rings and semi-local rings, which are defined below, are naturally topological rings. But the topology will be introduced in Chapter II, §16. We give here only ring-theoretic definitions of them.

A ring R is called a *quasi-semi-local ring* if it has only a finite number of maximal ideals; it is called a *quasi-local ring* if it has only one maximal ideal.

A Noetherian quasi-semi-local ring is called a *semi-local ring*; a Noetherian quasi-local ring is called a *local ring*.

When we say that $(R, \mathfrak{p}_1, \ldots, \mathfrak{p}_r)$ is a quasi-semi-local ring (or semi-local ring, or quasi-local ring, or local ring), we mean that R is a quasi-semi-local ring (or semi-local ring, *etc.*) and that the maximal ideals of R are the $\mathfrak{p}_i$.

It is sometimes convenient to have a name for quasi-local rings $(R, \mathfrak{m})$ such that $\bigcap_n \mathfrak{m}^n = 0$. Note that, by virtue of (4.2), local rings are included in the family of such quasi-local rings. Therefore we call such quasi-local rings *local rings which may not be Noetherian*. Similarly, a quasi-semi-local ring R with the Jacobson radical $\mathfrak{m}$ is called a *semi-local ring which may not be Noetherian* if $\bigcap_n \mathfrak{m}^n = 0$.

We give some applications of the lemma of Krull-Azumaya (4.1):

(5.1) *Let $(R, \mathfrak{m})$ be a quasi-local ring and let M be a finite R-module. Then a subset $\{u_\lambda\}$ of M is a basis for M if and only if the set of residue classes $\{u'_\lambda\}$ of $\{u_\lambda\}$ is a basis for $M/\mathfrak{m}M$ over $R/\mathfrak{m}$. Consequently, the u_λ form a minimal basis for M if and only if the u'_λ form a linearly independent basis for $M/\mathfrak{m}M$ over the field $R/\mathfrak{m}$.*

Proof: Setting $N = \sum Ru_i$, the assertion follows immediately from the lemma of Krull-Azumaya.

We note that the above proof shows that:

(5.2) *The first half of* (5.1) *is true for any ring R if $\mathfrak{m}$ is the Jacobson radical of R.*

The following is an immediate corollary to (5.1) and shows a nice property of quasi-local rings:

(5.3) *If M is a finite module over a quasi-local ring R, then any basis for M contains a minimal basis for M as a subset; if $u_1, \ldots, u_m$ and $v_1, \ldots, v_n$ are minimal bases of M, then $m = n$ and there is an invertible linear transformation T over R such that $(u_1, \ldots, u_n)T = (v_1, \ldots, v_n)$.*

Let R be a subring of a ring R'. We say that an ideal $\mathfrak{a}'$ of R' *lies over* an ideal $\mathfrak{a}$ of R if $\mathfrak{a} = \mathfrak{a}' \cap R$.

We say that a ring R is *dominated* by another ring R' if: (1) $R \subseteq R'$, (2) every ideal of R which is different from R generates an ideal in R' which is different from R', and (3) every maximal ideal of R' lies over a maximal ideal of R. In that case, we write $R \leq R'$; $R < R'$ means that $R \leq R'$ and $R \neq R'$.

Therefore, a quasi-local ring $(R', \mathfrak{m}')$ dominates a quasi-local ring $(R, \mathfrak{m})$ if and only if $R \subseteq R'$ and $\mathfrak{m} = \mathfrak{m}' \cap R$.

6. Rings of quotients

Let R be a ring and let S be a multiplicatively closed subset of R which does not contain zero. Let U be the set of non-zero divisors of R. Let $\mathfrak{n}$ be the set of elements a of R such that there is an element s of S with $as = 0$. Since S is multiplicatively closed, $\mathfrak{n}$ becomes an ideal of R. Let ϕ be the natural homomorphism from R onto $R/\mathfrak{n}$. Then we have the following lemma:

(6.1) *If a is an element of the multiplicatively closed set generated by U and S, then $\phi(a)$ is not a zero divisor in $R/\mathfrak{n}$.*

Proof: Since U and S are multiplicatively closed, $a = us$ with $u \in U$, $s \in S$. Assume that $\phi(a)\phi(b) = 0$ $(b \in R)$. Then $ab = usb \in \mathfrak{n}$, hence there is an element s' of S such that $usbs' = 0$. Since u is not a zero divisor, we have $ss'b = 0$. Since $ss' \in S$, we have $b \in \mathfrak{n}$, hence $\phi(b) = 0$, which proves that $\phi(a)$ is not a zero divisor in $R/\mathfrak{n}$.

Now we define the notion of rings of quotients; we must treat three cases.

In the set $P = \{(a, u) \mid a \in R, u \in U\}$, we introduce an equivalence relation such that (a, u) is equivalent to (b, v) if and only if $av = bu$. We denote the equivalence class of (a, u) by a/u. The set Q of the equivalence classes becomes a ring under the operations such that the sum and the product of a/u and b/v are $(av + bu)/uv$ and ab/uv, respectively. Q is called the *total quotient ring* of R. Elements a of R can be identified with $a/1$ of Q. Thus Q contains R and Q is generated by R and the inverses $1/u$ of the elements u of U.

Now we consider the general case: By (6.1), $\phi(S)$ consists only of non-zero-divisors, hence the subring of the total quotient ring of $\phi(R)$ generated by $\phi(R)$ and the inverses of the elements of $\phi(S)$ is well defined. This subring is called the *ring of quotients of R with respect to S.*

Note that $R_S = \{\phi(a)/\phi(s) \mid a \in R, s \in S\}$ and that $\phi(a)/\phi(s) = \phi(a)\cdot\phi(s)^{-1}$.

The third case occurs when S is the complement of a prime ideal $\mathfrak{p}$. Though this is a special case of the above, we use a different notation; R_S is called the *ring of quotients of R with respect to* $\mathfrak{p}$, and is denoted by $R_{\mathfrak{p}}$.

A ring R^* is called a *ring of quotients* of R if there is a multiplicatively closed subset S of R such that ($0 \notin S$ and) $R^* = R_S$.

We use the following notation:

(a) If $\mathfrak{a}$ is a subset of R, then the ideal of R_S generated by $\phi(\mathfrak{a})$ is denoted by $\mathfrak{a}R_S$.

(b) If $\mathfrak{a}'$ is an ideal of R_S, we denote by $\mathfrak{a}' \cap R$ the ideal $\phi^{-1}(\mathfrak{a}') = \phi^{-1}(\mathfrak{a}' \cap \phi(R))$.

The following is a characteristic property of R_S:

(6.2) *If there are a ring R' and a homomorphism σ from R into R' such that for any $s \in S$, $\sigma(s)$ has an inverse in R', then there is a homomorphism τ from R_S into R' such that $\sigma = \tau\phi$.*

Proof: Let $\mathfrak{a}$ be the kernel of σ. Since all elements of S are mapped to units, we see that $\sigma(\mathfrak{n}) = 0$; i.e., $\mathfrak{n} \subseteq \mathfrak{a}$, which means that there is a homomorphism τ' from $\phi(R)$ into R' such that $\sigma = \tau'\phi$. We define a mapping τ by the relation $\tau(\phi(a)/\phi(s)) = \tau'\phi(a)[\tau'\phi(s)]^{-1}$ and we see easily that this τ is the required homomorphism.

As a consequence, we have:

(6.3) *Let $\mathfrak{a}$ be an ideal of R which does not meet S and let σ be the natural homomorphism from R onto $R/\mathfrak{a}$. Then $\sigma(R)_{\sigma(S)} = R_S/\mathfrak{a}R_S$.*

(6.4) THEOREM: *If $\mathfrak{a}'$ is an ideal of R_S, then $(\mathfrak{a}' \cap R)R_S = \mathfrak{a}'$.*

Proof: We have

$$(\mathfrak{a}' \cap R)R_S = \phi(\phi^{-1}(\mathfrak{a}' \cap \phi(R))R_S = (\mathfrak{a}' \cap \phi(R))R_S \subseteq \mathfrak{a}'.$$

If $\phi(a)/\phi(s) \in \mathfrak{a}'$, then $\phi(a)$ is in $\mathfrak{a}' \cap \phi(R)$, and therefore $\phi(a)/\phi(s)$ is in $(\mathfrak{a}' \cap R)R_S$ (because $1/\phi(s)$ is in R_S), which proves that $(\mathfrak{a}' \cap R)R_S \supseteq \mathfrak{a}'$, and the assertion is proved.

(6.5) COROLLARY: *If R is Noetherian, then R_S is Noetherian.*

(6.6) THEOREM: *Assume that* $\mathfrak{q}$ *is a primary ideal of* R *belonging to a prime ideal* $\mathfrak{p}$. *Then*:

(a) *If* $\mathfrak{p}$ *meets* S, *then* $\mathfrak{p}R_S = \mathfrak{q}R_S = R_S$.

(b) *If* $\mathfrak{p}$ *does not meet* S, *then* $\mathfrak{q}$ *contains* $\mathfrak{n}$, $\mathfrak{p}R_S$ *is a prime ideal,* $\mathfrak{q}R_S$ *is primary to* $\mathfrak{p}R_S$, $\mathfrak{p}R_S \cap R = \mathfrak{p}$, *and* $\mathfrak{q}R_S \cap R = \mathfrak{q}$.

Proof: If $\mathfrak{p}$ meets S, then $\mathfrak{q}$ meets S because any power of an element of S is in S. Therefore we have (a). Assume that $\mathfrak{p}$ does not meet S. If a is in $\mathfrak{n}$, then there is an s in S such that $as = 0$, hence $as \in \mathfrak{q}$. Since $s \notin \mathfrak{p}$, it follows that $a \in \mathfrak{q}$, hence $\mathfrak{n} \subseteq \mathfrak{q}$. Let b be an element of $\mathfrak{q}R_S \cap R$. Then $\phi(b) = \phi(q)/\phi(s)$ with $q \in \mathfrak{q}$, $s \in S$. Hence $\phi(bs)$ is in $\phi(\mathfrak{q})$. Since $\mathfrak{n} \subseteq \mathfrak{q}$, we have $bs \in \mathfrak{q}$. Since $s \notin \mathfrak{p}$, we have $b \in \mathfrak{q}$, which proves that $\mathfrak{q}$ contains $\mathfrak{q}R_S \cap R$; since the converse inclusion is obvious, we have $\mathfrak{q} = \mathfrak{q}R_S \cap R$. As a particular case, where $\mathfrak{p} = \mathfrak{q}$, we have $\mathfrak{p} = \mathfrak{p}R_S \cap R$. Next we assume that $\phi(ab)/\phi(st) \in \mathfrak{q}R_S$ and that $\phi(a)/\phi(s) \notin \mathfrak{q}R_S$. Then $ab \in \mathfrak{q}R_S \cap R = \mathfrak{q}$ and $a \notin \mathfrak{q}$, hence $b^r \in \mathfrak{q}$ and $(\phi(b)/\phi(t))^r \in \mathfrak{q}R_S$ (for some r), which proves that $\mathfrak{q}R_S$ is a primary ideal. Now, applying this to the case where $\mathfrak{p} = \mathfrak{q}$, we see that $\mathfrak{p}R_S$ is a prime ideal because in that case r can be taken to be 1. Since elements of $\mathfrak{p}$ are nilpotent modulo $\mathfrak{q}$, elements of $\mathfrak{p}R_S$ are nilpotent modulo $\mathfrak{q}R_S$. Therefore $\mathfrak{q}R_S$ belongs to $\mathfrak{p}R_S$. Thus the proof is complete.

(6.7) COROLLARY: *Let* $\mathfrak{p}$ *be a prime ideal of* R. *Then* $\mathfrak{p}R_S$ *is a maximal ideal if and only if* $\mathfrak{p}$ *is maximal with respect to* S.

(6.8) COROLLARY: *If an ideal* $\mathfrak{a}$ *of* R *does not meet* S *then,* $\mathfrak{a}R_S \neq R_S$.

(6.9) THEOREM: *Let* $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *be primary ideals of* R. *Then* $(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n)R_S = \mathfrak{q}_1R_S \cap \cdots \cap \mathfrak{q}_nR_S$. *If* $\mathfrak{q}_1 \not\supseteq \bigcap_{i\geq 2} \mathfrak{q}_i$ *and if* $\mathfrak{q}_1R_S \neq R_S$, *then* $\mathfrak{q}_1R_S \not\supseteq \bigcap_{i\geq 2} \mathfrak{q}_iR_S$.

Proof: Set $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. We renumber $\mathfrak{q}_i$ so that $\mathfrak{q}_i \cap S$ is empty if and only if $i \leq r$. Since $\mathfrak{q}_iR_S$ contains $\mathfrak{a}R_S$, $\mathfrak{a}R_S$ is contained in $\mathfrak{q}_1R_S \cap \cdots \cap \mathfrak{q}_nR_S$ $(= \mathfrak{q}_1R_S \cap \cdots \cap \mathfrak{q}_rR_S)$. Let $\phi(a)/\phi(s)$ $(a \in R, s \in S)$ be an element of $\mathfrak{q}_1R_S \cap \cdots \cap \mathfrak{q}_rR_S$. Since $\mathfrak{q}_iR_S \cap R = \mathfrak{q}_i$ for $i \leq r$, a is in $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. Take elements $s_{r+1}, \ldots, s_n$ of S so that s_{r+j} is in $\mathfrak{q}_{r+j}$. Then $a' = as_{r+1} \cdots s_n$ is in $\mathfrak{a}$. Therefore $\phi(a)/\phi(s) = \phi(a')/\phi(ss_{r+1} \cdots s_n)$ is in $\mathfrak{a}R_S$, which proves the converse inclusion. Thus we see that $\mathfrak{a}R_S = \mathfrak{q}_1R_S \cap \cdots \cap \mathfrak{q}_rR_S$. Now we assume that $\mathfrak{q}_1 \not\supseteq \bigcap_{i\geq 2} \mathfrak{q}_i$ and that $r \geq 1$. Take an element a of $\bigcap_{i\geq 2} \mathfrak{q}_i$ which is not in $\mathfrak{q}_1$. Then since $\mathfrak{q}_1R_S \cap R = \mathfrak{q}_1$, $\phi(a)$ is not in $\mathfrak{q}_1R_S$, which shows that $\mathfrak{q}_1R_S \not\supseteq \bigcap_{i\geq 2} \mathfrak{q}_1R_S$.

(6.10) COROLLARY: *Assume that the zero ideal of R can be expressed as the intersection of primary ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$ of R, where $\mathfrak{q}_i \cap S$ is empty if and only if $i \leq r$. Then the ideal $\mathfrak{n}(=\phi^{-1}(0))$ coincides with $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$.*

Proof: $\mathfrak{n} = \phi^{-1}(0)$ and therefore $\mathfrak{n} = (0)R_S \cap R$. By our assumption, $(0)R_S = \mathfrak{q}_1 R_S \cap \cdots \cap \mathfrak{q}_r R_S$ and therefore $\mathfrak{n} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$.

(6.11) *Let R be a ring and let S be a multiplicatively closed subset of R which does not contain zero. Let S' be a multiplicatively closed subset of R_S which does not contain zero. Let S'' be the multiplicatively closed subset of R generated by S and all elements s'' of R such that with a suitable element s of S, $\phi(s'')/\phi(s)$ is in S', where ϕ is the natural homomorphism from R into R_S. Then $R_{S''} = (R_S)_{S'}$.*

Proof: Let θ and π be the natural homomorphisms from R into $R_{S''}$ and from R_S into $(R_S)_{S'}$, respectively. Then every element of $\pi\phi(S'')$ has inverse in $(R_S)_{S'}$ and $(R_S)_{S'}$ is generated by $\pi\phi(R)$ and inverses of elements of $\pi\phi(S'')$. Therefore there exists a homomorphism from $R_{S''}$ onto $(R_S)_{S'}$. Let $\mathfrak{n}''$ be the kernel of $\pi\phi$. Then for every element a of $\mathfrak{n}''$, there exists an element $\phi(s'')/\phi(s)(s \in S, s'' \in S'')$ of S' such that $\phi(a)\phi(s'')/\phi(s) = 0$. Then as'' is in the kernel of ϕ, whence there exists an element s' of S such that $as''s' = 0$. Since $s''s'$ is in S'', a is in the kernel of θ. Therefore $\theta = \pi\phi$, whence $R_{S''} = (R_S)_{S'}$.

(6.12) *Let R be a ring and let S be a multiplicatively closed subset of R which contains no zero divisor. If a ring R' contains R and is contained in R_S, then $R_S = R'_S$.*

The proof is straightforward, and we omit it.

We introduce the following notation: Let R be a ring and let x be a transcendental element over R. Let S be the set of polynomials $f \in R[x]$ whose coefficients generate the unit ideal R in R. Then S is a multiplicatively closed subset of $R[x]$, S contains no zero divisor because of the following lemma:

(6.13) *An element $\sum_i^r a_i x^i (a_i \in R)$ is a zero divisor in $R[x]$, if and only if there is an element $b \neq 0$ of R such that $ba_i = 0$ for every i.*

Proof: The *if* part is obvious. Assume that $\sum a_i x^i$ is a zero divisor. There is a non-zero element $\sum_0^s b_j x^j$ such that

$$(\sum a_i x^i)(\sum b_j x^j) = 0.$$

We prove the existence of b as in the assertion by induction on the degree s of $\sum b_j x^j$. If $s = 0$, it is obvious and we assume that $s > 0$.

If $(\sum a_i x^i)b_s = 0$, then there is nothing to prove, and we assume that $a_i b_s \neq 0$ for some i, which means that $a_j(\sum b_i x^i) \neq 0$ for some j; let t be the largest j such that the non-equality holds. Then

$$(\sum_0^t a_i x^i)(\sum b_j x^j) = 0$$

and therefore $a_t b_s = 0$. Therefore $f = a_t(\sum b_j x^j)$ is different from zero and $\deg f < s$. Furthermore, obviously $(\sum a_i x^i)f = 0$, and we prove the assertion by induction.

Now since S does not contain any zero divisor, the ring $R[x]_S$ contains R. This $R[x]_S$ is denoted by $R(x)$. When $x_1, \ldots, x_n$ are algebraically independent, we can define $R(x_1)(x_2) \cdots (x_n)$. This last ring is denoted by $R(x_1, \ldots, x_n)$, or simply by $R(x)$.

The following lemma is easily seen (*cf.* (6.17) below):

(6.14) *With R and the x_i as above, if R is quasi-local, or local, or quasi-semi-local, or semi-local or Noetherian then so is $R(x_1, \ldots, x_n)$, respectively.*

As an immediate consequence of (6.13), we have:

(6.15) *If $\mathfrak{q}$ is a primary ideal belonging to a prime ideal $\mathfrak{p}$ in R, then in the polynomial ring $R[x] = R[x_1, \ldots, x_n]$, $\mathfrak{p}R[x]$ is a prime ideal and $\mathfrak{q}R[x]$ is primary to $\mathfrak{p}R[x]$; obviously $\mathfrak{q}R[x] \cap R = \mathfrak{q}$.*

We note by the way that the following is obvious from the uniqueness of the expression of polynomials.

(6.16) *For ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ in R, we have, in the polynomial ring $R[x]$, $(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n)R[x] = \mathfrak{a}_1 R[x] \cap \cdots \cap \mathfrak{a}_n R[x]$.*

As for $R(x)$, we have the following results:

(6.17) (1) *If $\mathfrak{a}$ is an ideal of R, then $R(x)/\mathfrak{a}R(x) = (R/\mathfrak{a})(x)$;* (2) *if $\mathfrak{q}$ is a primary ideal with prime divisor $\mathfrak{p}$, then $\mathfrak{p}R(x)$ is prime, $\mathfrak{q}R(x)$ is primary to $\mathfrak{p}R(x)$, $\mathfrak{q}R(x) \cap R = \mathfrak{q}$, $\mathfrak{p}R(x) \cap R = \mathfrak{p}$;* (3) *if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals in R, then $(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n)R(x) = \mathfrak{a}_1 R(x) \cap \cdots \cap \mathfrak{a}_n R(x)$;* (4) *an ideal $\mathfrak{m}'$ of $R(x)$ is a maximal ideal of $R(x)$, if and only if there exists a maximal ideal $\mathfrak{m}$ of R such that $\mathfrak{m}' = \mathfrak{m}R(x)$; and* (5) *$R < R(x)$.*

Proof: (1), (2), and (3) are obvious by the case of $R[x]$ ((6.16)). The *if* part of (4) is obvious. Let $\mathfrak{m}'$ be a maximal ideal of $R(x)$. The set $\mathfrak{m}$ of coefficients of elements of $\mathfrak{m}' \cap R[x]$ forms an ideal of R. $\mathfrak{m} \neq R$ by the construction of $R(x)$. Since $\mathfrak{m}' \subseteq \mathfrak{m}R(x)$ and since $\mathfrak{m}'$ is maximal, we see that $\mathfrak{m}' = \mathfrak{m}R(x)$ and that $\mathfrak{m}$ is a maximal ideal of R, which completes the proof of (4). (5) follows from (4).

We add here a remark on tensor product:

(6.18) *Let S be a multiplicatively closed subset of a ring R such that $0 \notin S$. Then $\otimes_R R_S$ is exact.*

Proof: Let M be an arbitrary R-module. In the set

$$P = \{(m, s) \mid m \in M, s \in S\}$$

we introduce an equivalence relation such that (m, s) is equivalent to (m', s') if and only if there is an $s'' \in S$ such that $s''sm' = s''s'm$. The set P' of equivalence classes of P becomes an R_S module by the operations $(m, s) + (m', s') \equiv (s'm + sm', ss')$, $\phi(a)/\phi(s)(m, s') \equiv (am, ss')$ (ϕ and $\equiv$ being the natural homomorphism from R into R_S and the equivalence relation respectively). Then, as in the proof of (6.2), we see that there is a natural homomorphism from P' onto $M \otimes R_S$, and by the universal mapping property of the tensor product, we see that P' is naturally isomorphic to $M \otimes R_S$. Thus we may identify P' with $M \otimes R_S$. If the same is applied to a submodule N of M, then we see that $N \otimes R_S \subseteq M \otimes R_S$, and the assertion is proved.

EXERCISES: *1.* With R and the x_i as in (6.14), prove that $R(x_1, \ldots, x_n) = R[x_1, \ldots, x_n]_S$ with the set S of polynomials whose coefficients generate R.

2. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a ring R and let S be a multiplicatively closed subset of R such that $0 \notin S$. Prove that

$$\mathfrak{a}_1 R_S \cap \cdots \cap \mathfrak{a}_n R_S = (\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) R_S .$$

7. Prime divisors

For a given ideal $\mathfrak{a}$ of a ring R, let U be the set of elements of R which are not zero divisors modulo $\mathfrak{a}$. Then U is multiplicatively closed and does not meet $\mathfrak{a}$. A prime ideal $\mathfrak{p}$ is called a *maximal prime divisor* of $\mathfrak{a}$ if $\mathfrak{p}$ is a maximal ideal with respect to U and if $\mathfrak{p}$ contains $\mathfrak{a}$. A prime ideal $\mathfrak{q}$ of R is called a *prime divisor* of $\mathfrak{a}$ if there is a multiplicatively closed subset S of R which does not meet $\mathfrak{a}$ such that $\mathfrak{q}R_S$ is a maximal prime divisor of $\mathfrak{a}R_S$.

(7.1) *A prime divisor $\mathfrak{q}$ of $\mathfrak{a}$ contains $\mathfrak{a}$, and all elements of $\mathfrak{q}$ are zero divisors modulo $\mathfrak{a}$.*

Proof: S being as above, $\mathfrak{q}R_S$ contains $\mathfrak{a}R_S$ by definition. (6.6) shows that $\mathfrak{q} = \mathfrak{q}R_S \cap R$, which proves that $\mathfrak{a} \subseteq \mathfrak{q}$. Applying (6.1) to $R/\mathfrak{a}$, we see that all elements of $\mathfrak{q}$ are zero divisors modulo $\mathfrak{a}$.

(7.2) *A prime ideal $\mathfrak{p}$ is a maximal prime divisor of $\mathfrak{a}$ if and only if $\mathfrak{p}$ is a maximal member of the set of prime divisors.*

Proof: By the definition, a maximal prime divisor is a prime di-

visor. Let $\mathfrak{q}$ be a prime divisor of $\mathfrak{a}$. Then $\mathfrak{q}$ consists of zero divisors modulo $\mathfrak{a}$ by (7.1), hence $\mathfrak{q}$ is contained in a maximal prime divisor of $\mathfrak{a}$, which proves the assertion.

(7.3) *Let $\mathfrak{p}$ be a minimal prime divisor of $\mathfrak{a}$. Then $\mathfrak{a}R_{\mathfrak{p}} \cap R$ is primary to $\mathfrak{p}$.*

This $\mathfrak{a}R_{\mathfrak{p}} \cap R$ is called the *primary component* of $\mathfrak{a}$ belonging to $\mathfrak{p}$.

Proof: Since $\mathfrak{p}$ is minimal among prime ideals containing $\mathfrak{a}$, the same is true for $\mathfrak{p}R_{\mathfrak{p}}$ and $\mathfrak{a}R_{\mathfrak{p}}$. Therefore $\mathfrak{a}R_{\mathfrak{p}}$ is primary to $\mathfrak{p}R_{\mathfrak{p}}$, which proves our assertion by (2.12).

As an immediate consequence, we have:

(7.4) *A prime ideal $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$ if and only if it is minimal among prime divisors of $\mathfrak{a}$.*

(7.5) *Assume that an ideal $\mathfrak{a}$ of R is the intersection of primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ and if the intersection $\bigcap \mathfrak{q}_i$ is irredundant, then the set of prime divisors of $\mathfrak{a}$ coincides with the set of the prime divisors $\mathfrak{p}_i$ of the $\mathfrak{q}_i$.*

Proof: (6.9) applied to $R_{\mathfrak{p}}$ with $\mathfrak{p} = \mathfrak{p}_i$ shows that each $\mathfrak{p}_i$ is a prime divisor of $\mathfrak{a}$. Conversely, assume that $\mathfrak{p}$ is a prime divisor of $\mathfrak{a}$. Then for a multiplicatively closed set S which does not meet $\mathfrak{a}$, $\mathfrak{p}R_S$ is a maximal prime divisor of $\mathfrak{a}R_S = \bigcap \mathfrak{q}_i R_S$. An element a of R_S is a zero divisor modulo $\mathfrak{a}R_S$ if and only if a is in some $\mathfrak{p}_i R_S$ such that $\mathfrak{p}_i R_S \neq R_S$. It follows from this and (2.7) that the maximal prime divisors of $\mathfrak{a}R_S$ are some of $\mathfrak{p}_i R_S$. Hence (6.6) shows that $\mathfrak{p} = \mathfrak{p}_i$ for some i, which completes the proof.

(7.6) *An ideal is primary if and only if it has only one prime divisor.*

Proof: The *only if* part is a consequence of (7.5). Conversely, assume that an ideal $\mathfrak{a}$ has only one prime divisor $\mathfrak{p}$. (7.4) shows that $\mathfrak{p}$ is the unique minimal prime divisor of $\mathfrak{a}$, hence $\mathfrak{p}$ is the radical of $\mathfrak{a}$. Assume that b is a zero divisor modulo $\mathfrak{a}$. Then $\mathfrak{a} + bR$ consists of zero divisors modulo $\mathfrak{a}$, hence there is a maximal prime divisor of $\mathfrak{a}$ containing b by (2.2). Hence $b \in \mathfrak{p}$ and b is nilpotent modulo $\mathfrak{a}$, which proves that $\mathfrak{a}$ is primary to $\mathfrak{p}$.

A prime divisor of $\mathfrak{a}$ which is not minimal is called an *imbedded prime divisor* of $\mathfrak{a}$.

For a prime ideal $\mathfrak{p}$, $\mathfrak{p}$ is the unique minimal prime divisor of $\mathfrak{p}^r$ (for any natural number r). Hence the primary component $\mathfrak{q}_r$ of $\mathfrak{p}^r$ belonging to $\mathfrak{p}$ is well defined. This $\mathfrak{q}_r$ is called the rth *symbolic power* of $\mathfrak{p}$ and is denoted by $\mathfrak{p}^{(r)}$.

(7.7) *If $R_{\mathfrak{p}}$ is a local ring which may not be Noetherian, then the in-*

tersection $\mathfrak{n}$ *of all the symbolic powers* $\mathfrak{p}^{(r)}$ *of* $\mathfrak{p}$ *is the set of elements* x *of* R *such that* $xs = 0$ *for some* s *of* R *which is not in* $\mathfrak{p}$. *Namely,* $\mathfrak{n}$ *is the kernel of the natural homomorphism from* R *into* $R_{\mathfrak{p}}$.

Proof: Since $R_{\mathfrak{p}}$ is a local ring which may not be Noetherian, the intersection of $\mathfrak{p}^r R_{\mathfrak{p}}$ is zero. Since $\mathfrak{p}^{(r)} = \mathfrak{p}^r R_{\mathfrak{p}} \cap R$, the assertion follows.

As a corollary, we have:

(7.8) *If* R *is a Noetherian integral domain, then the intersection of symbolic powers of a prime ideal is zero.*

8. Primary decomposition of ideals

We prove here a theorem on the primary decomposition of graded ideals in a graded Noetherian ring, which includes the usual decomposition theorem as a special case (because any ring is a graded ring with the trivial gradation, which will be defined below).

We say that a ring R is a *graded ring* if R is the direct sum of additive subgroups $R_0, R_1, \ldots, R_n, \ldots$ such that $R_i R_j \subseteq R_{i+j}$ (then it follows that $1 \in R_0$). An R-module M is called a *graded module* if M is the direct sum of R_0-submodules $M_0, \ldots, M_n, \ldots$ such that $R_i M_j \subseteq M_{i+j}$. Elements of R_n or M_n are called *homogeneous elements* of *degree* n.

When we say that $R = \sum R_n$ is a graded ring or that $M = \sum M_n$ is a graded module, we mean that R_n or M_n are as above.

A submodule N of a graded module $M = \sum M_n$ is called *graded* if $N = \sum (N \cap M_n)$. This definition can be applied to ideals.

A gradation is called *trivial* if all homogeneous elements of positive degrees are zero.

(8.1) *A submodule* N *of a graded module* $M = \sum M_n$ *over a graded ring* $R = \sum R_n$ *is a graded submodule if and only if* N *is generated by homogeneous elements.*

Proof: The *only if* part is obvious. Assume that N is generated by homogeneous elements $f_{ni} (f_{ni} \in M_n)$. $\sum f_n \in N (f_n \in M_n)$ implies that $\sum f_n = \sum f_{ij} (\sum_k g_{kij})$ for some $g_{kij} \in R_k$, hence

$$f_n = \sum_{j+k=n} f_{jt} g_{kjt}$$

which is in N.

(8.2) *If* N_i *are graded submodules of* M *and if* $\mathfrak{a}_i$ *are graded ideals of* R, *then* $\bigcap N_i$, $\bigcap \mathfrak{a}_i$, $\sum N_i$, $\sum \mathfrak{a}_i$, $\mathfrak{a}_1 : \mathfrak{a}_2$, $N_1 : N_2$, $N_1 : \mathfrak{a}_1$, $\mathfrak{a}_1 N_1$ *are all graded.*

The proof is straightforward and we omit it.

(8.3) THEOREM: *A graded ideal* $\mathfrak{q}$ $(\neq R)$ *of a graded ring* $R = \sum R_i$ *is a primary ideal with prime divisor* $\mathfrak{p}$ *if and only if the following conditions are satisfied:* $\mathfrak{p}$ *is the ideal generated by all the homogeneous elements which are nilpotent modulo* $\mathfrak{q}$ *and, for homogeneous elements* a *and* b, $ab \in \mathfrak{q}$, $a \notin \mathfrak{p}$ *imply* $b \in \mathfrak{q}$.

Proof: The *only if* part is trivial. We prove the *if* part. Since, by our assumption, every element of $\mathfrak{p}$ is nilpotent modulo $\mathfrak{q}$, it is sufficient to show that $(\sum_s^t a_i)(\sum_u^v b_j) \in \mathfrak{q}$, $\sum a_i \notin \mathfrak{p}$ imply $\sum b_j \in \mathfrak{q}$, where $a_i \in R_i$, $b_j \in R_j$. We prove it by double induction on $m = t - s$ and $n = v - u$. If $m = 0$, we have $\sum a_s b_j \in \mathfrak{q}$, $a_s \notin \mathfrak{p}$. Since $\mathfrak{q}$ is graded, we have $a_s b_j \in \mathfrak{q}$, hence $b_j \in \mathfrak{q}$ and $\sum b_j \in \mathfrak{q}$. The case where $n = 0$ is proved similarly. Now we consider the general case. Since $a_s b_u$ is the $(s + u)$th degree part of $(\sum a_i)(\sum b_j)$ and since $\mathfrak{q}$ is graded, we have $a_s b_u \in \mathfrak{q}$. We have $(\sum a_i)(\sum a_s b_j) \in \mathfrak{q}$. Since $a_s b_u \equiv 0$ modulo $\mathfrak{q}$, $\sum a_s b_j \equiv \sum_{u+1}^v a_s b_j$ mod. $\mathfrak{q}$. Hence by our second induction, applied to $(\sum_s^t a_i)(\sum_{u+1}^v a_s b_j) \in \mathfrak{q}$ (which has the same m and one less n), we have $\sum a_s b_j \in \mathfrak{q}$. If $a_s \notin \mathfrak{p}$, then we apply the case where $t - s = 0$ and we have $\sum b_j \in \mathfrak{q}$. If $a_s \in \mathfrak{p}$, then

$$\sum_{s+1}^t a_i \notin \mathfrak{p}$$

and $(\sum_{s+1}^t a_i)(\sum b_j) \in \mathfrak{q}$. Hence by our first induction, we have $\sum b_j \in \mathfrak{q}$. Thus the proof is complete.

(8.4) COROLLARY: *If* $\mathfrak{q}$ *is a graded primary ideal of a graded ring, then the prime divisor of* $\mathfrak{q}$ *is also graded.*

(8.5) *If a graded ideal* $\mathfrak{a}$ *of a graded ring* R *is not primary and if* R *is Noetherian, then there are graded ideals* $\mathfrak{b}$ *and* $\mathfrak{c}$ *such that* $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, $\mathfrak{a} \subset \mathfrak{b}$, *and such that* $\mathfrak{a} \subset \mathfrak{c}$.

Proof: There are homogeneous elements b and c such that $bc \in \mathfrak{a}$, $b \notin \mathfrak{a}$ and such that $c^n \notin \mathfrak{a}$ for any natural number n by virtue of (8.3). Set $\mathfrak{d}_i = \mathfrak{a}:c^iR$. Since R is Noetherian, there is an n such that $\mathfrak{d}_{n-1} = \mathfrak{d}_n$. Set $\mathfrak{b} = \mathfrak{a} + bR$ and $\mathfrak{c} = \mathfrak{a} + c^nR$; they are graded because b and c are homogeneous. It is obvious that $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{a} \subset \mathfrak{c}$. Therefore it is sufficient to show that $\mathfrak{b} \cap \mathfrak{c} \subseteq \mathfrak{a}$. Let x be an element of $\mathfrak{b} \cap \mathfrak{c}$. Then $x = a + by = a' + c^n z (a, a' \in \mathfrak{a}; y, z \in R)$. $cx = ac + bcy \in \mathfrak{a}$, hence $cx = a'c + c^{n+1}z \in \mathfrak{a}$, which implies that $c^{n+1}z \in \mathfrak{a}$ and

$$z \in \mathfrak{a}:c^{n+1} = \mathfrak{d}_{n+1} = \mathfrak{d}_n = \mathfrak{a}:c^n.$$

Therefore $c^n z \in \mathfrak{a}$ and $x = a' + c^n z$ is in $\mathfrak{a}$, which completes the proof.

(8.6) *A graded ideal of a graded Noetherian ring R is the intersection of a finite number of graded primary ideals.*

Proof: Assume the contrary and let F be the set of graded ideals of R which are not the intersections of any finite number of graded primary ideals. Since R is Noetherian, there is a maximal member $\mathfrak{a}$ of F. $\mathfrak{a} \in F$ implies that $\mathfrak{a}$ is not primary, hence there are graded ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{a} \subset \mathfrak{c}$ and such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ by (8.5). $\mathfrak{b}$ and $\mathfrak{c}$ are the intersections of graded primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ and $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ respectively by the maximality of $\mathfrak{a}$. Then $\mathfrak{a} = \bigcap \mathfrak{q}_i$, which is a contradiction. Thus F is empty and the proof is complete. Now we have:

(8.7) THEOREM: *If $\mathfrak{a}$ is a graded ideal of a graded Noetherian ring R, then* (1) *there are only a finite number of prime divisors, say $\mathfrak{p}_1, \ldots, \ldots, \mathfrak{p}_r$, of $\mathfrak{a}$,* (2) *the $\mathfrak{p}_i$ are necessarily graded,* (3) *there are graded primary ideals $\mathfrak{q}_i$ belonging to the $\mathfrak{p}_i$ such that $\mathfrak{a} = \bigcap \mathfrak{q}_i$ and* (4) *if $\mathfrak{p}_j$ is a minimal prime divisor of $\mathfrak{a}$, then the $\mathfrak{q}_j$ in* (3) *is necessarily the primary component of $\mathfrak{a}$ belonging to $\mathfrak{p}_j$. Furthermore* (5) *$\mathfrak{a}$ cannot be the intersection of primary ideals of number less than r.*

The primary decomposition given in this theorem is called a *shortest primary decomposition* of $\mathfrak{a}$.

Proof: (1), (2) and (5) follow from (8.6), (7.5) and (8.4). (3) follows from (8.6) and (2.11). (4) follows from (6.6) and (6.9).

(8.8) COROLLARY: *A prime ideal $\mathfrak{p}$ of a Noetherian graded ring R is a prime divisor of a graded ideal $\mathfrak{a}$ of R if and only if there is a homogeneous element a of R such that $\mathfrak{a}:aR = \mathfrak{p}$.*

Proof: Let $\mathfrak{q}_i$ be as in (8.7) for $\mathfrak{a}$. Since $\mathfrak{a}:a = \bigcap(\mathfrak{q}_i:a)$, we prove the *if* part easily by virtue of (2.13). If $\mathfrak{p} = \mathfrak{p}_i$ for some i, say 1, then let b be a homogeneous element of $\mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r$ which is not in $\mathfrak{a}$. Then $\mathfrak{a}:b = \mathfrak{q}_1:b$, which is primary to $\mathfrak{p}$ by (2.13). Let c be a homogeneous element in $(\mathfrak{q}_1:b):\mathfrak{p}$ which is not in $\mathfrak{q}_1:b$. Then $(\mathfrak{q}_1:b):c$ contains $\mathfrak{p}$. Hence $(\mathfrak{q}_1:b):c = \mathfrak{p}$ by (2.13). Thus, with $a = bc$, we have $\mathfrak{a}:a = \mathfrak{p}$ by (1.2).

(8.9) THEOREM: *Two graded ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a graded ring R coincide with each other if and only if $\mathfrak{a}R_\mathfrak{m} = \mathfrak{b}R_\mathfrak{m}$ for every graded maximal ideal $\mathfrak{m}$ of R.*

Proof: The *only if* part is obvious. Assume the validity of $\mathfrak{a}R_\mathfrak{m} = \mathfrak{b}R_\mathfrak{m}$. Set $\mathfrak{c} = \mathfrak{a}:\mathfrak{b}$. $\mathfrak{c}R_\mathfrak{m} = \mathfrak{a}R_\mathfrak{m}:\mathfrak{b}R_\mathfrak{m} = R_\mathfrak{m}$, hence $\mathfrak{c}$ is not contained

in any graded maximal ideal of R. Since $\mathfrak{c}$ is graded by (8.2), we have $\mathfrak{c} = R$, and $\mathfrak{b} \subseteq \mathfrak{a}$. Similarly $\mathfrak{a} \subseteq \mathfrak{b}$, and $\mathfrak{a} = \mathfrak{b}$.

(8.9) can be generalized to the case of graded modules by the principle of idealization, hence in particular we have:

(8.10) COROLLARY: *Let M be a module over a ring R. If $M \otimes R_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of R, then $M = 0$.*

EXERCISES: *1*. Generalize the above (8.7) to Noetherian graded modules in the following way:

Let M be a module over a ring R. A submodule $P \neq M$ of M is called *primary* if any zero divisor with respect to M/P is nilpotent with respect to M/P. In this case $0:(M/P)$ $(= P:M)$ is a primary ideal. (Prove it.) The prime divisor of $0:(M/P)$ is called the *associated prime ideal* of P. If a submodule N of M is an irredundant intersection of primary submodules $P_1, \ldots, P_n$ then the associated prime ideals of the P_i are called *associated prime ideals* of N.

Assume that $M = \sum M_n$ is a graded module over a graded ring $R = \sum R_n$.

(a) Prove that the ring $R \oplus M$ given in the principle of idealization is a graded ring with the structure $\sum (R_n \oplus M_n)$ and a submodule N of M is graded if and only if it is a graded ideal of the ring $R \oplus M$.

(b) Prove that a submodule N of M is a primary submodule with associated prime ideal $\mathfrak{p}$ if $M \neq N$ and if there is a primary ideal $\mathfrak{q}^*$ of $R \oplus M$ with prime divisor $\mathfrak{p} \oplus M$ such that $N = \mathfrak{q}^* \cap M$.

(c) Then apply (8.7).

2. Prove the converse of (b) above in the following form:

If N is a primary submodule of M with associated prime ideal $\mathfrak{p}$, then with the primary ideal $\mathfrak{q} = N:M$, $\mathfrak{q}^* = \mathfrak{q} \oplus N$ is a primary ideal belonging to $\mathfrak{p} \oplus M$, and, with this $\mathfrak{q}^*$, $N = \mathfrak{q}^* \cap M$.

3. Show that an irredundant primary decomposition (or the associated prime ideals) of the submodule N of M does not necessarily correspond to an irredundant primary decomposition (or the prime divisors) of the ideal $(N:M)$. (Hint: Let $\mathfrak{q}_1$, $\mathfrak{q}_2$ be primary ideals of R, set $M = R/\mathfrak{q}_1 \oplus R/\mathfrak{q}_2$, and consider the decomposition of (0) in M.)

9. *The notions of height and altitude*

We say that a ring R is of *altitude* r if there is a chain of prime ideals $\mathfrak{p}_i$ such that $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r$ but there is no such chain with more terms. If there is no such r, we say that R is of infinite altitude.

For a prime ideal $\mathfrak{p}$ of R, the altitude of $R_{\mathfrak{p}}$ is called the *height* of $\mathfrak{p}$. Namely, height $\mathfrak{p}$ is the maximum of lengths of descending chains of prime ideals which begin with $\mathfrak{p}$ (length of a chain is defined to be one less than the number of terms of the chain).

For an ideal $\mathfrak{a}$ of R, the minimum of heights of minimal prime divisors of $\mathfrak{a}$ is called the *height* of $\mathfrak{a}$; the maximum (or *supremum*) of

these heights is called the *altitude* of $\mathfrak{a}$. altitude $R/\mathfrak{a}$ is called the *depth* of $\mathfrak{a}$.

We shall prove a fundamental theorem of Krull on altitudes of ideals in a Noetherian ring ((9.3), below).

In order to prove it, we need the *if* part of the following theorem on rings with minimum condition:

(9.1) THEOREM: *A ring R satisfies the minimum condition for ideals if and only if* (a) *R is Noetherian and* (b) altitude $R = 0$ (*namely, every prime ideal is maximal*). (THEOREM OF AKIZUKI)

Proof: Assume first that R satisfies the conditions (a) and (b). It follows that any maximal ideal is a minimal prime divisor of the zero ideal, hence we see by (8.7) that there are only a finite number of maximal ideals, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, and that the intersection $\mathfrak{m}$ of the $\mathfrak{p}_i$ is the radical of 0. Hence (3.15) shows that $\mathfrak{m}$ is nilpotent. Let r be such that $\mathfrak{m}^r = 0$. Then $R = R/\mathfrak{m}^r$, which implies by virtue of (1.4) that R is the direct sum of $R/\mathfrak{p}_i^r$. Each $\mathfrak{p}_i^{j-1}/\mathfrak{p}_i^j$ for $j = 1, \ldots, r$ is a finite module over the field $R/\mathfrak{p}_i$, hence it has a composition series. Therefore $R/\mathfrak{p}_i^r$, and hence also R, have composition series. Thus R satisfies the minimum condition. Conversely, assume that R satisfies the minimum condition. Let $\mathfrak{p}$ be an arbitrary prime ideal of R. $R/\mathfrak{p}$ satisfies the minimum condition because R does. If $R/\mathfrak{p}$ has a non-unit $x \neq 0$, then $\{x^n(R/\mathfrak{p})\}$ has no minimal member because $R/\mathfrak{p}$ is an integral domain. Thus $R/\mathfrak{p}$ must be a field, which proves that $\mathfrak{p}$ is maximal. Thus altitude $R = 0$. We see also that R has only a finite number of prime ideals; for if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{p}_{n+1}, \ldots$ were different maximal ideals, then we should have a descending chain $\mathfrak{p}_1 \supset (\mathfrak{p}_1 \cap \mathfrak{p}_2) \supset \cdots \supset (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n) \supset (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n+1}) \supset \cdots$. Let the maximal ideals be $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, and let $\mathfrak{m}$ be the intersection of them. Among the powers of $\mathfrak{m}$, there is a minimal member; let it be $\mathfrak{n} = \mathfrak{m}^r$. Assume for a moment that $\mathfrak{n} \neq 0$. We have $\mathfrak{n}^2 = \mathfrak{n} \neq 0$. Let $\mathfrak{b}$ be a minimal ideal among those which are contained in $\mathfrak{n}$ and whose product with $\mathfrak{n}$ is different from 0 and set $\mathfrak{p} = 0 : \mathfrak{b}\mathfrak{n}$. Since $\mathfrak{b}\mathfrak{n} \neq 0$, we have $\mathfrak{p} \neq R$. $cd \in \mathfrak{p}$, $c \notin \mathfrak{p}$ imply $cd\mathfrak{b}\mathfrak{n} = 0$ and $c\mathfrak{b}\mathfrak{n} \neq 0$, hence $c\mathfrak{b} = \mathfrak{b}$ by the minimality of $\mathfrak{b}$ and therefore $d\mathfrak{b}\mathfrak{n} = 0$, which implies that $d \in \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal and therefore $\mathfrak{n} \subseteq \mathfrak{p}$, which implies that $\mathfrak{b}\mathfrak{n} = \mathfrak{b}\mathfrak{n}^2 \subseteq \mathfrak{b}\mathfrak{n}\mathfrak{p} = 0$, which is a contradiction. Thus $\mathfrak{n} = 0$, i.e., $\mathfrak{m}^r = 0$. Therefore (1.4) shows that R is the direct sum of $R/\mathfrak{p}_i^r$, each of which satisfies the minimum condition. Hence each $\mathfrak{p}_i^{j-1}/\mathfrak{p}_i^j$ satisfies the minimum condition as an $R/\mathfrak{p}_i^j$ module, hence over the field $R/\mathfrak{p}_i$. Therefore

$\mathfrak{p}_i^{i-1}/\mathfrak{p}_i^i$ has a composition series, and therefore $R/\mathfrak{p}_i^r$, and R, too, have composition series. Hence R satisfies the maximum condition, too.

We prove next the following lemma of Krull:

(9.2) *Let a be a non-unit of a Noetherian integral domain R such that $a \neq 0$. If $\mathfrak{p}$ is a minimal prime divisor of aR, then* height $\mathfrak{p} = 1$.

Proof: Considering $R_{\mathfrak{p}}$, we may assume that $\mathfrak{p}$ is the unique maximal ideal of R. Let $\mathfrak{q}$ be a prime ideal of R such that $\mathfrak{q} \subset \mathfrak{p}$. Set $\mathfrak{a}_i = \mathfrak{q}^{(i)} + aR$. Since R/aR satisfies the minimum condition by (9.1), we see that there is an n such that $\mathfrak{a}_i = \mathfrak{a}_n$ for any $i \geq n$. Then we have $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(i)} + aR$. By the minimality of $\mathfrak{p}$, a is not in $\mathfrak{q}$. Therefore $\mathfrak{q}^{(n)}:aR = \mathfrak{q}^{(n)}$. Hence (4.3) implies that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(i)}$. Thus $\bigcap_i \mathfrak{q}^{(i)} = \mathfrak{q}^{(n)}$. On the other hand, (7.8) implies that $\bigcap_i \mathfrak{q}^{(i)} = 0$, hence we have $\mathfrak{q}^{(n)} = 0$, and $\mathfrak{q} = 0$. Thus height $\mathfrak{p} = 1$.

Now we come to an important theorem of Krull:

(9.3) THEOREM: *If an ideal $\mathfrak{a}$ of a Noetherian ring R is generated by r elements, then, for any minimal prime divisor $\mathfrak{p}$ of $\mathfrak{a}$,* height $\mathfrak{p}$ *is not greater than r, i.e.,* altitude $\mathfrak{a} \leq r$. (ALTITUDE THEOREM OF KRULL)

Proof: Let $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_s$ be a chain of prime ideals $\mathfrak{p}_i$. It is sufficient to show that $s \leq r$. If there are prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, then adding a maximal member of prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, we may assume that there is no such prime ideal. Considering $R_{\mathfrak{p}}$ instead of R, we may assume that $\mathfrak{p}$ is the unique maximal ideal of R. Let $a_1, \ldots, a_r$ be a basis for $\mathfrak{a}$; we may assume that $a_1 \notin \mathfrak{p}_1$ (for, $\mathfrak{a} \nsubseteq \mathfrak{p}_1$). Then there is no prime ideal except $\mathfrak{p}$ which contains $\mathfrak{p}_1 + a_1R$, which shows that $\mathfrak{p}_1 + a_1R$ is primary to $\mathfrak{p}$. Therefore there is a natural number t such that $a_i^t \in \mathfrak{p}_1 + a_1R$ (for all i). We write $a_i^t = a_1b_i + c_i$ with $b_i \in R$ and $c_i \in \mathfrak{p}_1$. Set $\mathfrak{a}' = \sum_2^r c_iR$. Let $\mathfrak{p}'$ be a minimal prime divisor of $\mathfrak{a}'$ contained in $\mathfrak{p}_1$. Since the radical of $\mathfrak{a}' + a_1R$ contains the a_i, $\mathfrak{a}' + a_1R$ is primary to $\mathfrak{p}$, hence $\mathfrak{p}' + a_1R$ is primary to $\mathfrak{p}$, which means that, in the ring $R/\mathfrak{p}'$, $\mathfrak{p}/\mathfrak{p}'$ is a minimal prime divisor of a principal ideal, which shows that height $\mathfrak{p}/\mathfrak{p}' = 1$ by (9.2). Since $\mathfrak{p}' \subseteq \mathfrak{p}_1$, we have $\mathfrak{p}' = \mathfrak{p}_1$. Since $\mathfrak{a}'$ is generated by $r - 1$ elements, we have height $\mathfrak{p}' \leq r - 1$, hence $s \leq r$. Thus the theorem is proved.

(9.4) COROLLARY: *The altitude of an ideal of a Noetherian ring is finite.*

(9.5) THEOREM: *If $\mathfrak{a}$ is an ideal of a Noetherian ring R and if*

height $\mathfrak{a} = r$, *then there are elements* $a_1, \ldots, a_r$ *of* $\mathfrak{a}$ *such that* $\sum_1^s a_i R$ *is of height* s *for any* $s \leq r$.

Proof: We construct a_i inductively. Assume that there are elements $a_1, \ldots, a_{s-1}$ of $\mathfrak{a}$ such that height $(\sum_1^t a_i R) = t$ for any $t \leq s - 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be all of the prime divisors of $\sum_1^{s-1} a_i R$ $(= 0$ if $s = 1)$ such that heights of them are $s - 1$. If $s - 1 < r$, then $\mathfrak{a}$ is not contained in any of the $\mathfrak{p}_i$, whence there is an element a_s of $\mathfrak{a}$ which is not contained in any of the $\mathfrak{p}_i$ by (2.7). Then height $\sum_1^s a_i R$ is at least s, whence it is s by (9.3).

As a consequence of (9.5), we see that:

(9.6) *If* $(R, \mathfrak{m})$ *is a local ring of altitude* r, *then there are* r *elements* $a_1, \ldots, a_r$ *of* $\mathfrak{m}$ *which generate a primary ideal belonging to* $\mathfrak{m}$ *but there is no primary ideal belonging to* $\mathfrak{m}$ *which is generated by* $r - 1$ *elements.*

The set of such elements a_i as above is called a *system of parameters* of R.

A system of parameters $x_1, \ldots, x_r$ of a local ring R is called a *regular system of parameters* if it generates the maximal ideal of R. A local ring which has regular system of parameters is called a *regular local ring.*

The following are consequences of (9.6).

(9.7) *Let* $(R, \mathfrak{m})$ *be a local ring. For a given element* x *of* $\mathfrak{m}$, *there is a system of parameters of* R *containing* x *if and only if* altitude R/xR = altitude $R - 1$; *each of the following conditions is sufficient*: (a) altitude $R/xR <$ altitude R, (b) *there is no prime ideal of altitude* 0 *which contains* x, (c) *there is no prime ideal of depth equal to* altitude R *which contains* x.

Proof: Let $x_1, \ldots, x_s$ be elements of $\mathfrak{m}$. Then their residue classes modulo xR generate a primary ideal belonging to $\mathfrak{m}/xR$ if and only if $x, x_1, \ldots, x_s$ generate a primary ideal belonging to $\mathfrak{m}$. From this fact, the assertion follows immediately.

The same idea proves:

(9.8) *With the same* $(R, \mathfrak{m})$ *as above, if* $x_1, \ldots, x_s$ *are elements of* $\mathfrak{m}$ *such that* height $\sum x_i R = s$, *then*

$$\text{altitude } R/\sum x_i R = \text{altitude } R - s.$$

(9.9) *If* $(R, \mathfrak{m})$ *is a local ring, then* $\text{length}_{R/\mathfrak{m}}\, \mathfrak{m}/\mathfrak{m}^2 \geq$ altitude R; *the equality holds if and only if* R *is regular.*

The proof is straightforward by virtue of (5.1).

(9.10) *If* R *is a Noetherian ring and if* $x_1, \ldots, x_n$ *are indeter-*

minates, then altitude $R[x_1, \ldots, x_n] = n +$ altitude R, *and* altitude $R(x_1, \ldots, x_n) =$ altitude R.

Proof: It is sufficient to consider the case where $n = 1$. We see that altitude $R[x_1] \geq$ altitude $R + 1$ by (6.15). Let $\mathfrak{m}'$ be a maximal ideal of $R[x_1]$ and set $\mathfrak{m} = \mathfrak{m}' \cap R$. It is sufficient to show that height $\mathfrak{m}' \leq$ height $\mathfrak{m} + 1$. In order to prove it, we may assume that $R = R_{\mathfrak{m}}$. $R[x_1]/\mathfrak{m}R[x_1] = (R/\mathfrak{m})[x_1]$, which is a principal ideal ring, whence there is an element f of $\mathfrak{m}'$ such that $\mathfrak{m}'$ is generated by $\mathfrak{m}$ and f. Let $y_1, \ldots, y_r$ be a system of parameters of R. Then we see that the y_i and f generate a primary ideal to $\mathfrak{m}'$, whence height $\mathfrak{m}' \leq$ height $\mathfrak{m} + 1$, and the first assertion is proved. Considering the case where $\mathfrak{m}' = \mathfrak{m}R[x] + xR[x]$, we see that height $\mathfrak{m} =$ height $\mathfrak{m}R[x]$, which proves the second assertion.

We make a remark, which is obvious from the definition of regularity.

(9.11) *Let R be a local ring. If there are r elements $a_1, \ldots, a_r$ of R such that* height $\sum a_iR = r$ *and such that $R/\sum a_iR$ is regular, then R is regular.*

We note that (9.10) is not true in general if we do not assume that R is Noetherian. (cf. Seidenberg [1])

We note that though (9.4) implies that the altitude of a semi-local ring is finite, it is not true in general that altitudes of Noetherian rings are finite; see Example 1 in the Appendix.

Let M be a module over a ring R. Then altitude $R/(0:M)$ is called the *operator altitude* of M and is denoted by op. alt M. M is called a *faithful* R-module if $0:M = 0$.

Note that the structure of M as an R-module is substantially the same as the structure of M as an $R/(0:M)$-module.

10. Integral dependence

Let R be a subring of a ring R'. An element a of R' is said to be *integral* over R if there are elements $c_1, \ldots, c_n$ of R such that $a^n + c_1a^{n-1} + \cdots + c_n = 0$, i.e., a is a root of a monic polynomial over R. We say that R' is *integral* over R if every element of R' is integral over R.

(10.1) *An element $a \in R'$ is integral over R if and only if there is a subring R'' of R' such that R'' is a finite R-module and such that $a \in R''$.*

Proof: If a is integral over R, then $R[a]$ is a finite R-module. Conversely, assume the existence of $R'' = \sum_1^n Ru_i$. $au_i = \sum_j a_{ij}u_j$

with $a_{ij} \in R$, hence, denoting by d the determinant $|\delta_{ij}a - a_{ij}|$ (δ_{ij} being Kronecker δ), we have $du_i = 0$, hence $dR'' = 0$ and $d = 0$. Since d is expressed as a monic polynomial in a with coefficients in R, we see that a is integral over R.

(10.2) COROLLARY: *The set R'' of elements of R' which are integral over R forms a ring.*

Proof: If $a, b \in R''$, then $R[a, b]$ is finite over R, hence every element of $R[a, b]$ is integral over R.

The ring R'' given above (10.2) is called the *integral closure* of R in R'. If $R'' = R$, we say that R is *integrally closed* in R'. A ring is said to be *integrally closed* if it is integrally closed in its total quotient ring.

(10.3) COROLLARY. *If $a \in R'$ is integral over a subring R^* and if R^* is integral over R, then a is integral over R. Consequently the integral closure R'' of R in R' is integrally closed in R'.*

Proof: Assume that $a \in R'$ is integral over R^*: $a^n + c_1a^{n-1} + \cdots + c_n = 0$ with $c_i \in R^*$. Then $R[c_1, \ldots, c_n, a]$ is finite over R, whence a is integral over R.

When R is a subring of a ring R', R' is an R-module. $R:R'$ is called the *conductor* of R in R'.

(10.4) *Assume that R is a Noetherian ring and that b is an element of a ring containing R'.* (1) *The conductor of R in $R[b]$ contains elements a and ideals $\mathfrak{a}$ of R such that $ab^n \in R$ for any natural number n; $\mathfrak{a}b \subseteq \mathfrak{a}$.* (2) *If the conductor of R in R' contains an element a which is not a zero divisor in R', then R' is a finite R-module, is integral over R and is contained in the total quotient ring of R.*

Proof: (1) is obvious, while (2) follows immediately from the fact that R is Noetherian and that $R' \subseteq Ra^{-1}$.

(10.5) *Let a be a non-zero-divisor of a ring R. If a^{-1} is integral over R, then $a^{-1} \in R$. Consequently, if a field is integral over an integral domain I, then I is a field.*

Proof: There are elements $c_1, \ldots, c_n$ of R such that $(a^{-1})^n + c_1(a^{-1})^{n-1} + \cdots + c_n = 0$, hence $a^{-1} = -(c_1 + c_2a + \cdots + c_na^{n-1})$, which is in R.

On the other hand, the definition of integral dependence implies immediately the following lemma:

(10.6) *If a ring R' is integral over its subring R, then* (1) *for any homomorphism ϕ defined on R', $\phi(R')$ is integral over $\phi(R)$ and* (2)

for any multiplicatively closed subset S of R which does not contain zero, R'_S is integral over R_S.

Now we have the following important result.

(10.7) THEOREM: *Assume that a ring R' is integral over its subring R. Let $\mathfrak{p}$ be a prime ideal of R and let S be the complement of $\mathfrak{p}$ in R. Then a prime ideal $\mathfrak{p}'$ of R' lies over $\mathfrak{p}$ if and only if $\mathfrak{p}'$ is maximal with respect to S.*

Proof: Assume at first that a prime ideal $\mathfrak{p}'$ of R' lies over $\mathfrak{p}$. Then $\mathfrak{p}'$ does not meet S, therefore $\mathfrak{p}'R'_S$ is different from R'_S. Hence $\mathfrak{p}R_S \subseteq \mathfrak{p}'R'_S \cap R_S \subset R_S$, which proves that $\mathfrak{p}'R'_S \cap R_S = \mathfrak{p}R_S$. Hence $R'_S/\mathfrak{p}'R'_S$ is integral over the field $R_S/\mathfrak{p}R_S$, which shows that $R'_S/\mathfrak{p}'R_S$ is a field, hence $\mathfrak{p}'R_S$ is maximal, which means that $\mathfrak{p}'$ is maximal with respect to S. Conversely, assume that $\mathfrak{p}'$ is maximal with respect to S. Then $\mathfrak{p}'R'_S$ is a maximal ideal and the field $R'_S/\mathfrak{p}'R_S$ is integral over $R_S/(\mathfrak{p}'R'_S \cap R_S)$. (10.5) implies that this last integral domain is a field, which means that $\mathfrak{p}'R'_S \cap R_S = \mathfrak{p}R_S$, which implies that $\mathfrak{p}' \cap R = \mathfrak{p}$.

(10.8) COROLLARY: *With the same R, R', and $\mathfrak{p}$ as above, there are prime ideals of R' which lie over $\mathfrak{p}$; there is no inclusion relation between any of these prime ideals of R'.* (LYING-OVER THEOREM)

(10.9) COROLLARY: *With the same R, R' as above, if $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r$ is an ascending chain of prime ideals in R and if a prime ideal $\mathfrak{p}'_0$ of R' lying over $\mathfrak{p}_0$ is given, then there is an ascending chain of prime ideals $\mathfrak{p}'_i$ which begins with $\mathfrak{p}'_0$ such that $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$ for each i. If, in this case, there is no prime ideal between $\mathfrak{p}_i$ and $\mathfrak{p}_{i+1}$, then there is no prime ideal between $\mathfrak{p}'_i$ and $\mathfrak{p}_{i+1}$.* (GOING-UP THEOREM).

Proof: The existence is easy by induction on n, while the last assertion follows from (10.8) (the lying-over theorem).

(10.10) COROLLARY: *If a ring R' is integral over a ring R, then* altitude R' = altitude R.

This follows from (10.9).

Another immediate consequence of (10.8) is:

(10.11) COROLLARY: *If a ring R' is integral over a ring R and if $\mathfrak{a}$ is an ideal of R different from R, then $\mathfrak{a}R' \neq 1$.*

Let R be an integral domain. A ring R' containing R is called an *integral extension* of R if R' is an integral domain and if R' is integral over R. If the field of quotients of R' is finite over that of R, we say that R' is *almost finite* over R.

An integrally closed integral domain is called a *normal ring*. The integral closure of an integral domain R in its field of quotients is called the *derived normal* ring of R.

When R is a normal ring, an integral extension R' of R is called a *Galois extension* of R if R' is the integral closure of R in a Galois extension (not necessarily separable) of the field of quotients of R, in the sense of Galois theory: the Galois group of the field extension is called the *Galois group* of the integral extension.

(10.12) THEOREM: *Let R be a normal ring and let R' be a Galois extension of R. Then for any prime ideal $\mathfrak{p}$ of R, the prime ideals of R' which lie over $\mathfrak{p}$ are conjugate to each other; that is, if prime ideals $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ lie over $\mathfrak{p}$, then there exists an automorphism σ of R' over R such that $\mathfrak{p}_1'^{\sigma} = \mathfrak{p}_2'$.*

Proof: We consider at first the case where R' is almost finite over R. Assuming the contrary, let $\mathfrak{p}_2', \ldots, \mathfrak{p}_n'$ be all of the prime ideals of R' which are conjugate to $\mathfrak{p}_2'$. Since there is no inclusion relation among the $\mathfrak{p}_i'$ by the lying-over theorem ((10.8)), there is an element a of $\mathfrak{p}_1'$ which is not in any of the $\mathfrak{p}_2', \ldots, \mathfrak{p}_n'$. Then no conjugate of a is in any of the $\mathfrak{p}_2', \ldots, \mathfrak{p}_n'$, whence the norm a^* of a with respect to R is not in $\mathfrak{p} = \mathfrak{p}_2' \cap R$. This is a contradiction because $a \in \mathfrak{p}_1'$ implies that $a^* \in \mathfrak{p}_1' \cap R = \mathfrak{p}$. Thus we have proved this case. Let us turn to the general case. Consider the set F of pairs (S, σ) of Galois extensions S of R contained in R' and an automorphism σ of S over R such that $(\mathfrak{p}_1' \cap S)^{\sigma} = \mathfrak{p}_2' \cap S$, for all possible S and σ. Then we introduce an order in F as follows: $(S, \sigma) \leq (S', \sigma')$ if and only if $S \subseteq S'$ and the restriction of σ' to S coincides with σ. With this order, we see that F is an inductive set, hence there is a maximal member, say (S^*, σ^*) of F. It is sufficient to show that $S^* = R'$. Let S'' be a Galois extension of R such that $S^* \subseteq S'' \subseteq R'$ and such that S'' is almost finite over S^*. There is an automorphism of S'' over R such that its restriction to S^* is σ^*; we denote such an automorphism by the same letter σ^*. Then $(\mathfrak{p}_1' \cap S'')^{\sigma^*}$ and $(\mathfrak{p}_2' \cap S'')$ lie over the same prime ideal $(\mathfrak{p}_2' \cap S^*)$, hence there is an automorphism σ'' of S'' over S^* such that $(\mathfrak{p}_1' \cap S'')^{\sigma^*\sigma''} = \mathfrak{p}_2' \cap S''$. By the maximality of S^*, we have $S'' = S^*$, which implies that $S^* = R'$, and the proof is complete.

(10.13) THEOREM: *Let R be a normal ring and let R' be a ring such that* (1) $R \subseteq R'$, (2) *R' is integral over R and* (3) *no non-zero ele-*

ment of R is a zero divisor in R'. If a prime ideal $\mathfrak{p}_1'$ of R' and a descending chain $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_r$ of prime ideals in R are given such that $\mathfrak{p}_1 = \mathfrak{p}_1' \cap R$, then there is a descending chain of prime ideals $\mathfrak{p}_i'$ in R' which begins with $\mathfrak{p}_1'$ and such that $\mathfrak{p}_i' \cap R = \mathfrak{p}_i$; here if $\mathfrak{p}_r = 0$ and if a prime ideal $\mathfrak{p}'$ of R' which lies over 0 and such that $\mathfrak{p}' \subseteq \mathfrak{p}_1'$ is pre-assigned, then there is such a chain with $\mathfrak{p}_r' = \mathfrak{p}'$. (GOING-DOWN THEOREM)

Proof: Since $\mathfrak{p}_1'$ contains zero, $\mathfrak{p}_1'$ contains a minimal prime divisor $\mathfrak{q}'$ of zero by (2.5). Since non-zero elements of R are not zero divisors in R', $\mathfrak{q}'$ lies over zero by (7.1). Thus it is sufficient to prove the last assertion. $R'/\mathfrak{p}'$ is an integral extension of R; if we see the existence of such a chain in $R'/\mathfrak{p}'$, then, considering the inverse image of the chain, we prove the assertion. Thus we may assume that R' is an integral extension of R. Let R'' be a Galois extension of R containing R' and let $\mathfrak{p}_1''$ be a prime ideal of R'' which lies over $\mathfrak{p}_1'$. Let $\mathfrak{q}_i'' \subset \cdots \subset \mathfrak{q}_1''$ be a chain of prime ideals in R'' such that $\mathfrak{q}_r'' \cap R = \mathfrak{p}_i$ by the going-up theorem ((10.9)). Since $\mathfrak{p}_1''$ and $\mathfrak{q}_1''$ lie over the same prime ideal $\mathfrak{p}_1$ of R, there is an automorphism σ of R'' over R such that $\mathfrak{q}_1''^{\sigma} = \mathfrak{p}_1''$. Then, obviously the chain of $(\mathfrak{q}_i''^{\sigma} \cap R')$ is the required one.

(10.14) THEOREM: *With the same R and R' as in* (10.13), *let $\mathfrak{a}'$ be an ideal of R' and set $\mathfrak{a} = \mathfrak{a}' \cap R$. Then* height $\mathfrak{a}$ = height $\mathfrak{a}'$.

Proof: We first consider the case where $\mathfrak{a}'$ is a prime ideal. For a chain $\mathfrak{a}' = \mathfrak{p}_0' \supset \mathfrak{p}_1' \supset \cdots \supset \mathfrak{p}_s'$ of prime ideals in R', we have a chain $\mathfrak{a} = \mathfrak{p}_0' \cap R \supset \mathfrak{p}_1' \cap R \supset \cdots \supset \mathfrak{p}_s' \cap R$ by the lying-over theorem (10.8)), whence height $\mathfrak{a}' \leq$ height $\mathfrak{a}$; similarly the converse inequality follows from (10.13), and height $\mathfrak{a}'$ = height $\mathfrak{a}$ in this case. Now we consider the general case. Let $\mathfrak{p}'$ be a prime divisor of $\mathfrak{a}'$ such that height $\mathfrak{a}'$ = height $\mathfrak{p}'$. Since $\mathfrak{p}' \cap R$ contains $\mathfrak{a}$, we have height $\mathfrak{a} \leq$ height $\mathfrak{p}' \cap R$ = height $\mathfrak{p}'$ = height $\mathfrak{a}'$. Conversely, let $\mathfrak{p}$ be a prime divisor of $\mathfrak{a}$ such that height $\mathfrak{a}$ = height $\mathfrak{p}$. Let $\mathfrak{p}'$ be a prime ideal of R' such that $\mathfrak{a}' \subseteq \mathfrak{p}'$ and such that $\mathfrak{p}' \cap R = \mathfrak{p}$; the existence follows from the lying-over theorem applied to $R'/\mathfrak{a}'$ and $R/\mathfrak{a}$ with the prime ideal $\mathfrak{p}/\mathfrak{a}$. Then we have height $\mathfrak{a}' \leq$ height $\mathfrak{p}'$ = height $\mathfrak{p}' \cap R$ = height $\mathfrak{a}$. Thus height $\mathfrak{a}'$ = height $\mathfrak{a}$.

(10.15) THEOREM: *Let R be a normal ring and let $f(x)$ be a monic polynomial in an indeterminate x with coefficients in R. Set $R' = R[x]/f \cdot R[x]$ and let d be the discriminant of $f(x)$. If R^* is the integral closure of R' in its total quotient ring Q, then dR^* is contained in R'.*

Proof: If $d = 0$, the assertion is obvious, and we assume that $d \neq 0$. Let a be the residue class of x in R'. Let K be the field of quotients of R and let L be a field containing all roots of $f(x)$. We note first that any element $a \neq 0$ of R is not a zero divisor in R', whence K is contained in Q and $Q = K[a]$. For each root a_i of $f(x)$, there exists an R-homomorphism ϕ_i from R^* into L such that $\phi_i(a) = a_i$. Now let b be an arbitrary element of R^*. Then $b = \sum_0^{n-1} u_j a^j$ ($u_i \in K$, $n =$ degree of $f(x)$). Then $\phi_i(b) = \sum u_j a_i^j$ and we regard that these equalities as linear equations in the unknown u_j. The determinant D of the coefficients is $\prod_{i<j}(a_i - a_j)$, hence $D^2 = d$. Since $\phi_i(b)$ and a_i are integral over R, the du_i are integral over R. Since du_i are in K and since R is a normal ring, we see that du_i are in R, hence db is in R', whence dR^* is contained in R'.

(10.16) COROLLARY: *If R' is an almost finite separable integral extension of a Noetherian normal ring R, then R' is a finite R-module.*

Proof: Since R' is separable, there is an element a of R' such that R' and $R[a]$ have same field of quotients. Let f be the irreducible monic polynomial over R which has a as a root and let d be the discriminant of $f(x)$. Because of the separability, $d \neq 0$. (10.15) implies that $dR' \subseteq R[a]$, whence R' is a submodule of the finite R-module $\sum_0^{n-1} (a^i/d)R$ ($n = \deg f(x)$). Since R is Noetherian, it follows that R' is a finite R-module.

(10.17) *Assume that $f(x)$ is a monic polynomial over an integral domain R. Let the roots of $f(x)$ be u_i ($i = 1, \ldots, r$) and let $f'(x)$ be the derivative of $f(x)$. Then the discriminant d of $f(x)$ coincides with* $(-1)^{(1+2+\cdots+r-1)} \prod_i f'(u_i)$.

Proof: $f(x) = (x - u_1) \cdots (x - u_r)$. Therefore, setting $g_i(x) = f(x)/(x - u_i)$, we have $f'(x) = \sum g_i(x)$, hence $f'(u_i) = g_i(u_i)$ for each i. Therefore $\prod_i f'(u_i) = \prod_i g_i(u_i) = (-1)^{(1+2+\cdots+r-1)} \prod_{i<j} (u_i - u_j)^2 = (-1)^{1+2+\cdots+r-1} d$.

By virtue of the above result, the following is a generalization of (10.15) in the case where R' is an integral domain.

(10.18) THEOREM: *Let R be a normal ring and let $f(x)$ be a monic polynomial over R. Let a be a root of $f(x)$ (in an integral extension of R). Let $f'(x)$ be the derivative of $f(x)$ and let R^* be the derived normal ring of $R[a]$. Then $f'(a)R^* \subseteq R[a]$.*

Proof: Let the roots of $f(x)$ be $a = u_1, u_2, \ldots, u_r$ and set $g_i(x) = f(x)/(x - u_i)$. Then $f'(a) = g_1(a)$. Therefore it is sufficient to prove

the assertion in the case where $f(x)$ is irreducible. If a is inseparable, then $f'(a) = 0$ and the assertion is obvious. Therefore we assume that a is separable over R. Let R'' be an almost finite separable Galois extension of R containing a and with Galois group G. Let H be the subgroup of G which corresponds to R^* and let $\sigma_1 = 1, \sigma_2, \cdots, \sigma_r$ be elements of G such that $a^{\sigma_i} = u_i$. Then it holds that $G = \sum H\sigma_i$. Furthermore $g_i(x) = f(x)/(x - a^{\sigma_i}) = g_1^{\sigma_i}(x)$. Let $c_i \in R[a]$ be such that $g_1(x) = c_{r-1}x^{r-1} + \cdots + c_0$. Then, for an arbitrary element b of R^*, we have $bf'(a) = bg_1(a) = \sum b^{\sigma_i} g_i(a) = \sum_{i,j} b^{\sigma_i} c_j^{\sigma_i} a^j$. Since $G = \sum H\sigma_i$, $\sum_i b^{\sigma_i} c_j^{\sigma_i}$ is invariant under any $\sigma \in G$, hence is in R. Thus we have $bf'(a) \in R[a]$, and the proof is complete.

EXERCISES: Let R' be a ring and let R be a subring of R'. Let $\mathfrak{a}$ be an ideal of R. An element $b \in R'$ is said to be *integral* over $\mathfrak{a}$ if there are elements $a_1, \cdots, a_n$ such that $a_i \in \mathfrak{a}^i$ for each i and such that $b^n + a_1 b^{n-1} + \cdots + a_n = 0$.

1. Prove that $b \in R'$ is integral over $\mathfrak{a}$ if and only if there are elements $u_1, \cdots, u_n$ of R' such that $bu_i \in \sum \mathfrak{a}u_i$ for any i and such that annihilators of $\sum R'u_i$ annihilate some powers of b.

2. Let $\mathfrak{b}$ be another ideal of R. Prove that if $a \in R'$ is integral over $\mathfrak{a}$ and if $b \in R'$ is integral over $\mathfrak{b}$, then ab is integral over $\mathfrak{ab}$.

3. Define the *integral closure* $\mathfrak{a}^*$ of $\mathfrak{a}$ in R' to be the set of all elements of R' which are integral over $\mathfrak{a}$. Prove that $\mathfrak{a}^*$ is an ideal of the integral closure R^* of R in R'. Prove also that $\mathfrak{a}^*$ is integrally closed in R', namely, that the integral closure of $\mathfrak{a}^*$ in R' is $\mathfrak{a}^*$.

4. Prove that when R is a Noetherian ring, an ideal $\mathfrak{b}$ contained in $\mathfrak{a}$ has the same integral closure in R (or R') if and only if there is a natural number r such that $\mathfrak{b}\mathfrak{a}^r = \mathfrak{a}^{r+1}$.

5. Assume that a ring R' is integral over its subring R and that x is an indeterminate. Prove that $R'(x)$ is integral over $R(x)$. (Hint: Let R'' be the integral closure of $R(x)$ in $R'(x)$. Use the fact that every maximal ideal of R'' lies over a maximal ideal of $R(x)$.)

11. Valuation rings

We say that a ring R is a *valuation ring* if R is an integral domain such that for any two elements a, b of R, it holds that either $aR \subseteq bR$ or $bR \subseteq aR$. When K is the field of quotients of a valuation ring R, we say that R is a valuation ring of K.

(11.1) THEOREM: *A ring R with a field of quotients K is a valuation ring of K if and only if one of the following conditions is satisfied:*

(1) *If $a \in K$, then either a or a^{-1} is in R.*

(2) *Every finitely generated ideal of R is principal and R is quasi-local.*

Proof: (1) is nothing but a restatement of the definition. Assume that R is a valuation ring and let $\mathfrak{m}$ be the set of non-units of R. Let $a_1, \ldots, a_r$ be arbitrary elements of $\mathfrak{m}$. Then there is an element a_s $(s \leq r)$ such that $a_j \in a_s R$ for any j. Hence the ideal generated by these elements is the principal ideal $a_s R$ which is contained in $\mathfrak{m}$, which implies (2). Conversely, if (2) is true, then for any two elements b, c of R, the ideal $bR + cR$ is principal, hence by (5.3), either $bR + cR = bR$ or $bR + cR = cR$, which shows that R is a valuation ring. Thus the theorem is proved.

(11.2) *Let R be a valuation ring.* (1) *If $\mathfrak{a}$ is an ideal of R and if $b \in R$ is not in $\mathfrak{a}$, then $\mathfrak{a} \subset bR$. If $\mathfrak{p}$ is a prime ideal of R, then* (2) *$R/\mathfrak{p}$ is a valuation ring and* (3) *$\mathfrak{p}$ is set-theoretically equal to $\mathfrak{p}R_{\mathfrak{p}}$.*

Proof: If $a \in \mathfrak{a}$, then $aR \subset bR$ (because $bR \nsubseteq aR$), which implies (1). (2) is therefore immediate from the definition. Let q be any element of $\mathfrak{p}R_{\mathfrak{p}}$. Then there is an element a of R which is not in $\mathfrak{p}$ and such that $p = aq$ is in $\mathfrak{p}$. Since $a \notin \mathfrak{p}$, $pR \subset aR$ by (1), and we have $q \in R$. Since $aq \in \mathfrak{p}$, we have $q \in \mathfrak{p}$, which proves (3).

(11.3) *If R is a valuation ring of a field K, then an arbitrary ring R' such that $R \subseteq R' \subseteq K$ is a valuation ring, and there is a prime ideal $\mathfrak{p}$ of R such that $R' = R_{\mathfrak{p}}$.*

Proof: The condition (1) in (11.1) is satisfied by R, hence by R', too. Therefore R' is a valuation ring, which implies R' is quasi-local by (11.1). Let $\mathfrak{p}'$ be the maximal ideal of R' and set $\mathfrak{p} = \mathfrak{p}' \cap R$. Then $R_{\mathfrak{p}} \subseteq R'$. Since any element of R' which is not in R is the inverse of a non-unit of R, by (11.1), we see that $R' \subseteq R_{\mathfrak{p}}$. Thus $R' = R_{\mathfrak{p}}$.

(11.4) *Let R be a valuation ring of a field K, let $\mathfrak{p}$ be the maximal ideal of R and let R^* be a valuation ring of the field $R/\mathfrak{p}$. Then the set $R' = \{x \mid x \in R,\ x \text{ modulo } \mathfrak{p} \in R^*\}$ is a valuation ring of K. $R'_{\mathfrak{p}} = R$ and $R'/\mathfrak{p} = R^*$*

This R' is called the *composite* of R with R^*.

Proof: Let a be an arbitrary element of K. If $a \notin R$, then $a^{-1} \in \mathfrak{p}$ and $a^{-1} \in R'$. Assume that $a \in R$. Since R^* is a valuation ring, either a modulo $\mathfrak{p} \in R^*$ or a^{-1} modulo $\mathfrak{p} \in R^*$, which shows that either $a \in R'$ or $a^{-1} \in R'$. Thus R' is a valuation ring. That $R'/\mathfrak{p} = R^*$ is obvious by the construction. That $R'_{\mathfrak{p}} = R$ follows from (11.3).

(11.5) *Let R be a valuation ring of a field K and let k be a subfield of K. Then $R \cap k$ is a valuation ring of k.*

The proof is straightforward by (11.1).

(11.6) *A valuation ring R is a normal ring.*

Proof: Let a be an element of the derived normal ring of R. If $a \notin R$, then $a^{-1} \in R$, hence we see that a^{-1} has its inverse in R by (10.5), which is a contradiction to the assumption that $a \notin R$. Thus $a \in R$, and R is normal.

A mapping v from a field K onto a set G^* is called an *additive valuation*, or merely a *valuation*, if the following conditions are satisfied: (1) G^* is the union of a linearly ordered additive group G and an element ∞ which is defined to be greater than any element of G, (2) $v(a) = \infty$ if and only if $a = 0$, (3) $v(ab) = v(a) + v(b)$ (hence, v is a homomorphism from the multiplicative group of non-zero elements of K onto G), (4) $v(a + b) \geq \min(v(a), v(b))$.

G is called the *value group* of v.

Two valuations v and v' of a field K are called *equivalent* to each other if there is an isomorphism σ from the value group G onto G' such that $\sigma(v(a)) = v'(a)$ for any $a\ (\neq 0) \in K$.

(11.7) *If v is a valuation, then $v(1) = 0, v(a^{-1}) = -v(a), v(-a) = v(a)$, and when $v(a) < v(b)$ it follows that $v(a + b) = v(a)$.*

Proof: $v(1) = v(1 \cdot 1) = v(1) + v(1)$, whence $v(1) = 0$. Hence $0 = v(1) = v(a) + v(a^{-1})$, and $v(a^{-1}) = -v(a)$. $0 = v(1) = 2v(-1)$, and $v(-1) = 0$, hence $v(-a) = v(a)$. $v(a) < v(b)$ implies $v(a + b) \geq v(a) = v(a + b - b) \geq \min(v(a + b), v(b))$, which shows that $v(a + b) = v(a)$.

If v is an additive valuation of a field K, then by the definition, it is obvious that the set $R = \{x \mid x \in K, v(x) \geq 0\}$ forms a ring. The formula $v(a^{-1}) = -v(a)$ implies that either a or a^{-1} is in R, hence R is a valuation ring. $v(a) \geq v(b)$ if and only if $aR \subseteq bR$. Thus it is easy to see that the value group is isomorphic to the multiplicative group $\{aR \mid a \neq 0\}$ with opposite order. This R is called the *valuation ring* of v. Conversely, assume that R is a valuation ring of a field K. Then the mapping v^* such that $v^*(a) = aR$ is a homomorphism from the multiplicative group of non-zero elements a of K onto that of the aR. For two elements $a, b \in K$, let c, a', b' be elements of R such that $a = a'/c, b = b'/c$. Then $a'R + b'R = \max(a'R, b'R)$, which shows that $aR \subseteq bR$ or $aR \supseteq bR$ and that $aR + bR = \max(aR, bR)$. Thus we see that $\{aR\}$ is linearly ordered and that $a + b \in \max(aR, bR)$. Therefore we see that v^* can be modified to be a valuation v (by the opposite order and changing multiplication to addition), and the valuation ring of v is R. v is unique up to equivalence. Thus we have

(11.8) *There is a one-one correspondence between valuation rings R*

of a given field K and equivalence classes of additive valuations v of K in such a way that R corresponds to the class of v if and only if R is the valuation ring of v.

We prove next the following existence theorem of valuation rings:

(11.9) *Let R be a subring of a field K and let $0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_s$ be an ascending chain of prime ideals in R. Then there exists a valuation ring V of K such that V has prime ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_s$ which lie over $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ respectively.*

Proof: We prove the assertion by induction on s. When $s = 1$: Considering $R_\mathfrak{p}$ with $\mathfrak{p} = \mathfrak{p}_1$, we may assume that $\mathfrak{p}_1$ is the unique maximal ideal of R. Let F be the set of subrings S of K such that $\mathfrak{p}_1 S \neq S$ and such that $R \subseteq S$. F is an inductive set, and therefore there is a maximal member S^* of F. Then S^* is quasi-local, for, otherwise, if $\mathfrak{m}$ is a maximal ideal of S^* containing $\mathfrak{p}_1 S^*$, then $S^*_\mathfrak{m} \in F$, which contradicts to the maximality of S^*. Let x be an element of K which is not in S^*. $x \notin S^*$ implies that $\mathfrak{p}_1 S^*[x]$ contains 1, namely, there are elements $p_0, \ldots, p_n$ of $\mathfrak{p}_1 S^*$ such that $1 + p_0 + p_1 x + \cdots + p_n x^n = 0$. Since S^* is quasi-local, $1 + p_0$ is a unit in S^*, which means that x^{-1} is integral over S^*. Hence $\mathfrak{p}_1 S^*[x^{-1}]$ does not contain 1 by (10.11). The maximality of S^* implies that $x^{-1} \in S^*$. Thus S^* is a valuation ring, and is obviously the required one, because we assumed that $\mathfrak{p}_1$ is the unique maximal ideal of R. Now, we assume that such a V, say V' with prime ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_{s-1}$, exists for the chain $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_{s-1}$. Considering $V'_{\mathfrak{n}_{s-1}}$, we may assume that $\mathfrak{n}_{s-1}$ is maximal. $R^* = R/\mathfrak{p}_{s-1}$ is a subring of the field $V'/\mathfrak{n}_{s-1}$ and has a prime ideal $\mathfrak{p}_s/\mathfrak{p}_{s-1}$. Hence, by the case where $s = 1$, there is a valuation ring V^* of $V'/\mathfrak{n}_{s-1}$ such that V^* has a prime ideal which lies over $\mathfrak{p}_s/\mathfrak{p}_{s-1}$. Then, as is easily seen, the composite of V' with V^* is the required valuation ring.

(11.10) *Let $R_1, \ldots, R_n$ be valuation rings of the same field K. For a given element a of K, there exists a natural number s such that both $a/(1 + a + \cdots + a^{s-1})$ and $1/(1 + a + \cdots + a^{s-1})$ are in the intersection D of the rings R_i.*

Proof: Let $\mathfrak{p}_i$ be the maximal ideal of R_i. We consider an arbitrarily given i ($\leq n$). If $a \notin R_i$, then by a valuation v_i with the valuation ring R_i, $0 = v_i(1) > v_i(a) \geq v_i(a^{s-1}) = v_i(1 + a + \cdots + a^{s-1})$ for any $s \geq 2$, whence i $s \geq 2$, these elements are in the R_i. Consider the case where $a \in R_i$. Since $1 + a + \cdots + a^{s-1} = (1 - a^s)/(1 - a)$, when a modulo $\mathfrak{p}_i$ is a primitive (e_i)tb root of 1 with

$e_i \geq 2$, then for s which are prime to e_i, these two elements are in the R_i. When $a - 1 \in \mathfrak{p}_i$, for s which are not multiple of the characteristic of $R/\mathfrak{p}_i$, these two elements are in the R_i. In the other case, these two elements are in the R_i for any s. By the finiteness of the number n of the R_i, there is surely an s which satisfies the above requirement for any i, and the assertion is proved.

(11.11) THEOREM: *Let $R_1, \cdots, R_n$ be valuation rings of the same field K and assume that $R_i \nsubseteq R_j$ for any $(i \neq j)$. Let $\mathfrak{p}_i$ be the maximal ideal of R_i, let D be the intersection of the R_i and set $\mathfrak{q}_i = \mathfrak{p}_i \cap D$. Then we have (1) an ideal $\mathfrak{m}$ of D is maximal if and only if $\mathfrak{m} = \mathfrak{q}_i$ for some i and (2) $R_i = D_{\mathfrak{q}_i}$.* (THEOREM OF INDEPENDENCE OF VALUATIONS)

Proof: We prove (2) at first. Let a be an arbitrary element of R_i. Let s be such that both $1/(1 + a + \cdots + a^{s-1})$ and $a/(1 + a + \cdots + a^{s-1})$ are in D, by virtue of (11.10). Since $a \in R_i$, we have $1 + a + \cdots + a^{s-1} \in R_i$, whence it is a unit in R_i. Therefore $1/(1 + a + \cdots + a^{s-1}) \notin \mathfrak{q}_i$ and therefore a is in $D_{\mathfrak{q}_i}$. Thus $R_i \subseteq D_{\mathfrak{q}_i}$. Since the converse inclusion is obvious, we have (2). (2) implies that $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j$ for any $(i \neq j)$. Therefore there is an element e_i of $\bigcap_{j \neq i} \mathfrak{q}_j$ which is not in $\mathfrak{q}_i$ for each i. Let $\mathfrak{a}$ be an ideal of D which is not contained in any of the $\mathfrak{q}_i$. Then $\mathfrak{a}$ contains an element a_i which is not in $\mathfrak{q}_i$, hence $\mathfrak{a}$ contains $\sum a_i e_i$. $\sum a_i e_i$ is not in any $\mathfrak{q}_i$. It follows that $\sum a_i e_i$ is a unit in any R_i, and therefore it is a unit in D, too. Therefore $\mathfrak{a} = D$. This implies that any maximal ideal $\mathfrak{m}$ of D is one of the $\mathfrak{q}_i$. Since $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j$ for any $(i \neq j)$, we see the converse, and the proof is complete.

We add here some remarks on normal rings.

(11.12) THEOREM: *An integral domain R is a normal ring if and only if R is an intersection of valuation rings of the field of quotients K of R.*

Proof: If R is the intersection of valuation rings V_λ, then, since each V_λ is normal, R is normal. Conversely, assume that R is normal and let b be an element of K which is not in R. Set $R' = R[1/b]$. If there is a relation $(1/b)(\sum a_i(1/b)^i) = 1$ $(a_i \in R)$, then we see that b is integral over R, which is not the case. Therefore $1/b$ is not a unit in R', whence there is a valuation ring V of K such that $1/b$ is a non-unit in V and such that $R \subseteq R' \subseteq V$ by (11.9). Thus we see that b is not in V, whence b is not in the intersection of valuation

rings of K which contain R. Therefore we see that R is the intersection of all valuation rings V of K such that $R \subseteq V$.

(11.13) *Assume that R is a normal ring and that b is an element of the field of quotients K of R. Then the kernel $\mathfrak{n}$ of the R-homomorphism ϕ, from $R[x]$ (x being a transcendental element over R) onto $R[b]$ such that $\phi(x) = b$, is generated by polynomials $cx - d$ such that $b = d/c$ ($c, d \in R$).*

Proof: Assume that $\sum_0^n a_i x^i \in \mathfrak{n}$ ($a_i \in R$) and let V be an arbitrary valuation ring of K such that $R \subseteq V$. Since $\sum a_i b^i = 0$, we have $a_n b^n V = (a_{n-1} b^{n-1} + \cdots + a_0) V \subseteq b^{n-1} V$, which implies that $a_n b V \subseteq V$, *i.e.*, $a_n b \in V$. Since V is arbitrary, we have $a_n b \in R$ by (11.12), whence $a_n x - d \in \mathfrak{n}$ with $d = a_n b$. Therefore we complete the proof by induction on n.

EXERCISES: *1.* With the same notation as in (11.11), prove that if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals of $R_1, \ldots, R_n$ respectively such that there is no inclusion relations among the minimal prime divisors of them, then $D/\bigcap(\mathfrak{a}_i)$ is the direct sum of the $R_i/\mathfrak{a}_i$.

2. Prove that a quasi-local integral domain with the field of quotients K is a valuation ring of K if and only if any ring R' such that $R \subset R' \subseteq K$ contains the inverse of some non-unit of R.

3. Assume that a ring R' dominates a valuation ring R of a field K. Prove that $R' \cap K = R$.

4. Let R be a valuation ring of a field K and let K' be an algebraic extension of K. Let R' be the integral closure of R in K'. Prove that valuation rings of K' which dominate R are just rings of quotients of R' with respect to maximal ideals, in the following way: (1) When K' is a finite Galois extension of K; let V be a valuation ring of K' dominating R and let D be the intersection of all the conjugates of V. Prove that $D = R'$. Then apply (11.11). (2) When K' is finite over K; apply the result in (1) to the smallest Galois extension of K containing K'. (3) Prove the general case, applying (2) to finite subextensions.

5. Let R be a valuation ring of a field K and let K' be an over-field of K. Prove that there is a valuation ring R' of K' such that $R < R'$ and such that the residue class field of R' is algebraic over that of R, in the following way:

Let $\{u_\lambda\}$ be a transcendance base of K' over K and set $K'' = K(\{u_\lambda\})$. Prove the existence of such a valuation ring of K''. Then apply *4* above.

12. Noetherian normal rings

Let us begin with the following remark:

(12.1) *A local ring $(R, \mathfrak{m})$ which is not a field is a valuation ring if and only if height $\mathfrak{m} \geq 1$ and $\mathfrak{m}$ is principal. In this case, height $\mathfrak{m} = 1$.*

Proof: The *only if* part is obvious. We prove the *if* part. height

$\mathfrak{m} = 1$ by the altitude theorem of Krull. Let $\mathfrak{q}$ be a minimal prime divisor of zero and let p be a basis for $\mathfrak{m}$. Since $p \notin \mathfrak{q}$, we have $\mathfrak{q}:p = \mathfrak{q}$. On the other hand, $\mathfrak{q} \subseteq pR$, hence $\mathfrak{q} = 0$ by (4.3). Thus R is an integral domain. Let $\mathfrak{a} \neq 0$ be an ideal of R, and let n be such that $\mathfrak{a} \subseteq p^nR$, $\mathfrak{a} \nsubseteq p^{n+1}R$. Then $\mathfrak{a} = (\mathfrak{a}:p^n)p^n$. If $\mathfrak{a}:p^n \neq R$, then $\mathfrak{a}:p^n \subseteq pR$ and $\mathfrak{a} \subseteq p^{n+1}R$ which is not the case. Thus $\mathfrak{a} = p^nR$. Therefore we see that every non-zero ideal of R is a power of pR, hence R is a valuation ring.

Next we have the following lemma:

(12.2) *Let a, b, c, d be elements of a ring R such that $ad = bc$. If a is not a zero divisor, then $aR:cR \subseteq bR:dR$. Consequently if both a and b are non-zero divisors, then we have $aR:cR = bR:dR$.*

Proof: $x \in aR:cR$ implies $cx = ay$ with $y \in R$, hence $ayb = bcx = adx$. Therefore $by = dx$, and $x \in bR:dR$.

(12.3) *Let $\mathfrak{p}$ be a prime ideal of a Noetherian ring R. Assume that $R_\mathfrak{p}$ is not a valuation ring. Then for any non-zero divisor $a \in \mathfrak{p}$ and for any element b of $aR:\mathfrak{p}$, b/a is integral over R and the conductor of R in $R[b/a]$ contains $\mathfrak{p}$.*

Proof: Let p be any arbitrary element of $\mathfrak{p}$. Then $bp = ar$ with an $r \in R$. If $r \notin \mathfrak{p}$, then $\mathfrak{p} \subseteq aR:bR \subseteq pR:rR \subseteq \mathfrak{p}$ (by virtue of (12.2)), which implies that $\mathfrak{p} = pR:rR$ and we see that $\mathfrak{p}R_\mathfrak{p}$ is generated by p, hence $R_\mathfrak{p}$ is a valuation ring by (12.1), which is a contradiction. Thus $(b/a)\mathfrak{p} \subseteq \mathfrak{p}$, and the assertion is proved by (10.4).

As an immediate consequence of (12.3), we have

(12.4) THEOREM: *A normal local ring of altitude* 1 *is a valuation ring.*

(12.5) THEOREM: *Let $\mathfrak{p}$ be a prime ideal of a Noetherian ring R and assume that $\mathfrak{p}$ contains an element a which is not a zero divisor. Then $\mathfrak{p}$ is a prime divisor of aR if and only if either* height $\mathfrak{p} = 1$ *and $R_\mathfrak{p}$ is a valuation ring or there exist a, $b \in R$ such that b/a is integral over R and such that the conductor of R in $R[b/a]$ coincides with $\mathfrak{p}$.*

Proof: Assume at first that $\mathfrak{p}$ is a prime divisor of aR and that $R_\mathfrak{p}$ is not a valuation ring. Let b be an element of R such that $\mathfrak{p} = aR:bR$ (by (8.8)). Then $b \in aR:\mathfrak{p}$, hence, by (12.3), b/a is integral over R and the conductor $\mathfrak{c}$ of R in $R[b/a]$ contains $\mathfrak{p}$. If $c \in \mathfrak{c}$, then $cb/a \in R$, *i.e.*, $cb \in aR$, hence $c \in aR:b = \mathfrak{p}$. Thus the conductor $\mathfrak{c}$ coincides with $\mathfrak{p}$. Conversely assume at first that height $\mathfrak{p} = 1$. Then obviously $\mathfrak{p}$ is a minimal prime divisor of aR. Assume next that $\mathfrak{p}$ is the conductor of R in $R[b/a]$. Then $\mathfrak{p}R_\mathfrak{p}$ is the conductor of $R_\mathfrak{p}$ in $R_\mathfrak{p}[b/a]$.

Since $(b/a)\mathfrak{p} \subseteq R$, we have $b\mathfrak{p} \subseteq aR$, and $\mathfrak{p} \subseteq aR{:}bR$, and therefore $\mathfrak{p}R_{\mathfrak{p}} \subseteq aR_{\mathfrak{p}}{:}bR_{\mathfrak{p}} \neq R_{\mathfrak{p}}$, which implies that $\mathfrak{p}R_{\mathfrak{p}} = aR_{\mathfrak{p}}{:}bR_{\mathfrak{p}}$; hence $\mathfrak{p}R_{\mathfrak{p}}$ is a maximal prime divisor of $aR_{\mathfrak{p}}$, and the assertion is proved.

(12.6) THEOREM: *If R is a Noetherian ring and if a prime ideal $\mathfrak{p}$ is a prime divisor of aR with a non-zero-divisor a of R, then for any non-zero-divisor b contained in $\mathfrak{p}$, $\mathfrak{p}$ is a prime divisor of bR.*

Proof: By (8.8), there is an element c of R such that $aR{:}cR = \mathfrak{p}$. Then, since $b \in \mathfrak{p}$, there is an element $d \in R$ such that $bc = ad$. It follows from (12.2) that $aR{:}cR = bR{:}dR$, hence $\mathfrak{p} = bR{:}dR$, which implies that $\mathfrak{p}$ is a prime divisor of bR by virtue of (8.8).

(12.7) COROLLARY: *Let R be a Noetherian ring and let a, b be elements of R such that a is not a zero divisor, $b/a \notin R$ and such that b/a is integral over R. Then either there is a minimal prime divisor $\mathfrak{p}$ of aR such that $R_{\mathfrak{p}}$ is not a normal ring or there exists an imbedded prime divisor of aR.*

Proof: Assume that the prime divisors $\mathfrak{p}_i$ of aR are all minimal and that $R_{\mathfrak{p}}$ are normal for any $\mathfrak{p} = \mathfrak{p}_i$. Let $\mathfrak{q}_i$ be the primary component of aR belonging to $\mathfrak{p}_i$. Since b/a is integral over R, it is integral over $R_{\mathfrak{p}_i}$ which is a normal ring, hence $b/a \in R_{\mathfrak{p}_i}$, and $b \in aR_{\mathfrak{p}_i} \cap R = \mathfrak{q}_i$. Thus $b \in \bigcap \mathfrak{q}_i = aR$, and $b/a \in R$. Thus we have proved the assertion.

(12.8) *If R is a normal ring, then any ring of quotients of R is also a normal ring.*

Proof: If a is integral over R_S, then there is an element $s \in S$ such that as is integral over R, which proves the assertion.

(12.9) THEOREM: *A Noetherian integral domain R is a normal ring if and only if the following two conditions are satisfied: (1) If $\mathfrak{p}$ is a prime ideal of height 1 in R, then $R_{\mathfrak{p}}$ is a normal ring and (2) if $\mathfrak{p}$ is a prime divisor of a principal ideal $\neq 0$, then* height $\mathfrak{p} = 1$.

Proof: Assume that R is normal. Then (1) holds good by (12.8), while the validity of (2) follows from (12.5). The converse is an immediate consequence of (12.7).

A Noetherian normal ring of altitude 1 is called a *Dedekind domain*. (12.4) and (1.4) imply that:

(12.10) *Any ideal $\mathfrak{a} \neq 0$ of a Dedekind domain R is the product of maximal ideals of R, and such an expression is uniquely determined by $\mathfrak{a}$.*

EXERCISES: *1.* Let $\mathfrak{p}$ be a prime ideal of a Noetherian ring R and assume that

height $\mathfrak{p} \geq 1$. Prove that $R_{\mathfrak{p}}$ is a valuation ring if and only if there is no primary ideal $\mathfrak{q}$ such that $\mathfrak{p}^{(2)} \subset \mathfrak{q} \subset \mathfrak{p}$.

2. Prove that a Noetherian ring R is integrally closed if and only if R is the direct sum of finite number of Noetherian rings R_i such that either R_i is a normal ring or every maximal ideal of R_i is a prime divisor of zero (namely, every non-unit of R_i is a zero divisor).

3. Let R be a Noetherian normal ring. Prove that every principal ideal aR of R is an intersection of symbolic powers of prime divisors of aR.

4. Let R be a Noetherian integral domain. Assume that every ideal of R is a product of prime ideals. Prove that R is either a Dedekind domain or a field.

5. Let R be a Dedekind domain with field of quotients K. Prove that the set of non-zero finite R-submodules of K forms a multiplicative group by the natural multiplication.

6. Assume that M is a finite module over a Noetherian ring R, that $a \in R$ is not a zero divisor with respect to M and that $\mathfrak{p}$ is an associated prime ideal of aM (in M). Prove that if $b \in \mathfrak{p}$ is not a zero divisor with respect to M, then $\mathfrak{p}$ is an associated prime ideal of bM.

13. Unique factorization rings

An element a of a ring R is called *irreducible* (in R) if a is not a product of any two non-units of R. We say that an integral domain R is a *unique factorization ring* if (1) every element $a \neq 0$ of R is the product of a finite number of irreducible elements and (2) if $a = a_1 \cdots a_m = b_1 \cdots b_n$ with irreducible elements a_i and b_j, then $m = n$ and there is a permutation π of the i such that $a_{\pi(i)}R = b_iR$.

An element $a \neq 0$ of an integral domain R is called a *prime element* if aR is a prime ideal of R. It is obvious that a prime element is an irreducible element, but not conversely.

Note that the condition (1) above is satisfied by any Noetherian integral domain.

(13.1) THEOREM: *A Noetherian integral domain R is a unique factorization ring if and only if every prime ideal $\mathfrak{p}$ of height 1 in R is principal.*

Proof: Assume that R is a unique factorization ring. For any prime ideal $\mathfrak{p}$ of height 1, let a be an irreducible element of R contained in $\mathfrak{p}$. Let b be an element of $aR:\mathfrak{p}$ which is not in aR. Assume for a moment that $aR \neq \mathfrak{p}$. Then let $c \in \mathfrak{p}$ such that $c \notin aR$. Then $bc \in aR$, and therefore there is an element $d \in R$ such that $bc = ad$. But a is not an irreducible factor of b or c, which is a contradiction. Thus $\mathfrak{p} = aR$ and the *only if* part is proved. Assume conversely that every prime ideal of height 1 is principal and let $a_1 \cdots a_m = b_1 \cdots b_n$ be factoriza-

tions of an element c as products of irreducible elements a_i and b_j. We prove the uniqueness by induction on n. When $n = 1$, c is irreducible and the assertion is obvious. By assumption, irreducible elements which are non-units are prime elements. Since $a_1 \cdots a_m \in b_1R$, which is prime, some $a_i \in b_1R$; we may assume that $a_1 \in b_1R$. Since a_1R is prime, we have $a_1R = b_1R$, and therefore there is a unit u such that $a_2 \cdots a_m = (ub_2)b_3 \cdots b_n$, whence, by induction, we have the proof of the uniqueness.

(13.2) *If R is a unique factorization ring, then for any multiplicatively closed set S which does not contain 0, R_S is a unique factorization ring.*

Proof: A prime element of R is either a unit or a prime element of R_S. Furthermore, ideals of R_S are generated by ideals of R, hence the assertion follows from the definition.

(13.3) *A unique factorization ring R is a normal ring.*

Proof: Assume that a/b $(a, b \in R)$ is integral over R: $(a/b)^n + c_1(a/b)^{n-1} + \cdots + c_n = 0$ $(c_i \in R)$. We may assume that a and b have no common prime factor. Assume that p is a prime factor of b. Then, since $a^n + c_1a^{n-1}b + \cdots + c_nb^n = 0$, we have $a^n \in pR$ and $a \in pR$, which is a contradiction, and $a/b \in R$.

(13.4) COROLLARY: *The polynomial ring in a finite number of algebraically independent elements over a field is a normal ring.*

EXERCISES: *1*. Let R be a Noetherian normal ring and let S be a multiplicatively closed subset of R which does not contain 0. Assume that (1) there is a natural number e such that $\mathfrak{q}^{(e)}$ is principal, for any prime ideal $\mathfrak{q}$ of height 1 in R such that $\mathfrak{q}$ meets S and that (2) there is a natural number f such that $\mathfrak{p}'^{(f)}$ is principal for any prime ideal $\mathfrak{p}'$ of height 1 in R_S. Prove that for any prime ideal $\mathfrak{p}$ of height 1 in R, $\mathfrak{p}^{(ef)}$ is principal.

2. Assume that $p_1, \ldots, p_r$ are prime elements of an integral domain R. Prove that an ideal $\mathfrak{a}$ of R has prime divisors only among the p_iR if and only if $\mathfrak{a}$ is a principal ideal generated by the product of some powers of p_i.

3. Prove that an integral domain R is a unique factorization ring if and only if (1) R satisfies the maximum condition for principal ideals and (2) every prime ideal of R different from zero contains a principal prime ideal different from zero.

4. Give an example of a normal ring R, which is not a unique factorization ring, in which every prime ideal of height 1 is principal.

14. A normalization theorem

When I is a subring of an integral domain R and when K and L are the fields of quotients of I and R respectively, then we know

the transcendence degree of L over K, which is defined to be the *transcendence degree* of R over I.

(14.1) *Let K be a field and let $x_1, \ldots, x_n$ be algebraically independent elements over K. If y_1 is an element of $K[x] = K[x_1, \ldots, x_n]$ which is not in K, then there are elements $y_2, \ldots, y_n$ of $K[x]$ such that* (1) *$y_i = x_i + x_1^{m_i}$ for some natural numbers m_i $(i = 2, \ldots, n)$ and* (2) *$K[x]$ is integral over $K[y_1, \ldots, y_n]$ (and therefore $y_1, \ldots, y_n$ are algebraically independent over K). Furthermore,* (3) *if a natural number $s > 1$ is given, all the m_i can be chosen to be powers of s.*

Proof: We write y_1 as $\sum a_i M_i$, where $a_i \in K$, $a_i \neq 0$ and the M_i are monomials in the x_i. We define weights $m_1 = 1, m_2, \ldots, m_n$ of $x_1, x_2, \ldots, x_n$ such that one M_i, say M_1, has greater weight than the others; let t be a power of s such that t is greater than the degree d of y_1 and set $m_i = t^{i-1}$ for each i. Then, since weight $x_r^d <$ weight x_{i+1} for any $i = 1, 2, \ldots, n-1$, we see that the m_i satisfies the requirement on the weights (considering a lexicographical order of the monomials M_i). Set $y_i = x_i + x_1^{m_i}$ for $i = 2, \ldots, n$. Then y_1 can be written $\pm a_1 x_1^w + f_1 x^{w-1} + \cdots + f_w$ where $w =$ weight M_1 and the f_i are polynomials in $y_2, \ldots, y_n$ with coefficients in K. Therefore x_1 is integral over $K[y_1, \ldots, y_n]$, whence the x_i, which are in $K[y_1, \ldots, y_n, x_1]$, are integral over $K[y_1, \ldots, y_n]$. Thus the y_i are the required elements.

(14.2) THEOREM: *Let K be a field and let $x_1, \ldots, x_n$ be algebraically independent elements over K. If $\mathfrak{a}$ is an ideal of height r in the polynomial ring $K[x] = K[x_1, \ldots, x_n]$, then there are elements $y_1, \ldots, y_n$ of $K[x]$ such that* (1) *$K[x]$ is integral over $K[y] = K[y_1, \ldots, y_n]$,* (2) *$\mathfrak{a} \cap K[y]$ is generated by $y_1, \ldots, y_r$ and* (3) *$y_{r+j} = x_{r+j} + f_j$ with polynomials f_j in $x_1, \ldots, x_r$ with coefficients in the prime integral domain π of K for each $j = 1, 2, \ldots, n-r$. If K is of characteristic $p \neq 0$, then the f_j can be chosen such that $f_j \in \pi[x_1^p, \ldots, x_r^p]$.* (NORMALIZATION THEOREM FOR POLYNOMIAL RINGS)

Proof: We prove the assertion by induction on r. If $r = 0$, the assertion is obvious. Assume that $r \geq 1$ and let $\mathfrak{a}'$ be an ideal of $K[x]$ such that height $\mathfrak{a}' = r - 1$ and such that $\mathfrak{a}' \subseteq \mathfrak{a}$. Then, by induction, there are elements $y_1, \ldots, y_{r-1}, y_r', \ldots, y_n'$ of $K[x]$ which satisfy the conditions in our assertion with $\mathfrak{a}'$ instead of $\mathfrak{a}$. Since height $\mathfrak{a} = r$, we have by (10.14) that height $(\mathfrak{a} \cap K[y_1, \ldots, y_{r-1}, y_r', \ldots, y_n']) = r$. On the other hand, we have $y_i \in \mathfrak{a}' \subseteq \mathfrak{a} (1 \leq i \leq r-1)$ by construction. Therefore there is an element y_r of $\mathfrak{a} \cap K[y_r', \ldots, y_n']$

which is not zero. Then, applying (14.1) to y_r and $K[y_r', \ldots, y_n']$, we see the existence of $y_{r+1}, \ldots, y_n$ of $K[y_r', \ldots, y_n']$ such that (a) $y_{r+j} = y_{r+j}' + y_r'^{m_j}$ (if the characteristic $p \neq 0$, m_j can be powers of p) and such that (b) $K[y_r', \ldots, y_n']$ is integral over $K[y_r, \ldots, y_n]$. The first condition (a) implies the validity of (3) (and the statement in parentheses implies the validity of the last statement in the theorem), while the condition (b) implies the integral dependence of $K[x]$ over $K[y]$. Since $y_1, \ldots, y_r$ are in $\mathfrak{a}$, $\mathfrak{a} \cap K[y]$ contains them. Since $\sum_1^r y_i K[y]$ is a prime ideal of height r and since height $\mathfrak{a} \cap K[y] = r$, the inclusion implies the equality. Thus the theorem is proved.

(14.3) COROLLARY: *Let I be an integral domain and let $x_1, \ldots, x_n$ be algebraically independent elements over I. Let K be the field of quotients of I. If $\mathfrak{a}$ is an ideal of $I[x] = I[x_1, \ldots, x_n]$ such that $\mathfrak{a} \cap I = 0$, then there are elements $y_1, \ldots, y_n$ of $I[x]$ and an element $a(\neq 0)$ of I such that (1) $I[a^{-1}][x]$ is integral over $I[a^{-1}][y]$, (2) $\mathfrak{a}I[a^{-1}][x] \cap I[a^{-1}][y]$ is generated by $y_1, \ldots, y_r$ with $r =$ height $\mathfrak{a}K[x]$ and (3) $y_{r+j} = x_{r+j} + f_j$ with polynomials f_j in $x_1, \ldots, x_r$ with coefficients in the prime integral domain for each $j = 1, \ldots, n - r$.*

Proof: Set $\mathfrak{a}' = \mathfrak{a}K[x]$, and let $y_1, \ldots, y_n$ be as in (14.2) applied to $\mathfrak{a}'$ and $K[x]$. Then (3) is valid for them. Since $y_1, \ldots, y_r$ are in $\mathfrak{a}'$, there is an element $a_i \neq 0$ of I such that $a_i y \in \mathfrak{a}$ for each i. Since K is a field, $a_1 y_1, \ldots, a_r y_r$ are as good as $y_1, \ldots, y_r$. Therefore we may assume that $y_1, \ldots, y_r$ are in $\mathfrak{a}$. Since x_i is integral over $K[y]$, there is an element $c_i(\neq 0)$ of I such that $c_i x_i$ is integral over $I[y]$ for each i. Let a be the product of all the c_i. Then we see easily that this a and the above y_j are the required elements.

(14.4) THEOREM: *Assume that a ring R is generated by elements $b_1, \ldots, b_n$ over an integral domain I. Assume furthermore that no elenent $a(\neq 0)$ of I is a zero divisor in R. Then there are elements $z_1, \ldots, z_t$ of $\pi[b_1, \ldots, b_n]$ (where π is the prime integral domain of I) which are algebraically independent over I and an element $a(\neq 0)$ of I such that $R[a^{-1}]$ is integral over $I[a^{-1}, z_1, \ldots, z_t]$.* (NORMALIZATION THEOREM FOR FINITELY GENERATED RINGS)

Proof: Let $x_1, \ldots, x_n$ be indeterminates. Then there is a uniquely determined homomorphism ϕ from $I[x] = I[x_1, \ldots, x_n]$ onto $I[b]$ such that $\phi(x_i) = b_i$ for each i. Let $\mathfrak{a}$ be the kernel of ϕ, and let $y_1, \ldots, y_n$, and a be elements as in (14.3) applied to $\mathfrak{a}$ and $I[x]$. Set $z_i = \phi(y_{r+i})$. Since $y_i \in \mathfrak{a}$ for $i \leq r$, $I[a^{-1}][b]$ is integral over

$I[a^{-1}][z]$. Since $\mathfrak{a} \cap I[y_{r+1}, \ldots, y_n] = 0$, the z_i are algebraically independent over I. Since $y_{r+j} \in \pi[x_1, \ldots, x_n]$, we have $z_i \in \pi[b_1, \ldots, b_n]$, and the assertion is proved.

(14.5) THEOREM: *Let R be an integral domain which is generated by a finite number of elements $b_1, \ldots, b_n$ over a field K. If $\mathfrak{p}_0, \ldots, \mathfrak{p}_t$ are prime ideals such that $\mathfrak{p}_0 = 0$, $\mathfrak{p}_t$ is maximal, $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_t$ and such that there is no prime ideal $\mathfrak{q}$ such that $\mathfrak{p}_{i-1} \subset \mathfrak{q} \subset \mathfrak{p}_i$ for any i, then t must be the transcendence degree of R over K.*

Proof: We prove the assertion by induction on t. There are algebraically independent elements $z_1, \ldots, z_u$ over $K (z_i \in R)$ such that R is integral over $K[z]$, by (14.4). If $t = 0$, then $K[z]$, is a field by (10.5) whence $u = 0$ and the assertion is true. Assume that $t > 0$. Then applying (14.1) to $\mathfrak{p}_1 \cap K[z]$ and $K[z]$, we may assume that $z_1 \in \mathfrak{p}_1$. Then $\mathfrak{p}_1 \cap K[z] = z_1 K[z]$ by (10.14). Then, applying the induction assumption to $R/\mathfrak{p}_1$, which is integral over $K[z]/z_1 K[z]$, and to the prime ideals $\mathfrak{p}_i/\mathfrak{p}_1$, we see that $t - 1 = u - 1$, whence $t = u$, which proves the assertion.

(14.6) COROLLARY: *If an integral domain R is finitely generated over a field K, then for any prime ideal $\mathfrak{p}$ of R,* height $\mathfrak{p}$ + depth $\mathfrak{p}$ *is equal to the transcendence degree of R over K and* depth $\mathfrak{p}$ *is equal to the transcendence degree of $R/\mathfrak{p}$ over K.*

(14.7) THEOREM: *If an integral domain R is generated by n elements over a field K, and if $\mathfrak{m}$ is a maximal ideal of R, then $\mathfrak{m}$ is generated by n elements and $R/\mathfrak{m}$ is algebraic over K.*

Proof: That $R/\mathfrak{m}$ is algebraic over K follows from (14.6). Let $b_1, \ldots, b_n$ be such that $R = K[b_1, \ldots, b_n]$. Let c_i be (b_i modulo $\mathfrak{m}$) for each i and let $f_i'(x_i)$ be the irreducible monic polynomial over $K[c_1, \ldots, c_{i-1}]$ which has c_i as a root. Let f_i be the monic polynomial in b_i with coefficients in $K[b_1, \ldots, b_{i-1}]$ which is obtained from f_i' replacing $c_1, \ldots, c_{i-1}, x_i$ with $b_1, \ldots, b_{i-1}, b_i$, respectively. Then we see that $R/(\sum f_i R) = K[c_1, \ldots, c_n]$, and therefore $\mathfrak{m} = \sum f_i R$, which proves the assertion.

(14.8) COROLLARY: *Let $x_1, \ldots, x_n$ be algebraically independent elements over an integral domain I. Let $\mathfrak{p}$ be a prime ideal of $I[x] = I[x_1, \ldots, x_n]$. If $I_{(\mathfrak{p} \cap I)}$ is a regular local ring, then $I[x]_{\mathfrak{p}}$ is a regular local ring.*

Proof: We may assume that $I = I_{(\mathfrak{p} \cap I)}$. Let $f_1, \ldots, f_s$ be a regular

system of parameters of I. We set $\mathfrak{q} = \mathfrak{p} \cap I$, $K = I/\mathfrak{q}$, and $z_i = x_i$ modulo $\mathfrak{q}I[x]$. Then, obviously the z_i are algebraically independent over K and $I[x]/\mathfrak{q}I[x] = K[z]$. We set $\mathfrak{p}' = \mathfrak{p}/\mathfrak{q}I[x]$, and apply (14.2) to $\mathfrak{p}'$ and $K[z]$; let $y_1, \ldots, y_n$ be as in (14.2) applied to our case. Then $K[z] = K[z_1, \ldots, z_r, y_{r+1}, \ldots, y_n]$. Let L be the field of quotients of $K[y_{r+1}, \ldots, y_n]$. Then $\mathfrak{p}'L[z_1, \ldots, z_r]$ is a maximal ideal of $L[z_1, \ldots, z_r]$, and therefore it is generated by r elements, whence $\mathfrak{p}'K[z]_{\mathfrak{p}'}$ is generated by r elements, which implies that $\mathfrak{p}I[x]_{\mathfrak{p}}$ is generated by $r + s$ elements. Since height $\mathfrak{p}' = r$, we see that height $\mathfrak{p} \geq r + s$ by (6.15), whence $I[x]_{\mathfrak{p}}$ is a regular local ring.

(14.9) THEOREM: *If a ring R is finitely generated over a field K, then the Jacobson radical of R is the radical of R.* (HILBERT ZERO-POINTS THEOREM)

Proof: We first assume that R is an integral domain. Let f be an element of R which is not zero and consider $R[1/f]$. (14.6) implies that maximal ideals of $R[1/f]$ lie over maximal ideals of R, which implies that there are maximal ideals which do not contain f. Since f is arbitrary, it follows that the Jacobson radical of R is zero. Now we consider the general case. The above result shows that if $\mathfrak{p}$ is a prime ideal of R, then the intersection of maximal ideals of R which contain $\mathfrak{p}$ coincides with $\mathfrak{p}$, and therefore we get the result.

(14.10) *Let $x_1, \ldots, x_n$ be algebraically independent elements over an integral domain I. Then there is a maximal ideal $\mathfrak{m}$ of $I[x]$ such that $\mathfrak{m} \cap I = 0$ if and only if there is an element $a(\neq 0)$ of I such that $I[a^{-1}]$ is the field of quotients of I.*

Proof: If there is such an element a, then a maximal ideal $\mathfrak{m}$ of $I[x]$, such that $ax_1 - 1 \in \mathfrak{m}$, lies over zero of I. Assume conversely that there is a maximal ideal $\mathfrak{m}$ of $I[x]$ which lies over zero of I. Then, applying (14.4) to $I[x]/\mathfrak{m}$, which is a field, we see that the t in (14.4) must be zero in this case, and $I[a^{-1}]$ is a field by (10.5). Thus the proof is complete.

EXERCISE: With the same K, x_i and $\mathfrak{a}$ as in (14.2), assume that K contains infinitely many elements. Prove that there are elements $y_1, \ldots, y_n$ of $K[x]$ satisfying (1) and (2) in (14.2) and such that the y_{r+j} $(j = 1, 2, \ldots, n - r)$ are linear combinations of the x_i with coefficients in K.

CHAPTER II

Completions

15. Formal power series ring

Let R be a ring and let $x_1, \ldots, x_r$ be indeterminates. Let F_d be the module of homogeneous forms of degree d in the x_i with coefficients in R for every $d = 0, 1, \ldots, n, \ldots$. The set F of infinite sums $\sum a_i$ with $a_i \in F_i$ forms a ring by the obvious operations $(\sum a_i) + (\sum b_i) = \sum (a_i + b_i)$, $(\sum a_i)(\sum b_i) = \sum_n (\sum_{i+j=n} a_i b_j)$. This F is called the *formal power series ring* or merely the *power series ring* in the x_i with coefficients R, and is denoted by $R[[x_1, \ldots, x_r]]$ or simply by $R[[x]]$. Elements of $R[[x]]$ are called (*formal*) *power series* in the x_i with coefficients in R. For an element $\sum a_i$ of $R[[x]] (a_i \in F_i)$, the number n, such that $a_n \neq 0$ and such that $a_i = 0$ for $i < n$, is called the *leading degree* of the element, and the a_n is called the *leading form* of the element. The leading form of 0 is defined to be 0. a_0 is called the *constant term* of the element.

Note that $R[x]$ is a subring of $R[[x]]$ by the obvious identification that a finite sum $\sum_0^r a_i$ is identified with infinite sum $\sum_0^\infty a_i$ with $a_i = 0$ for $i > r$.

The above notation will be fixed throughout this section.

(15.1) THEOREM: *There is a one-one correspondence between all maximal ideals* $\mathfrak{m}$ *of* R *and all maximal ideals* $\mathfrak{m}^*$ *of* $R[[x]]$ *in such a way that* $\mathfrak{m}^*$ *corresponds to* $\mathfrak{m}$ *if and only if* $\mathfrak{m}^*$ *is generated by* $\mathfrak{m}$ *and the* x_i.

Proof: We see obviously that, when $\mathfrak{m}$ is a maximal ideal of R, the ideal $\mathfrak{m}R[[x]] + \sum x_i R[[x]]$ is a maximal ideal of $R[[x]]$. Let $\mathfrak{m}^*$ be a maximal ideal of $R[[x]]$ and let $\mathfrak{m}$ be the set of constant terms of elements of $\mathfrak{m}^*$. Then $\mathfrak{m}$ is obviously an ideal of R. If we know that $\mathfrak{m} \neq R$, then $\mathfrak{m}^*$ is contained in $\mathfrak{m}R + \sum x_i R[[x]]$, and we see that $\mathfrak{m}^* = \mathfrak{m}R[[x]] + \sum x_i R[[x]]$ and that $\mathfrak{m}$ is maximal. Therefore it is sufficient to show that $\mathfrak{m} \neq R$. Assume the contrary. Then there is an element $\sum a_i$ of $\mathfrak{m}^*$ with $a_0 = 1$. Set $b = -(\sum_1^\infty a_i)$. Then we

can consider $f \quad \sum_0^m b'$ which is equal to $\sum c_i$ where each c_n is defined to be the nth degree part of $\sum_0^m b'$ for an $m \quad n$, hence for any $m \geq n$. Since $(\sum a_i)(\sum_0^m b^i) \quad (1 \quad b)(\sum_0^n b^i) \quad 1 - b^{n+1}$, we see that $(\sum a_i)(\sum_0^n c_i) = 1 + (\sum$ (terms of degree $> n$)), which means that the nth degree part of $(\sum a_i)(\sum c_i)$ is 1 or zero according as n is zero or not. Thus we see that the element $\sum a_i$ is unit, which contradicts to the assumption that $\sum a_i \in \mathfrak{m}^*$, and the proof is completed.

(15.2) COROLLARY: *An element $f \in R[[x]]$ is a unit if and only if the constant term of f is a unit in R.*

(15.3) THEOREM: *If R is Noetherian, then $R[[x]]$ is also Noetherian.*

Proof: Let $\mathfrak{a}$ be an arbitrary ideal of $R[[x]]$. It is sufficient to show that $\mathfrak{a}$ has a finite basis. Let $\mathfrak{a}^*$ be the set of leading forms of elements of $\mathfrak{a}$. Then $\mathfrak{a}^*$ generates an ideal of the polynomial ring $R[x]$, which has a finite basis (over $R[x]$), say $f_1^*, \ldots, f_t^*$, consisting of elements of $\mathfrak{a}^*$. Let f_i be an element of $\mathfrak{a}$ which has f_i^* as its leading form and let $\mathfrak{a}'$ be the ideal of $R[[x]]$ generated by the $f_1, \ldots, f_t$. Let g be an arbitrary element of $\mathfrak{a}$. By the choice of $\mathfrak{a}'$, there is an element $\sum f_i h_{i,0}$ of $\mathfrak{a}'$ which has the same leading form as g, and the same is applied to $g - \sum f_i h_{i,0}$ and so on. Thus we see that there is a sequence of elements $\sum f_i h_{i,n} (h_{i,n} \in R[[x]]; n = 0, 1, 2, \ldots)$ such that (1) $\sum f_i h_{i,n}$ has leading degree greater than that of $\sum f_i h_{i,n-1}$ and (2) $\sum f_i h_{i,n}$ and $g - \sum_{j<n} (\sum f_i h_{i,j})$ have the same leading form. This shows that the terms of each degree of g and $\sum_n (\sum_i f_i h_{i,n})$ coincide to each other, whence $g = \sum_n (\sum_i f_i h_{i,n}) = \sum_i f_i (\sum_n h_{i,n})$, and $g \in \mathfrak{a}'$. Thus we have $\mathfrak{a} = \mathfrak{a}'$, which completes the proof.

(15.4) COROLLARY: *If R is a semi-local ring, then so is $R[[x]]$, too; If R is a local ring, then so is $R[[x]]$.*

EXERCISES: *1.* Prove that if R is a semi-local ring, which may not be Noetherian, then so is $R[[x]]$.

2. Prove that $R[[x_1, x_2]] = R[[x_1]][[x_2]]$, and similarly, that $R[[x_1, \ldots, \ldots, x_r]] = R[[x_1]] \cdots [[x_r]]$.

16. An ideal-adic topology

Let $\mathfrak{a}$ be an ideal of a ring R and let M be an R-module. Let F be the family of $\mathfrak{a}^n M$. We introduce a topology on M, which may not be a T_0-topology, taking F to be a base of neighborhoods of zero of R, which means that open sets of M are unions of an arbitrary number

of sets of the form $b + \mathfrak{a}^n M$ ($b \in M$). This topology is called the $\mathfrak{a}$-*adic topology* of M. Then addition is continuous (*i.e.*, $f(x, y) = x + y$ is a continuous function from $M \times M$ into M) and the multiplication of elements of R is also continuous (*i.e.*, $f(x, y) = xy$ is a continuous function from $R \times M$ into M, where the topology of R is assumed to be the $\mathfrak{a}$-adic topology of R).

We retain the above meanings of R, M, and $\mathfrak{a}$ throughout this section.

(16.1) *The $\mathfrak{a}$-adic topology of M is T_0 if and only if $\bigcap \mathfrak{a}^n M = 0$. If the $\mathfrak{a}$-adic topology of M is T_0, then the following distance function r makes M a metric space*: $r(x, x) = 0$; $r(x, y) = 2^{-n}$ *if and only if* $x - y \in \mathfrak{a}^n M$ *and* $x - y \notin \mathfrak{a}^{n+1} M$.

The proof is straightforward and we omit it.

(16.2) *A submodule N of the R-module M is an open set of M in the $\mathfrak{a}$-adic topology, if and only if $N : M$ contains some power of $\mathfrak{a}$. In that case, N is also a closed set.*

Proof: If N is an open set, then $0 \in N$ implies $\mathfrak{a}^n M \subseteq N$ for some n. Conversely, if $\mathfrak{a}^n M \subseteq N$, then since N is a submodule, $b + \mathfrak{a}^n M \subseteq N$ for any $b \in N$, and N is the union of the open sets $b + \mathfrak{a}^n M$, which proves that N is open. If N is open, then the complement $M - N$ of N is the union of $x + N$ with $x \in M - N$, and each $x + N$ is open, hence $M - N$ is open. Thus N is closed.

(16.3) THEOREM: *The closure N^* of a submodule N of M in M with the $\mathfrak{a}$-adic topology coincides with $\bigcap_n (N + \mathfrak{a}^n M)$.*

Proof: Since each $N + \mathfrak{a}^n M$ is an open set, it is a closed set by (16.2). Hence $N^* \subseteq N + \mathfrak{a}^n M$ for any n, and $N^* \subseteq \bigcap (N + \mathfrak{a}^n M)$. Conversely, let x be an arbitrary element of $\bigcap (N + \mathfrak{a}^n M)$. Then $x = b_n + a_n$ with $b_n \in N$, $a_n \in \mathfrak{a}^n M$ for each n, which shows that, for any n, $x + \mathfrak{a}^n M$ meets N. Since the $x + \mathfrak{a}^n M$ form a basis for the neighborhoods of x, it follows that x is in the closure N^* of N. Thus the assertion is proved.

(16.4) COROLLARY: *For a submodule N of M, the $\mathfrak{a}$-adic topology of M/N is T_0 if and only if N is a closed subset in the $\mathfrak{a}$-adic topology of M.*

Proof: The $\mathfrak{a}$-adic topology of M/N is T_0 if and only if

$$\bigcap (\mathfrak{a}^n M + N)/N = 0$$

by (16.1), or equivalently, $\bigcap (\mathfrak{a}^n M + N) = N$, which proves the assertion.

We note that, when N is a submodule of M, the $\mathfrak{a}$-adic topology of N may be different from the topology of N as a subspace of M. Hence the following theorem is really noteworthy:

(16.5) THEOREM: *If M is a Noetherian module, then for any submodule N of M, the $\mathfrak{a}$-adic topology of N coincides with the topology of N as a subspace of M with the $\mathfrak{a}$-adic topology.*

Proof: By virtue of (3.17), we may assume that R is Noetherian. It is obvious that $\mathfrak{a}^n N \subseteq \mathfrak{a}^n M \cap N$. The lemma of Artin-Rees (3.7) implies that $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N) \subseteq \mathfrak{a}^{n-r}N$, thus we prove the assertion.

On the other hand, it should be remarked that:

(16.6) *Let R^* be the ring $R \oplus M$ in the principle of idealization. Then the $\mathfrak{a}$-adic topology of M coincides with the topology of M as a subspace of R^* with $(\mathfrak{a} \oplus M)$-adic topology (which is equivalent to $\mathfrak{a}R^*$-adic topology).*

The proof is straightforward and we omit it.

Now we consider semi-local rings. On a semi-local ring which may not be Noetherian, we define the Jacobson-radical-adic topology to be the *natural topology*. When M is a finite module over a semi-local ring R with Jacobson radical $\mathfrak{m}$, then the $\mathfrak{m}$-adic topology of M is defined to be the *natural topology* of M. This definition is justified by (16.5).

(16.7) THEOREM: *Assume that M is a finite module over a semi-local ring R with Jacobson radical $\mathfrak{m}$. Then an arbitrary submodule N of M is a closed subspace of M and $N = \bigcap_n (N + \mathfrak{m}^n M)$.*

Proof: Since M/N is Noetherian, it is a T_0-space by (4.2), and we prove the assertion by (16.3), (16.4) and (16.5).

(16.8) THEOREM: *Assume that a semi-local ring R' is a finite module over a semi-local ring R. Then the topology of R' as a semi-local ring coincides with that of R' as a finite R-module. If, furthermore, R' contains R (whence R' dominates R), then R is a closed subspace of R'.*

Proof: Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the Jacobson radicals of R and R' respectively. $R'/\mathfrak{m}R'$ is a finite R-module, hence is a finite $R/\mathfrak{m}$-module. Therefore, there exists a natural number n such that $\mathfrak{m}'^n \subseteq \mathfrak{m}R'$, which shows that $\mathfrak{m}'^{ns} \subseteq \mathfrak{m}^s R' \subseteq \mathfrak{m}'^s$, and the first assertion is proved. The last assertion follows from the first one by virtue of (16.7).

EXERCISES: *1.* We say that $(R, \mathfrak{a})$ is a *Zariski ring* if R is Noetherian ring

associated with the $\mathfrak{a}$-adic topology ($\mathfrak{a}$ being an ideal of R) such that every ideal of R is a closed set. Prove that an $\mathfrak{a}$-adic Noetherian ring R is a Zariski ring if and only if every element a of R such that $a - 1 \in \mathfrak{a}$ is a unit in R.

2. Prove that if $(R, \mathfrak{a})$ is a Zariski ring and if $\mathfrak{b}$ is an ideal of R contained in $\mathfrak{a}$, then $(R, \mathfrak{b})$ is also a Zariski ring.

3. Generalize (16.7) to the case of a Zariski ring R.

4. Adapt (16.8) to the case of a Zariski ring and prove it.

5. Let $(R, \mathfrak{a})$ be a Zariski ring and let $x_1, \ldots, x_r$ be indeterminates. Prove that $(R[|x|], \mathfrak{a}R[[x]] + \sum x_i R[[x]])$ is a Zariski ring.

6. Let M be a module over a ring R with an ideal $\mathfrak{a}$. Assume that the $\mathfrak{a}$-adic topology of M is T_0. Set $\mathfrak{b} = (\mathfrak{a} + (0:M))/(0:M)$. Prove that (1) the $\mathfrak{a}$-adic topology of M coincides with the $\mathfrak{b}$-adic topology of M and (2) the $\mathfrak{b}$-adic topology of $R/(0:M)$ is T_0.

7. Let M be a module over a ring R with an ideal $\mathfrak{a}$. Let N be a submodule of M which is closed in the $\mathfrak{a}$-adic topology of M. Prove that $N:M$ is closed in the $\mathfrak{a}$-adic topology of R.

17. Completions

This section is concerned with completions of semi-local rings and with completions of finite modules over semi-local rings. But we begin with a case a bit more general so that the readers can see some general facts in the case of semi-local rings which may not be Noetherian.

Let R be a ring and let M be an R-module. Assume that M is a metric space with a distance function $r(x, y)$ such that (1) $r(x, y) = r(x - y, 0)$ for any $x, y \in M$, (2) for any positive real number ϵ, the set U_ϵ of x such that $r(x, 0) < \epsilon$ forms an R-submodule of M.

We note the following fact which follows immediately from the above condition.

(17.1) *If* $r(a, b) > r(c, d)$, *then* $r(a, b) = r(a + c, b + d)$.

With this metric, we can discuss completions as usual. Namely: A sequence $\{c_n\}$ of elements $c_n (n = 1, 2, \ldots)$ of M is called a *Cauchy sequence* if for any given positive number ϵ, there is a natural number N such that, for any m and n which are greater than N, $r(c_m, c_n) < \epsilon$. An element a is said to be a *limit* of a Cauchy sequence $\{c_n\}$ if

$$\lim_{n\to\infty} r(c_n, a) = 0;$$

if such an a exists for a given $\{c_n\}$, then a is unique and is denoted by $\lim c_n$. M is said to be *complete* if every Cauchy sequence in M has a limit in M. An R-module M^*, having the following properties, is called a *completion* of M: (1) M^* is a metric space with a distance

function r^* such that $r^*(x^*, y^*) \quad r^*(x^* \quad y^*, 0)$ for any $x^*, y^* \in M^*$ (2) M^* is complete, (3) M is a dense subspace of M^*, and (4) if x^* and y^* are limits of Cauchy sequences $\{x_n\}$ and $\{y_n\}$ respectively, then $r^*(x^*, y^*) = \lim_{n\to\infty} r(x_n, y_n)$.

We give one more definition concerning Cauchy sequences: A Cauchy sequence $\{c_n\}$ is called a *regular sequence* if $r(c_j, c_n) < \frac{1}{2}^n$ for any n and for any $j > n$. Then as a general fact in metric spaces, we have

(17.2) *For any Cauchy sequence* $\{c_n\}$ *in* M, *there is a regular sequence* $\{d_n\}$ *such that* $\lim r(c_n, d_n) = 0$.

Now we prove the existence of completions:

(17.3) THEOREM: *M has a completion M^* which is unique up to isomorphisms (with regards to topologies). The set U_ϵ^* of elements x^* of M^* such that $r^*(x^*, 0) < \epsilon$ forms an R-submodule of M^* and is the closure of U_ϵ in M^*. M^*/U_ϵ^* is naturally isomorphic to M/U_ϵ. If M is a ring and if the U_ϵ are ideals, then M^* is naturally a ring whose multiplication is such that* $(\lim c_n^*)(\lim d_n^*) = \lim(c_n^* d_n^*)$ *for any Cauchy sequences* $\{c_n^*\}$ *and* $\{d_n^*\}$ *in* M^*, *and the* U_ϵ^* *are ideals of* M^*.

Proof: Let C and C^* be the set of Cauchy sequences and regular sequences in M respectively. In C, we introduce the following operations: $\{c_n\} + \{c_n'\} = \{c_n + c_n'\}$, $a\{c_n\} = \{ac_n\} (a \in R)$, and when M is a ring (as above), $\{c_n\}\{c_n'\} = \{c_n c_n'\}$. Thus C becomes an R-module; when M is a ring, C becomes a ring. Let $\mathfrak{n}$ be the set of Cauchy sequences which have zero as limits. Then $\mathfrak{n}$ is a submodule of C; when M is a ring, $\mathfrak{n}$ is an ideal. We shall show that $C/\mathfrak{n}$ is a completion of M, identifying an element a of M with the class of Cauchy sequences which have a as the limit. We define a function $r^*(x^*, y^*)$ $(x^*, y^* \in C/\mathfrak{n})$ to be $\lim_{n\to\infty} r(x_n, y_n)$ with representatives $\{x_n\}$, $\{y_n\}$ of x^*, y^*. By virtue of (17.1), we see that $r^*(x^*, y^*) = r(x_n, y_n)$ for sufficiently large n except for the case where $x^* = y^*$. With this r^*, $C/\mathfrak{n}$ becomes a metric space as is easily seen. Furthermore, if x^* is a class in $C/\mathfrak{n}$ containing $\{c_n\}$, then $x^* = \lim c_n$ in this topology. Thus M is dense in $C/\mathfrak{n}$. Let $\{x_n^*\}$ be a Cauchy sequence in $C/\mathfrak{n}$. Let $\{x_{ni}\}$ be regular sequences in M such that $x_n^* = \lim x_{ni}$. Then by the regularity of the $\{x_{ni}\}$, the sequence $\{x_{nn}\}$ becomes a Cauchy sequence, hence has a limit x^* in $C/\mathfrak{n}$. Then we see that x^* is a limit of the sequence $\{x_n^*\}$. Thus $C/\mathfrak{n}$ is a completion of M. The uniqueness of M^* is rather obvious, because elements of M^* must be in one-one correspondence

with elements of $C/\mathfrak{n}$. The other assertions in our theorem have now become easy and we omit the details.

(17.4) THEOREM: *Assume that* $\mathfrak{a}$ *is an ideal of* R *and that the metric of* M *is given by the* $\mathfrak{a}$*-adic topology (by* (16.1)*). If* $\mathfrak{a}$ *has a finite basis, then the topology of the completion* M^* *is the* $\mathfrak{a}$*-adic topology.*

Proof: It is sufficient, by virtue of (17.3), to show that the closure N_n^* of $\mathfrak{a}^nM$ in M^* is $\mathfrak{a}^nM^*$. Let x^* be an arbitrary element of N_n^*. Then $x^* = \lim x_i$ with $\{x_i\}$ such that $x_1 \in \mathfrak{a}^nM$ and such that $x_i - x_{i+1} \in \mathfrak{a}^{n+i}M = \mathfrak{a}^n(\mathfrak{a}^iM)$. Let $a_1, \ldots, a_t$ be a basis for $\mathfrak{a}^n$. Then $x_i - x_{i+1} = \sum_j a_j b_{ji}$ with $b_{ji} \in \mathfrak{a}^iM$. For each j, the series $\sum_i b_{ji}$ is convergent (*i.e.*, $\{\sum_{i=1}^t b_{ji}\}$ is a Cauchy sequence) and express an element b_j^* of M^*. Then we see that $x^* = \sum a_j b_j^*$, which is in $\mathfrak{a}^nM^*$. Thus $N_n^* \subseteq \mathfrak{a}^nM^*$. Since the converse inclusion is obvious, the proof is complete.

(17.5) THEOREM: *Assume that the* $\mathfrak{a}$*-adic topology of* R *is* T_0 *and that* $\mathfrak{a}$ *has a finite basis* $a_1, \ldots, a_r$. *Let* $x_1, \ldots, x_r$ *be indeterminates and consider the formal power series ring* $R[[x]]$. *Then the completion* R^* *of* R *is (isomorphic to) the ring* $R[[x]]/\mathfrak{n}^*$, *where* $\mathfrak{n}^*$ *is the closure of the ideal* $\mathfrak{n} = \sum (x_i - a_i)R[[x]]$ *in* $R[[x]]$ *with the* $(\mathfrak{n} + \mathfrak{a}R[[x]])$*-adic topology (= the* $(\mathfrak{a}R[[x]] + \sum x_i R[[x]])$*-adic topology).*

Proof: We consider the map ϕ from $R[[x]]$ into R^* such that if $f = \sum f_i(x) \in R[[x]]$ ($f_i(x)$ being homogeneous form of degree i) then $\phi(f) = \sum f_i(a)$. Then we see that ϕ is a homomorphism from $R[[x]]$ onto R^* and that the kernel $\mathfrak{n}'$ of ϕ contains $x - a$, hence $\mathfrak{n}$. $f = \sum f_i(x)$ is in $\mathfrak{n}'$ if and only if $\sum f_i(a) = 0$. Let $f_u(x)$ be the leading form of f. Then $\sum f_i(a) = 0$ implies that $f_u(a) \in \mathfrak{a}^{u+1}$, and there is a homogeneous form $h_{u+1}(x)$ of degree $u + 1$ such that $f_u(a) = h_{u+1}(a)$. $f - f_u(x) + h_{u+1}(x)$ has leading degree greater than u and $f \equiv f - f_u(x) + h_{u+1}(x)$ modulo $\mathfrak{n}$. Thus, repeating the same, we see that if $f \in \mathfrak{n}'$, then $f \in \mathfrak{n} + (\sum x_i R[[x]])^n$ for any n. Conversely, if $f \in \bigcap(\mathfrak{n} + (\sum x_i R[[x]])^n)$, then we see that $\sum f_i(a) \in \bigcap_n \mathfrak{a}^n = 0$. Thus we have $\mathfrak{n}' = \bigcap_n (\mathfrak{n} + (\sum x_i R[[x]])^n) = \bigcap_n (\mathfrak{n} + \mathfrak{a}^n R[[x]]) = \mathfrak{n}^*$.

(17.6) COROLLARY: *Assume that* R *is a semi-local ring with Jacobson radical* $\mathfrak{m}$ *and assume that elements* $a_1, \ldots, a_r$ *generate an ideal which has* $\mathfrak{m}$ *as its radical. Then the completion* R^* *of* R *is a semi-local ring and is (isomorphic to) the ring*

$$R[[x_1, \ldots, x_r]]/(\sum (x_i - a_i)R[[x]]),$$

where the x_i are indeterminates. The topology of R^* as the completion of R coincides with that of R^* as a semi-local ring.

Proof: Set $\mathfrak{a} = \sum a_i R$. Then since the radical of $\mathfrak{a}$ is $\mathfrak{m}$, the $\mathfrak{a}$-adic topology is equivalent to the $\mathfrak{m}$-adic topology. Therefore we can apply (17.4) and (17.5). Since $R[[x]]$ is a semi-local ring by (15.4), every ideal of $R[[x]]$ is closed, whence we have $R^* = R[[x]]/(\sum (x_i - a_i)R[[x]])$ by (17.5). The coincidence of topology follows from (17.4).

Another important fact concerning the completions of semi-local rings is:

(17.7) THEOREM: *Let $(R, \mathfrak{p}_1, \ldots, \mathfrak{p}_r)$ be a semi-local ring. Then the completion R^* of R is the direct sum of completions R_i^* of local rings $R_i = R_{\mathfrak{p}i}$.*

Proof: Let $\mathfrak{m}$ be the Jacobson radical of R, *i.e.*, $\mathfrak{m} = \bigcap_i \mathfrak{p}_i$. Then, for each natural number n, $R/\mathfrak{m}^n$ is the direct sum of $R/\mathfrak{p}_i^n$ and there are $e_{i,n} \in R$ such that $1 - \sum_i e_{i,n} \in \mathfrak{m}^n$, $e_{i,n} \in \mathfrak{p}_j^n$ if $i \neq j$, hence $1 - e_{i,n} \in \mathfrak{p}_i^n$. Then for each i, $e_{i,n} - e_{i,n+1} \in \mathfrak{p}_1^n \cap \cdots \cap \mathfrak{p}_r^n = \mathfrak{m}^n$ and therefore the sequence $\{e_{i,n}\}$ has a limit e_i in R^*. Since

$$\lim \sum_i e_{i,n} = 1,$$

we have $\sum e_i = 1$. Since $e_{i,n}e_{j,n} \in \mathfrak{m}^n (i \neq j)$, we have $e_i e_j = 0$ if $i \neq j$. Hence we have $e_i^2 = e_i$. Thus R^* is the direct sum of ideals R^*e_i, which are rings with identities e_i. We shall prove now that R^*e_i is (isomorphic to) the completion of R_i. Let $\{c_n\}$ be a Cauchy sequence in R_i such that $c_n - c_{n+1} \in \mathfrak{p}_i^n R_i$. Since $R/\mathfrak{p}_i^n = R_i/\mathfrak{p}_i^n R_i$ for any n, there is a sequence $\{c_n'\}$ of elements c_n' of R such that (c_n modulo $\mathfrak{p}_i^n R_i$) = (c_n' modulo $\mathfrak{p}_i^n$) for every n. Then the sequence $\{c_n' e_{i,n}\}$ is a Cauchy sequence in R and $\lim c_n' e_{i,n} = \lim c_n' e_{i,n}^2 = e_i(\lim c_n' e_{i,n})$. Hence the limit of $\{c_n' e_{i,n}\}$ is in R^*e_i. It is easy to see that the map $\lim c_n \to \lim c_n' e_{i,n}$ gives a one-one correspondence between the completion R_i^* and R^*e_i. Then we see easily that R_i^* is isomorphic to R^*e_i.

Now we go back to the completions of modules:

(17.8) THEOREM: *Assume that R is a semi-local ring and that M is a finite R-module. Let R^* be the completion of R. Then $M \otimes_R R^*$ is the completion of M, whose topology as a finite R^*-module coincides with its topology as the completion of M.*

Proof: Let $\mathfrak{m}$ be the Jacobson radical of R. Then $\mathfrak{m}R^*$ is the Jacobson radical of R^* by (17.6). Furthermore $R^*/\mathfrak{m}^nR^* = R/\mathfrak{m}^nR$. Now, $(M \otimes R^*)/\mathfrak{m}^n(M \otimes R^*) = (M/\mathfrak{m}^nM) \otimes (R^*/\mathfrak{m}^nR^*) = M/\mathfrak{m}^nM$. Since $\bigcap \mathfrak{m}^nM = 0$, we see that $M \otimes R^*$ contains M (by the identification $m = m \otimes 1$ for any $m \in M$), and furthermore that $\mathfrak{m}^n(M \otimes R^*) \cap M = \mathfrak{m}^nM$. This shows that M is a subspace of $M \otimes R^*$. An arbitrary element c^* of $M \otimes R^*$ can be expressed as $\sum m_i \otimes r_i^*$ with $m_i \in M$ and $r_i^* = \lim_n r_{i,n}$ with $r_{i,n} \in R$. Then c^* is the limit of $\{\sum m_i r_{i,n}\}$ as is easily seen. Thus M is dense in $M \otimes R^*$. Let $\{c_n^*\}$ be a regular sequence in $M \otimes R^*$. Let $u_1, \ldots, u_t$ be a basis for M. Since $(M \otimes R^*)/\mathfrak{m}^n(M \otimes R^*) = M/\mathfrak{m}^nM$, there is a sequence $\{c_n\}$ in M such that $c_n^* - c_n \in \mathfrak{m}^n(M \otimes R^*)$. $c_{n+1} - c_n$ is in $\mathfrak{m}^nM$, hence is expressed as $\sum u_i m_{in} (m_{in} \in \mathfrak{m}^n)$. For each i, $\sum m_{in}$ has limit r_i^* in R^*. Furthermore, we see that $\sum u_i \otimes r_i^*$ is the limit of the sequence $\{c_n^*\}$. Thus $M \otimes R^*$ is complete.

(17.9) COROLLARY: *Let $\mathfrak{a}$ be an ideal of a semi-local ring R. Let R^* be the completion of R. Then the completion of $\mathfrak{a}$ is $\mathfrak{a}R^*$ and $\mathfrak{a}R^*$ is isomorphic to $\mathfrak{a} \otimes R^*$. Furthermore $\mathfrak{a}R^* \cap R = \mathfrak{a}$, and $R^*/\mathfrak{a}R^*$ is the completion of $R/\mathfrak{a}$.*

Proof: The first assertion follows from (16.5), hence the second assertion follows from (17.8). Since $\mathfrak{a}$ is a closed set by (16.7) and since $\mathfrak{a}R^*$ is its closure in R^*, we see that $\mathfrak{a}R^* \cap R = \mathfrak{a}$. The completion of $R/\mathfrak{a}$ is $(R/\mathfrak{a}) \otimes R^*$, which is obviously $R^*/\mathfrak{a}R^*$.

Similarly, we have for modules:

(17.10) COROLLARY: *Let N be a submodule of a finite module M over a semi-local ring R. Then the closure N^* of N in the completion M^* of M is the completion of N and we have $N^* \cap M = N$. Furthermore, M^*/N^* is the completion of M/N.*

If we identify M^* with $M \otimes R^*$, then N^* is surely identified with $N \otimes R^*$ in $M \otimes R^*$ as is easily seen. That N^* is the completion of N implies that the usual tensor product $N \otimes R^*$ is isomorphic to the submodule $N \otimes R^*$ in $M \otimes R^*$. Hence we have

(17.11) COROLLARY: *If R is a semi-local ring, then $\otimes_R R^*$ is exact.*

(17.12) *Let $(R, \mathfrak{p}_1, \ldots, \mathfrak{p}_r)$ be a semi-local ring and let R^* be the completions of R. Then we have* altitude R^* = altitude R.

Proof: altitude $R = \max\{\text{altitude } R_{\mathfrak{p}_i}\}$. On the other hand, R^* is the direct sum of completions of $R_{\mathfrak{p}_i}$. Therefore it is sufficient to prove the assertion in the case where R is a local ring with maximal

ideal $\mathfrak{m}$ $\mathfrak{p}_i$. We prove the assertion by induction on altitude R^*. If altitude R^* 0, then R^* has discrete topology, whence R R^*, and altitude R^* altitude R in this case. Assuming that altitude $R^* > 0$, let $x_1, \ldots, x_s$ be a system of parameters of R. Then the x_i generate an ideal which is primary to $\mathfrak{m}R^*$ in R^*. Therefore we see that altitude $R^* \leq$ altitude R and that there is an element x_i, say x_1, such that R^*/x_1R^* has altitude less than altitude R^*, whence altitude R^*/x_1R^* = altitude $R^* - 1$ by (9.7). Since R^*/x_1R^* is the completion of R/x_1R, we see that altitude R^*/x_1R^* = altitude R/x_1R by our induction assumption. Thus we have altitude R^* = altitude $R^*/x_1R^* + 1$ = altitude $R/x_1R + 1 \geq$ altitude R, whence we have altitude R^* = altitude R.

(17.13) COROLLARY: *Let R be a local ring and let R^* be the completion of R. Then any system of parameters of R is a system of parameters of R^*.*

EXERCISES: *1.* Prove that the completion of a Zariski ring is a Zariski ring.

2. Confirm that (17.9), (17.10) and (17.11) can be generalized to the case of Zariski rings without any substantial change of proofs.

3. Let R be a ring with an ideal $\mathfrak{a}$ and let M be an R-module. Assume that the $\mathfrak{a}$-adic topologies of M and R are T_0, hence metric. Prove that the completion M^* is naturally a module over the completion R^* of R. Prove furthermore that if $\mathfrak{a}$ has a finite basis, then the topology of M^* is the $\mathfrak{a}R^*$-adic topology.

18. Exact tensor products

We saw in Section 17 that if R^* is the completion of a semi-local ring R, then $\otimes_R R^*$ is exact. Therefore, we prove here some general properties of exact tensor products, which can be applied to the case of semi-local rings immediately.

(18.1) THEOREM: *Let R be a ring and let R^* be a ring which is an R-module, and such that $\otimes_R R^*$ is exact.*

Let M be an R-module. Then we have the following, where N_i are submodules of M and $\mathfrak{a}$ is an ideal of R:

(1) $(N_1 \cap \cdots \cap N_r) \otimes R^* = (N_1 \otimes R^*) \cap \cdots \cap (N_r \otimes R^*)$.

(2) $(N_1{:}N_2) \otimes R^* = ((N_1 \otimes R^*){:}(N_2 \otimes R^*))$, *provided that N_2 has a finite basis.*

(3) $(N_1{:}\mathfrak{a}) \otimes R^* = (N_1 \otimes R^*){:}\mathfrak{a}R^*$, *provided that $\mathfrak{a}$ has a finite basis.*

(4) *If an element a of R is not a zero divisor with respect to N_1, then a is not a zero divisor with respect to $N_1 \otimes R^*$.*

(5) *If elements* $u_1, \ldots, u_r$ *of* M *are linearly independent over* R, *then* $u_1 \otimes 1, \ldots, u_r \otimes 1$ *in* $M \otimes R^*$ *are linearly independent over* R^*.

Proof: In order to prove (1), we have only to prove the case where $r = 2$. From $(N_1 + N_2)/N_1 = N_2/(N_1 \cap N_2)$, we have $(N_2 \otimes R^*)/(N_1 \cap N_2) \otimes R^* = ((N_1 + N_2) \otimes R^*)/(N_1 \otimes R^*) = (N_2 \otimes R^*)/((N_1 \otimes R^*) \cap (N_2 \otimes R^*))$, which proves (1). Since N_2 has a finite basis, in order to prove (2), we may assume that $N_2 = bR$ with an element $b \in N_2$, by virtue of (1) above and (1.2). The map ϕ defined by $\phi(x \text{ modulo } N_1{:}bR) = (bx \text{ modulo } N_1 \cap bR)$ is an isomorphism from $R/(N_1{:}bR)$ onto $bR/(N_1 \cap bR)$ by (1.5). Therefore $R^*/(N_1{:}bR)R^* \overset{\phi \otimes R^*}{\cong} (b \otimes R^*)/((N_1 \cap bR) \otimes R^*) = (b \otimes R^*)/((N_1 \otimes R^*) \cap (b \otimes R^*)) \overset{\phi^{*-1}}{\cong} R^*/((N_1 \otimes R^*){:}(b \otimes R^*))$, where ϕ^* is defined similarly as ϕ. Hence we have (2). (3) is proved similarly as (2), using M instead of R in the above proof. That a is not a zero divisor with respect to N_1 implies $[0{:}aR]N_1 = 0$, hence by (3) applied to $N_1 = M$ we have $[0{:}aR^*]N_1 \otimes R^* = 0$, which proves (4). As for (5), $u_i \otimes 1$ in $(\sum u_i R) \otimes R^*$ are linearly independent, hence the exactness implies (5).

(18.2) COROLLARY: *Let* M *be a finite module over a semi-local ring* R *and let* M^* *and* R^* *be the completions of* M *and* R *respectively. Then we have* op. altitude M^* = op. altitude M.

Proof: $0{:}M^* = (0{:}M)R^*$ by (2) in (18.1), and $R^*/(0{:}M^*)$ is the completion of $R/(0{:}M)$ by (17.9). Therefore we have the assertion by (17.12).

(18.3) THEOREM: *With the same* R *and* R^* *as in* (18.1), *assume furthermore that there is no ideal* $\mathfrak{a}$ *of* R *such that* $\mathfrak{a} \neq R$ *and* $\mathfrak{a}R^* = R^*$. *Then* $R \subseteq R^*$ *and, for any ideal* $\mathfrak{a}$ *of* R, *it holds that* $\mathfrak{a}R^* \cap R = \mathfrak{a}$.

Proof: Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R. Assume that $\mathfrak{b}$ has a finite basis. If $\mathfrak{b}R^* \subseteq \mathfrak{a}R^*$ then $R^* = \mathfrak{a}R^*{:}\mathfrak{b}R^* = (\mathfrak{a}{:}\mathfrak{b})R^*$, whence $\mathfrak{b} \subseteq \mathfrak{a}$. Applying this to $\mathfrak{a} = 0$ and $\mathfrak{b} = bR$ with $b \in 0{:}R^*$ (as an R-module), we have $\mathfrak{b} = 0$ and $R \subseteq R^*$. Applying the same to $\mathfrak{b} \subseteq \mathfrak{a}R^* \cap R$, we have $\mathfrak{a}R^* \cap R \subseteq \mathfrak{a}$, whence $\mathfrak{a}R^* \cap R = \mathfrak{a}$.

(18.4) *With the same* R *and* R^* *as in* (18.1), *assume furthermore that* $R \subseteq R^*$ *and that* $\mathfrak{a}R^* \cap R = \mathfrak{a}$ *for any ideal* $\mathfrak{a}$ *of* R. *Then* (1) *the total quotient ring* K *of* R *is naturally a subring of the total quotient ring* K^* *of* R^*, *and* (2) *for any ideal* $\mathfrak{a}$ *of* R, $K \cap \mathfrak{a}R^* = \mathfrak{a}$, *hence in particular* $K \cap R^* = R$.

Proof: (1) follows from (1) in (18.1). $a/b \in K \cap \mathfrak{a}R^*$ ($a, b \in R$, b is a non-zero-divisor) implies that $a \in b\mathfrak{a}R^*$, hence $a \in b\mathfrak{a}R^* \cap R = b\mathfrak{a}$, and we have $a/b \in \mathfrak{a}$. This proves that $K \cap \mathfrak{a}R^* \subseteq \mathfrak{a}$, and we have (2).

(18.5) *With the same R, R^* and M as in* (18.1), *assume furthermore the same assumptions as in* (18.4) *above. Then the map ϕ such that $\phi(m) = m \otimes 1$ ($m \in M$) gives an isomorphism from M into $M \otimes R^*$.*

Proof: For a fixed $m \in M$, $mr \to mr \otimes 1$ ($r \in R$) gives an isomorphism from mR into $mR \otimes R^*$, hence the exactness proves the assertion.

Next we give some sufficient conditions for a tensor product to be exact.

(18.6) *Let R be a ring and let R^* be a ring which is an R-module. If, for any ideal $\mathfrak{a}$ of R, the natural map from $\mathfrak{a} \otimes R'$ onto $\mathfrak{a}R^*$ is an isomorphism, then $\otimes_R R^*$ is exact.*

Proof: Let M be a finite R-module and let N be a finite R-module contained in M. We shall prove that $N \otimes R^* \subseteq M \otimes R^*$. Let $u_1, \ldots, u_r$ be a basis for M, and we set $N_i = (\sum_1^{i-1} u_j R) + N$. If $N_{i-1} \otimes R^* \subseteq N_i \otimes R^*$ for any i, then the assertion is proved. Thus we may assume that $u_1, \ldots, u_{r-1} \in N$. Let F be a free R-module with free base $U_1, \ldots, U_r$, and let ϕ be the homomorphism from F onto M such that $\phi(U_i) = u_i$. Set $G = \sum_1^{i-1} RU_i$, $H = \phi^{-1}(N)$, $K = \phi^{-1}(0)$. Then, with $\mathfrak{a} = N:M = N:u_rR$, $H = G \oplus \mathfrak{a}U_r$. Therefore $H \otimes R^* = (G \otimes R^*) \oplus (\mathfrak{a}U_r \otimes R^*)$, $F \otimes R^* = (G \otimes R^*) \oplus (U_rR \otimes R^*)$. Since, by our assumption, $\mathfrak{a}U_r \otimes R^* \subseteq U_rR \otimes R^*$, we have $H \otimes R^* \subseteq F \otimes R^*$. Hence $K \otimes R^*$ in $H \otimes R^*$ coincides with $K \otimes R^*$ in $F \otimes R^*$, which proves that $N \otimes R^* = (H \otimes R^*)/(K \otimes R^*) \subseteq (F \otimes R^*)/(K \otimes R^*) = M \otimes R^*$. Thus we complete the proof.

(18.7) THEOREM: *Assume that R and R^* are Noetherian rings such that R^* is an R-module. Let ϕ be the homomorphism from R into R^* such that $\phi(a) = a \cdot 1$ (in R^*). Let $\mathfrak{M}^*$ be the set of maximal ideals of R^* and let $\mathfrak{M}$ be the set of prime ideals $\mathfrak{m}$ of R such that $\mathfrak{m} = \phi^{-1}(\mathfrak{m}^*)$ with $\mathfrak{m}^* \in \mathfrak{M}^*$. Then $\otimes_R R^*$ is exact if and only if the following is true: If $\mathfrak{q}$ is a primary ideal with prime divisor $\mathfrak{m} \in \mathfrak{M}$ and if b is an element of R such that $\mathfrak{q}:bR = \mathfrak{m}$, then $\mathfrak{q}R^*:bR^* = \mathfrak{m}R^*$.*

Proof: The *only if* part is obvious by (18.1). We assume that the condition holds good. We remark first that the condition is carried

to any pairs $(R_{\mathfrak{m}}, R^*_{\mathfrak{m}^*})$ ($\mathfrak{m} = \phi^{-1}(\mathfrak{m}^*)$, $\mathfrak{m}^* \in \mathfrak{M}^*$) and also to $(R/\mathfrak{a}, R^*/\mathfrak{a}R^*)$ for any ideal $\mathfrak{a}$ of R. Let M be a finite R module and let N be a submodule of M. Let K be the kernel of the map $f \otimes R^*$ from $N \otimes R^*$ into $M \otimes R^*$. It is sufficient to prove that $K = 0$. Applying (8.10) to K, we have only to prove the assertions for such pairs $(R_{\mathfrak{m}}, R^*_{\mathfrak{m}^*})$. Thus we may assume that R and R^* are local rings with maximal ideals $\mathfrak{m}$ and $\mathfrak{m}^*$ and that $\mathfrak{m} = \phi^{-1}(\mathfrak{m}^*)$. (1) Assume at first that $\mathfrak{m}$ is nilpotent. In order to prove that $K = 0$, we may assume that N is an ideal and that $M = R$ by (18.6). We use the induction on length R. If length $R = 1$, then R is a field, and the assertion is obvious. Assuming that length $R > 1$, let b be an element of N such that length $bR = 1$, *i.e.*, $0:bR = \mathfrak{m}$. By our induction assumption, $\otimes_{R/bR}(R^*/bR^*)$ is exact, which means that the natural map from $(N/bR) \otimes (R^*/bR)$ into R^*/bR^* is an isomorphism. Therefore K is contained in $b \otimes R^*$. Since $0:bR^* = \mathfrak{m}R^*$, we have that both $b \otimes R^*$ and bR^* are faithful $R^*/\mathfrak{m}R^*$-modules, hence $K = 0$. Thus we have settled this case. (2) Now we prove the general case. By (1) above, we see that $\otimes_{R/\mathfrak{m}^n} R^*/\mathfrak{m}^n R^*$ is exact for any n, which implies that $(N/(\mathfrak{m}^n M \cap N)) \otimes (R^*/\mathfrak{m}^n R^*)$ is naturally contained in

$$(M/\mathfrak{m}^n M) \otimes (R^*/\mathfrak{m}^n R^*).$$

Therefore we see that K is contained in $(\mathfrak{m}^n M \cap N) \otimes R^*$ in $N \otimes R^*$. Since $\mathfrak{m}^n M \cap N \subseteq \mathfrak{m}^{n-r}N$ for an r and for any $n \geq r$ by the lemma of Artin-Rees, we see that $K \subseteq \bigcap_n \mathfrak{m}^n(N \otimes R^*)$, which must be zero because R^* is a local ring. Thus $K = 0$, which completes the proof.

(18.8) COROLLARY: *Assume that a Noetherian ring R is dominated by a Noetherian ring R^* and that for any maximal ideal $\mathfrak{m}$ of R the ideal $\mathfrak{m}R^*$ is a maximal ideal of R^*. Then $\otimes_R R^*$ is exact if and only if $\mathfrak{q}R^* \cap R = \mathfrak{q}$ for any primary ideal $\mathfrak{q}$ of R such that the radical of $\mathfrak{q}$ is a maximal ideal.*

In particular, if a semi-local ring R is a dense subspace of a semi local ring R', then $\otimes_R R'$ is exact.

We note that this (18.8) gives another proof of (17.11). Furthermore, as an immediate consequence of (18.8), we have the following corollary by virtue of (6.17).

(18.9) COROLLARY: *Let $x_1, \ldots, x_n$ be algebraically independent*

elements over a Noetherian ring R. Then $\otimes_R R\langle x\rangle$ is exact. (Cf. Exercise 2 below).

(18.10) *Let R and R^* be rings such that R^* is an R-module and such that $\otimes_R R^*$ is exact. Let ϕ be the natural homomorphism from R into R^* ($\phi(r) = r\cdot 1$ with $1 \in R^*$). Let $\mathfrak{a}$ be an ideal of R and let S and S^* be multiplicatively closed subsets of R and R^* respectively such that $\phi(S) \subseteq S^*$ and such that $S \cap \mathfrak{a} = S^* \cap \mathfrak{a}R^* = \text{empty}$. Set $R' = R_S/\mathfrak{a}R_S$ and $R'' = R^*_{S^*}/\mathfrak{a}R^*_{S^*}$. Then $\otimes_{R'} R''$ is exact.*

Proof: If M is an $R/\mathfrak{a}$-module, then M is an R-module and

$$M \otimes_{R/\mathfrak{a}} (R^*/\mathfrak{a}R^*) = M \otimes_R R^*.$$

Therefore we see easily that $\otimes_{R/\mathfrak{a}} R^*/\mathfrak{a}R^*$ is exact. Hence, we may assume that $\mathfrak{a} = 0$. Since $\otimes_{R^*} R''$ is exact by (6.18), we see that $\otimes_R R''$ is exact. If M is an R'-module, then M is an R-module and $M \otimes_{R'} R'' = M \otimes_R R''$, and therefore the assertion is proved easily.

(18.11) THEOREM: *Let R and R^* be Noetherian rings such that R^* is an R-module and such that $\otimes_R R^*$ is exact. Let $\mathfrak{a}$ be an ideal of R and let $\mathfrak{p}^*$ be a prime ideal of R^*. Then $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{a}R^*$ if and only if there is a prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ such that $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{p}R^*$. $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{a}R^*$ if and only if there is a minimal prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ such that $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{p}R^*$.*

Proof: Assume that $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{p}R^*$ with a prime divisor $\mathfrak{p}$ of $\mathfrak{a}$. Then there are elements $b \in R$ and $c^* \in R^*$ such that $\mathfrak{p} = \mathfrak{a}:bR$, $\mathfrak{p}^* = \mathfrak{p}R^*:c^*R^*$ by (8.8). Since $\mathfrak{p}R^* = \mathfrak{a}R^*:bR^*$ by (18.1), we have $\mathfrak{p}^* = (\mathfrak{a}R^*:bR^*):c^*R^* = \mathfrak{a}R^*:bc^*R^*$, and $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{a}R^*$. Conversely, assume that $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{a}R^*$. Let $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a shortest primary decomposition of $\mathfrak{a}$. Then $\mathfrak{a}R^* = \bigcap \mathfrak{q}_iR^*$, whence $\mathfrak{p}^*$ is a prime divisor of some $\mathfrak{q}_iR^*$, say, $\mathfrak{q}_1R^*$. Let $\mathfrak{p}$ be the prime divisor of $\mathfrak{q} = \mathfrak{q}_1$. We shall prove that $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{p}R^*$ by induction on length $R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$. We may assume that $\mathfrak{q} = 0$ by (18.10). If the length is 1, then the assertion is obvious because $\mathfrak{p} = \mathfrak{q}$. Let a be an element of $\mathfrak{p}$ such that $\mathfrak{p} = 0:aR$, and let $\mathfrak{q}' = aR_\mathfrak{p} \cap R$. Then there is an element d of R which is not in $\mathfrak{p}$ such that $d\mathfrak{q}' \subseteq aR$. Let $\mathfrak{q}_1^* \cap \cdots \cap \mathfrak{q}_s^*$ be a shortest primary decomposition of zero in R^* such that the prime divisor $\mathfrak{p}_i^*$ of $\mathfrak{q}_i^*$ is a prime divisor of $\mathfrak{p}R^*$ if and only if $i \leq t$. Since $\mathfrak{p} = 0:aR$, $\mathfrak{p}R^* = \bigcap(\mathfrak{q}_i^*:aR^*)$ by (18.1), whence by our assumption on the prime divisors $\mathfrak{p}R^* = \mathfrak{q}_1^*:aR^*) \cap \cdots \cap (\mathfrak{q}_t^*:aR^*)$. Let b^* be an arbitrary element of

$\mathfrak{q}_1^* \cap \cdots \cap \mathfrak{q}_t^*$. By our induction, the prime divisors of $\mathfrak{q}'R^*$ are $\mathfrak{p}_1^*, \ldots, \mathfrak{p}_t^*$, whence $b^* \in \mathfrak{q}'R^*$, and therefore $b^*d \in aR^*$, whence there exists an element c^* of R^* such that $b^*d = ac^*$.

$$c^* \in b^*dR^* : aR^* \subseteq (\mathfrak{q}_1^* \cap \cdots \cap \mathfrak{q}_t^*) : aR^* = \mathfrak{p}R^*.$$

Therefore $ac^* = 0$, whence $b^*d = 0$. Hence $b^* \in 0 : dR^* = (0 : dR)R^* = 0$, and $s = t$, which proves the assertion. Now we consider the last assertion. Assume that $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{a}R^*$. Then $\mathfrak{p}^*$ is a prime divisor of $\mathfrak{p}R^*$ with a prime divisor $\mathfrak{p}$ of $\mathfrak{a}$. The minimality of $\mathfrak{p}^*$ implies that $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{p}R^*$ and that $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$. Conversely, assume that $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$ and that $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{p}R^*$. Let $\mathfrak{p}^{**}$ be a minimal prime divisor of $\mathfrak{a}R^*$ such that $\mathfrak{p}^{**} \subseteq \mathfrak{p}^*$. Let ϕ be the natural homomorphism from R into R^* ($\phi(a) = a \cdot 1$ with $1 \in R^*$), and let $\mathfrak{p}'$ be $\phi^{-1}(\mathfrak{p}^{**})$. Then $\mathfrak{p}'$ is a prime ideal by (2.12) and $\mathfrak{p}'$ is contained in $\mathfrak{p}$ because $\mathfrak{p} = \phi^{-1}(\mathfrak{p}^*)$ (for, non-zero elements of $R/\mathfrak{p}$ are not zero divisors with respect to $R^*/\mathfrak{p}R^*$ by (18.1)). By the minimality of $\mathfrak{p}$, we have $\mathfrak{p}' = \mathfrak{p}$, whence $\mathfrak{p}^{**}$ is a prime divisor of $\mathfrak{p}R^*$, which implies that $\mathfrak{p}^{**} = \mathfrak{p}^*$ by the minimality of $\mathfrak{p}^*$ and by that $\mathfrak{p}^{**} \subseteq \mathfrak{p}^*$. Thus $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{a}R^*$.

We say that a module M over a ring R is *torsion-free* if every non-zero-divisor in R is not a zero divisor with respect to M.

(18.12) THEOREM: *Let R and R' be Noetherian rings such that R' is an R-module and such that $\otimes_R R'$ is exact. If M is a torsion-free R-module and if every prime divisor of zero in R is of height at most* 1, *then $M \otimes_R R'$ is a torsion-free R'-module.*

Proof: Let R^* and R'^* be the rings $R \oplus M$ and $R' \oplus (M \otimes R')$ respectively in the principle of idealization. If N is an R^*-module, then N is an R-module, and $N \otimes_R R'$ is naturally identified with $N \otimes_{R^*} (R' \otimes_R R^*) = N \otimes_{R^*} R'^*$. Therefore we see that $\otimes_{R^*} R'^*$ is exact. In order to prove (18.12), we may assume that M is a finite module. Assume that $a \in R'$ is a zero divisor with respect to $M \otimes R'$. Then a is a zero divisor in R'^*, and there is a prime divisor $\mathfrak{p}'^*$ of zero in R'^* such that $a \in \mathfrak{p}'^*$. (18.11) implies that there is a prime divisor $\mathfrak{p}^*$ of zero in R^* such that $\mathfrak{p}'^*$ is a prime divisor of $\mathfrak{p}^*R'^*$. Since $M^2 = 0$, we have $M \subseteq \mathfrak{p}^*$, and therefore $\mathfrak{p}^* = \mathfrak{p} \oplus M$ with a prime ideal $\mathfrak{p}$ of R. Similarly, $\mathfrak{p}'^* = \mathfrak{p}' \oplus (M \otimes R')$ with a prime ideal $\mathfrak{p}'$ of R'. Since M is torsion-free, we see that $\mathfrak{p}$ consists merely of zero

divisors, hence is a prime divisor of zero by our assumption on R. Since $R'^*/(M \otimes R') \cong R'$ and since $R^*/M \cong R$, the fact that $\mathfrak{p}'^*$ is a prime divisor of $\mathfrak{p}^*R'^*$ implies that $\mathfrak{p}'$ is a prime divisor of $\mathfrak{p}R'$. Since $\otimes_R R'$ is exact and since $\mathfrak{p}$ is a prime divisor of zero in R, we see that $\mathfrak{p}'$ is a prime divisor of zero in R' by (18.11), whence a is a zero divisor in R', which completes the proof.

Exercises: *1.* Assume that R, R^*, R^{**} are rings such that $\otimes_R R^*$ and $\otimes_{R^*} R^{**}$ are exact. Prove that $\otimes_R R^{**}$ is exact.

2. Let $x_1, \ldots, x_n$ be algebraically independent elements over a ring R. Prove that $\otimes_R R[x]$ and $\otimes_R R(x)$ are exact. (Hint: Prove first the exactness of $\otimes_R R[x]$ using the fact that $R[x]$ has a free base over R.)

3. Let R^* be a ring which is a module over a Noetherian ring R. Prove that $\otimes_R R^*$ is exact if $(\mathfrak{a}:b)R^* = \mathfrak{a}R^*:bR^*$ for any ideal $\mathfrak{a}$ and any element b of R.

4. Let $(R, \mathfrak{a})$ be a Zariski ring and let M be a finite R-module. Let S be the set of non-zero-divisors with respect to M and let N^* be the completion of a submodule N of M. Prove that $(M \otimes R_S) \cap N^* = N$, where, $M \otimes R_S$ and N^* are naturally imbedded in $M \otimes R_S^*$ (R^* being the completion of R).

5. Let $(R, \mathfrak{a})$ be a Zariski ring and let R^* be the completion of R. Let $\mathfrak{b}$ be an ideal of R. Prove that if $\mathfrak{b}R^*$ is principal then $\mathfrak{b}$ is principal. (Hint: $\mathfrak{b}/\mathfrak{b}\mathfrak{a} = \mathfrak{b}/\mathfrak{b}\mathfrak{a} \otimes R/\mathfrak{a} = \mathfrak{b}/\mathfrak{b}\mathfrak{a} \otimes R^*/\mathfrak{a}R^* = \mathfrak{b}R^*/\mathfrak{b}\mathfrak{a}R^*$.)

6. Prove that if the completion R^* of a Zariski ring $(R, \mathfrak{a})$ is a unique factorization ring, then R is also a unique factorization ring. (Hint: Let $\mathfrak{p}$ be an arbitrary prime ideal of height 1 in R and let S be the complement of $\mathfrak{p}$ in R. Then, show that $\mathfrak{p}R_S^*$ is principal and that every maximal prime divisor of $\mathfrak{p}R^*$ does not meet S. Then conclude that $\mathfrak{p}R^*$ has only prime divisors of height 1 and then that $\mathfrak{p}R^*$ is principal.)

7. Let R^* be a ring containing a ring R such that (a) $\otimes_R R^*$ is exact and (b) $\mathfrak{a}R^* \cap R = \mathfrak{a}$ holds for any ideal $\mathfrak{a}$ of R. Let M be an R-module. Prove that if $M \otimes R^*$ is a finite R^*-module then M is a finite R-module.

19. The theorem of transition

We say that the *theorem of transition* holds for rings R and R' if (1) R is dominated by R' and (2) if $\mathfrak{q}$ is a primary ideal in R such that the prime divisor of $\mathfrak{q}$ is a maximal ideal, say $\mathfrak{m}$, then

$$\text{length}_{R'} R'/\mathfrak{q}R'$$

is finite and it holds that

$$\text{length}_{R'} R'/\mathfrak{q}R' = (\text{length}_{R'} R'/\mathfrak{m}R')(\text{length}_R R/\mathfrak{q}).$$

(19.1) Theorem: *Let R and R' be Noetherian rings such that $R \leq R'$. Assume that, for any maximal ideal $\mathfrak{m}$ of R, the length of $R'/\mathfrak{m}R'$ is finite (i.e., the prime divisors of $\mathfrak{m}R'$ are all maximal). Then*

each of the followings is a necessary and sufficient condition for the validity of the theorem of transition for the rings R and R':

(a) *If $\mathfrak{q}$ is a primary ideal belonging to a maximal ideal $\mathfrak{m}$ in R and if $\mathfrak{q}:bR \neq \mathfrak{m}$ for an element b of R, then $\mathfrak{q}R':bR' = \mathfrak{m}R'$.*

(b) *$\otimes_R R'$ is exact.*

(c) *For any maximal ideal $\mathfrak{m}'$ of R', the theorem of transition holds for $R_{(\mathfrak{m}'\cap R)}$ and $R_{\mathfrak{m}'}$.*

(d) *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R, then $(\mathfrak{a}:\mathfrak{b})R' = \mathfrak{a}R':\mathfrak{b}R'$.*

Proof: We show first that the validity of the theorem of transition implies (a). Set $\mathfrak{q}' = \mathfrak{q} + bR$. Then length $R/\mathfrak{q}$ = length $R/\mathfrak{q}' + 1$, hence length $R'/\mathfrak{q}R'$ = length $R'/\mathfrak{q}'R'$ + length $R'/\mathfrak{m}R'$, which implies that length $R'/\mathfrak{m}R'$ = length $\mathfrak{q}'R'/\mathfrak{q}R'$ = length $bR'/(bR' \cap \mathfrak{q}R')$ = length $R'/(\mathfrak{q}R':bR')$, which implies that $\mathfrak{m}R' = \mathfrak{q}R':bR'$. This proof being reversible by induction on length $R/\mathfrak{q}$, we see the equivalence with (a). (a) implies (b) by (18.7). (b) implies (d) by (18.1), while (d) implies (a) obviously. Thus (a), (b) and (d) are equivalent. It is obvious that (c) implies the validity of the theorem of transition; the converse is also obvious except for the fact that $R^* = R_{(\mathfrak{m}\cap R)} \subseteq R^{**} = R_{\mathfrak{m}'}$, which is proved as follows: $\otimes_{R^*}R^{**}$ is exact by (b) and (18.10), whence (18.3) implies the inclusion relation.

(19.2) COROLLARY: *Assume that the theorem of transition holds for Noetherian rings R and R'.*

(1) *For any ideal $\mathfrak{a}$ of R, the theorem of transition holds for the rings $R/\mathfrak{a}$ and $R'/\mathfrak{a}R'$.*

(2) *Assume that S and S' are multiplicatively closed subsets of R and R' respectively such that every maximal ideal $\mathfrak{P}'$ with respect to S' in R' is a minimal prime divisor of $\mathfrak{P}R'$ for some maximal ideal $\mathfrak{P}$ with respect to S in R and conversely that if $\mathfrak{P}$ is maximal ideal with respect to S in R, then $\mathfrak{P}R'$ does not meet S'. Then the theorem of transition holds for the rings R_S and $R'_{S'}$.*

(3) *If R_S and $R'_{S'}$ in (2) are semi-local rings, then R_S is a subspace of $R'_{S'}$.*

Proof: We note first that $\otimes_R R'$ is exact by (19.1). Since $\mathfrak{a}R' \cap R = \mathfrak{a}$ by (18.3), the validity of (1) is obvious. $\otimes_{R_S} R'_{S'}$ is exact by (18.10). Therefore, by our assumption and by (18.3), R_S is a subring of $R'_{S'}$, hence R_S is dominated by $R'_{S'}$. Therefore (2) is proved

19.Hby ( ). (3) is easy because $\mathfrak{a}''R'_{S'} \cap R_S = \mathfrak{a}''$ for any ideal $\mathfrak{a}$ of R_S, hence in particular for the Jacobson radical $\mathfrak{a}$.

Exercise: Let R and R' be Noetherian rings such that R' is an R module. Assume that the following statements are true: (a) there is no maximal ideal of R which generates R' in R', (b) the natural image R^* of R in R' ($R^* = R/(0:R')$) is dominated by R' and (c) the condition (2) in the definition of the theorem of transition holds for R and R'. Prove that $R \subseteq R'$.

CHAPTER III

Multiplicities

20. Homogeneous rings

A ring R is called a *homogeneous ring* over a ring A if R is a graded ring $\sum R_i$ such that $A = R_0$ and such that R is generated by R_1 over A. If furthermore R_1 is generated by algebraically independent elements over A, then R is called a *homogeneous polynomial ring*. A graded ideal of a homogeneous ring is called a *homogeneous ideal*.

The above definition shows that homogeneous rings are nothing but homomorphic images of homogeneous polynomial rings whose kernels are homogeneous ideals.

(20.1) *A homogeneous ring $R = \sum R_n$ is Noetherian if and only if R_0 and R_1 are Noetherian (i.e., R_0 is a Noetherian ring and R_1 has a finite basis over R_0).*

Proof: The *if* part is obvious. Conversely, assume that R is Noetherian. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R_0, then that $\mathfrak{a} \neq \mathfrak{b}$ implies that $\mathfrak{a}R \neq \mathfrak{b}R$ (because $\mathfrak{a} = \mathfrak{a}R \cap R_0$, $\mathfrak{b} = \mathfrak{b}R \cap R_0$), and we see that R_0 is Noetherian. If $\mathfrak{a}$ and $\mathfrak{b}$ are submodules of R_1, then that $\mathfrak{a} \neq \mathfrak{b}$ implies that $\mathfrak{a}R \neq \mathfrak{b}R$, and we see that R_1 is Noetherian.

Let $R = \sum R_n$ be a graded ring and let $M = \sum M_n$ is a graded module over R. We retain these definitions of R and M throughout this section. The length of M_n (as an R_0-module) is a function of n for $n = 0, 1, 2, \ldots$. This function is called the *κ-function* of M (over R_0) and is denoted by $\kappa_{R_0}(M; n)$ or simply by $\kappa(M; n)$. If there is a polynomial $f(x)$ in one indeterminate x whose coefficients are rational numbers such that $f(n) = \sum_0^n \kappa(M; i)$ for sufficiently large n, then the polynomial $f(x)$ is called the *σ-polynomial* of M and is denoted by $\sigma_R(M; n)$ or by $\sigma(M; n)$. It is obvious that M has a σ-polynomial if and only if each $\kappa(M; n)$ is finite and furthermore $\kappa(M; n)$ is a polynomial in n for sufficiently large n. When $\mathfrak{a}$ is a graded ideal of R, $\kappa(R/\mathfrak{a}; n)$ is called the *Hilbert characteristic function* of $\mathfrak{a}$ and is denoted by $\chi(\mathfrak{a}; n)$.

(20.2) *If N and N' are graded submodules of M, then*

$$\kappa(N \mid N'; n) \mid \kappa(N \cap N'; n) \quad \kappa(N; n) \mid \kappa(N'; n).$$

Similarly if $\mathfrak{a}$ *and* $\mathfrak{b}$ *are graded ideals of* R, *then* $\chi(\mathfrak{a} \mid \mathfrak{b}; n) + \chi(\mathfrak{a} \cap \mathfrak{b}; n) = \chi(\mathfrak{a}; n) + \chi(\mathfrak{b}; n)$.

Proof: $(N_n + N'_n)/N_n = N'_n/(N_n \cap N'_n)$, which implies the assertion.

(20.3) *Let* $N = \sum N_n$ *be a graded submodule of* M *and let* f *be a homogeneous element of degree* d *in* M. *Then* $\kappa(N + fR; n) = \kappa(N; n) + \chi(N{:}fR; n - d)$. *Similarly, if* $M = R$, *then*

$$\chi(N + fR; n) = \chi(N; n) - \chi(N{:}fR; n - d).$$

Proof: By (1.5), $(N + fR)/N$ is isomorphic to $R/(N{:}fR)$. By the nature of the isomorphism, we see that $(N + fR)_n/N_n$ is isomorphic to $R_{n-d}/(N{:}fR)_{n-d}$, which implies the assertion.

(20.4) *Assume that* R *is a homogeneous polynomial ring in indeterminates* $x_1, \ldots, x_s$ *over a ring* A *which satisfies the minimum condition for ideals. Then* $\kappa(R; n) = \binom{n + s - 1}{s - 1} \cdot$ *length* A.

Proof: The number of monomials of degree n is equal to

$$\binom{n + s - 1}{s - 1}$$

and the assertion is proved.

(20.5) THEOREM: *Assume that* R *is a Noetherian homogeneous ring over a ring of altitude zero. If a graded* R*-module* M *has a finite basis, then* M *has a* σ*-polynomial.*

Proof: At first, we consider the case where $M = R/\mathfrak{a}$ with a graded ideal $\mathfrak{a}$. Assuming the contrary, let F be the set of graded ideals $\mathfrak{a}$ such that $R/\mathfrak{a}$ has no σ-polynomial. Since R is Noetherian, F has a maximal member, say $\mathfrak{a}^*$. If depth $\mathfrak{a}^* = 0$, then $R/\mathfrak{a}^*$ has a finite length, say l, and $R/\mathfrak{a}^*$ has the constant l as its σ-polynomial, which is a contradiction. Thus depth $\mathfrak{a}^* \geq 1$, therefore there is a homogeneous element f of degree 1 which is not in $\mathfrak{a}^*$. (20.3) implies that $\chi(\mathfrak{a}^* + fR; n) = \chi(\mathfrak{a}^*; n) - \chi(\mathfrak{a}^*{:}fR; n - 1)$. By the maximality of $\mathfrak{a}^*$, $\chi(\mathfrak{a}^* + fR; n)$ is a polynomial in n for large n, say, for $n \geq m$. If $\mathfrak{a}^*{:}fR \neq \mathfrak{a}^*$, then $\chi(\mathfrak{a}^*{:}fR; n - 1)$ is a polynomial in n for large n and we see that $\chi(\mathfrak{a}^*; n)$ is a polynomial for such n, which is a contradiction. If $\mathfrak{a}^*{:}fR = \mathfrak{a}^*$, then summing up the equalities $\chi(\mathfrak{a}^* + fR; r) = \chi(\mathfrak{a}^*; r) - \chi(\mathfrak{a}^*; r - 1)$ for $r = m, m + 1, \ldots, n$, we see that

$\chi(\mathfrak{a}^*; n) \quad \sum_m^n \chi(\mathfrak{a}^* \mid fR; i) \mid$ (constant), and $\chi(\mathfrak{a}^*; n)$ is a polynomial for large n, which is also a contradiction. Thus F is empty and this case is settled. Now we prove the general case by induction on the number of homogeneous generators of M. Let $u_1, \ldots, u_s$ be a basis for M such that each u_i is homogeneous. If $s = 1$, then M is isomorphic to $R/(0:M)$, and therefore the assertion is true in this case. Set $N = \sum_1^{s-1} u_i R$. Then, by our induction, we assume that N has a σ-polynomial $f(x)$. $M/N = u_s R/(u_s R \cap N)$, and therefore M/N has a σ-polynomial $g(x)$. Since length M_n = length N_n + length (M_n/N_n), we see that $f(x) + g(x)$ is a σ-polynomial of M, and the assertion is proved.

(20.6) *If $R_0/(0:M)$ is the direct sum of local rings $A_i (i = 1, \ldots, r)$, then denoting by e_i the identity of A_i, M is the direct sum of Me_i and* $\kappa_{R_0}(M; n) = \sum_i \kappa_{A_i}(Me_i; n)$.

Proof: $\sigma_i(m) = me_i$ defines a homomorphism from M onto Me_i, hence into M. Obviously $\sum \sigma_i$ is the identity map, hence M is generated by the Me_i. $\sum m_i = 0$ $(m_i \in Me_i)$ means that, since $m_i e_i = m_i$, $0 = e_j(\sum m_j) = m_j$. Thus we see that M is the direct sum of the Me_i, and the assertion is proved.

(20.7) *Assume that R_0 is a local ring with maximal ideal $\mathfrak{m}$. If $(A, \mathfrak{n})$ is a local ring which is dominated by R_0 and if $K = R_0/\mathfrak{m}$ is a finite algebraic extension of $K' = A/\mathfrak{n}$, then*

$$\kappa_A(M, n) = [K:K'] \cdot \kappa_{R_0}(M; n).$$

Proof: Let $M_n = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(r)} = 0$ be a composition series of M_n as an R_0-module. Then each $G^{(i)}/G^{(i+1)}$ is isomorphic to K, whence it has length $[K:K']$ as an A-module. Thus we prove the assertion.

A polynomial $f(x)$ in one indeterminate x, whose coefficients are rational numbers, is called a *numerical polynomial* if there exists an integer N such that $f(n)$ is an integer for any integer n such that $n \geq N$. σ-polynomials are numerical.

(20.8) *If $f(x)$ is a numerical polynomial of degree d, then there are integers $c_0, \ldots, c_d$ such that* $f(x) = c_0 \binom{x+d}{d} + c_1 \binom{x+d-1}{d-1} + \cdots + c_{d-1} \binom{x+1}{1} + c_d$, *where the $\binom{r}{s}$ are binomial coefficients. Consequently, $f(n)$ is an integer for any integer n and if a is a coefficient of $f(x)$ then $a \cdot (d!)$ is an integer.*

Proof: We prove the assertion by induction on d. If $d = 0$, then the assertion is obvious. Assume that $d > 0$. Let c be the coefficient of x^d. Then $f(x) - f(x-1) = cdx^{d-1} + (\text{terms of lower degrees})$. Since $f(x) - f(x-1)$ is also numerical, $c_0 = c(d!)$ is an integer. Therefore $f(x) - c_0\binom{x+d}{d}$ is a numerical polynomial of degree less than d, and we prove the assertion by our induction.

21. λ-Polynomials

Let $\mathfrak{a}$ be an ideal of a ring R and let M be an R-module. Set $F_n = \mathfrak{a}^n/\mathfrak{a}^{n+1}$ and $G_n = \mathfrak{a}^n M/\mathfrak{a}^{n+1}M$, for $n = 0, 1, 2, \ldots$.

When $a \in F_m$, $b \in F_n$, we define ab as follows: let a' and b' be elements of $\mathfrak{a}^m$ and $\mathfrak{a}^n$ respectively such that $a = (a' \text{ modulo } \mathfrak{a}^{m+1})$, $b = (b' \text{ modulo } \mathfrak{a}^{n+1})$ and then we define $ab = (a'b' \text{ modulo } \mathfrak{a}^{m+n+1})$ $(\in F_{n+m})$. This multiplication defines a ring structure in the direct sum F of all the F_n, and F becomes a graded ring. Furthermore, since $F_n = \mathfrak{a}^n/\mathfrak{a}^{n+1}$, it follows that $F_n = (F_1)^n$, which implies that F is a homogeneous ring. This homogeneous ring F is called the *form ring* of R with respect to $\mathfrak{a}$. When $a \in \mathfrak{a}^n$ and $a \notin \mathfrak{a}^{n+1}$, n is called the *degree* of a with respect to $\mathfrak{a}$ and $(a \bmod \mathfrak{a}^{n+1})$ is called the $\mathfrak{a}$-*form* of a.

The direct sum G of all the G_i becomes similarly a graded module over F. This G is called the *form module* of M with respect to $\mathfrak{a}$.

It is obvious that length $M/\mathfrak{a}^{n+1}M = \sum_0^n$ length $\mathfrak{a}^i M/\mathfrak{a}^{i+1}M = \sum_0^n \kappa(G; i)$. Therefore we see by virtue of (20.5) that

(21.1) *Assume that R and M are Noetherian and that depth $\mathfrak{a} = 0$. Then there is a numerical polynomial $f(x)$ such that length $M/\mathfrak{a}^{n+1}M = f(n)$ for all n that are greater than a fixed integer; $f(x)$ is nothing but the σ-polynomial of the form module G.*

Now, applying (20.6) and (20.7) to the above result, we see that:

(21.2) THEOREM: *Let M be a finite module over a Noetherian ring R and let $\mathfrak{a}$ be an ideal of R such that depth $\mathfrak{a} = 0$. Furthermore let R' be a Noetherian ring such that* (1) *R is an R'-module,* (2) *with*

$$\mathfrak{a}' = \{a \mid a \in R', aR \subseteq \mathfrak{a}\},$$

$R'/\mathfrak{a}'$ is dominated by $R/\mathfrak{a}$ and (3) $[R/\mathfrak{m}_i : R'/\mathfrak{m}_i']$ *are finite, where $\mathfrak{m}_i$ $(i = 1, \ldots, s)$ are the prime divisors of $\mathfrak{a}$ and $\mathfrak{m}_i'$ are the maximal ideals of R' such that $\mathfrak{m}_i'/\mathfrak{a}' = (\mathfrak{m}_i/\mathfrak{a}) \cap (R'/\mathfrak{a}')$. Then:* (a) *there is a numerical polynomial $f(x)$ such that $f(n) = \text{length}_{R'} M/\mathfrak{a}^n M$ for*

any sufficiently large natural number n, (b) if G is the form module of M with respect to $\mathfrak{a}$, then $f(n+1) - o_{R'/\mathfrak{a}'}(G; n), f(n+1) - f(n) \geq \lambda_{R'/\mathfrak{a}'}(G; n)$ for sufficiently large natural numbers n and (c) $f(n) = \sum |R/\mathfrak{m}_i : R'/\mathfrak{m}_i'| \cdot \text{length}_{R_i} \cdot M \otimes_R R_i/\mathfrak{a}^n M \otimes_R R_i$, where $R_i = R_{\mathfrak{m}_i}$.

We denote the $f(x)$ given just above by

$$\lambda_{R'}(\mathfrak{a}; M; x),$$

which is called a λ-*polynomial* of M. $\lambda_R(\mathfrak{a}; M; x)$ may be denoted simply by $\lambda(\mathfrak{a}; M; x)$ and M may be omitted if $M = R$.

By our definition, we see immediately that:

(21.3) *When R is a semi-local ring with completion R^*, then*

$$\lambda_{R'}(\mathfrak{a}; M; x) = \lambda_{R'}(\mathfrak{a}R^*; M \otimes R^*; x).$$

We see also the following by virtue of (18.9), (19.1).

(21.4) *With the same R, R', $\mathfrak{a}$ and M as in* (21.2), *if X is a transcendental element over R, then $\lambda_{R'(X)}(\mathfrak{a}R(X); M \otimes R(X); x) = \lambda_{R'}(\mathfrak{a}; M; x)$.*

(21.5) THEOREM: *With the same R, R', $\mathfrak{a}$ and M as in* (21.2), *let N be a submodule of M. Set $g(x) = \lambda_{R'}(\mathfrak{a}; N; x) + \lambda_{R'}(\mathfrak{a}; M/N; x) - \lambda_{R'}(\mathfrak{a}; M; x)$. Then $g(n) = \text{length}_{R'}(\mathfrak{a}^n M \cap N)/\mathfrak{a}^n N \leq \text{length}_{R'} \cdot \mathfrak{a}^{n-r}N/\mathfrak{a}^n N$ with a fixed natural number r and for a sufficiently large natural number n, and therefore $g(x)$ is of lower degree than $\lambda_{R'}(\mathfrak{a}; N; x)$, except for the case where $\lambda_{R'}(\mathfrak{a}; N; n)$ is of degree 0 and $g(x) = 0$.*

Proof: Since $(M/N)/\mathfrak{a}^n(M/N) = M/(\mathfrak{a}^n M + N)$ and since $(\mathfrak{a}^n M + N)/\mathfrak{a}^n M = N/(\mathfrak{a}^n M \cap N)$, we have the first equality. Since $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$ by the lemma of Artin-Rees, we have $\mathfrak{a}^n N \subseteq \mathfrak{a}^n M \cap N \subseteq \mathfrak{a}^{n-r}N$, which shows the inequality. If $\lambda_{R'}(\mathfrak{a}; N; x)$ is a constant, then $\mathfrak{a}^m N = 0$ for sufficiently large m and we see that $g(x) = 0$ by the inequality just proved. Assume that $\lambda_{R'}(\mathfrak{a}; N; x)$ is not constant. Then $g(x) \leq \lambda_{R'}(\mathfrak{a}; N; x) - \lambda_{R'}(\mathfrak{a}; N; x - r)$, which is of lower degree than $\lambda_R(\mathfrak{a}; N; x)$, and thus we complete the proof.

22. *Superficial elements*

Let $R = \sum R_n$ be a Noetherian homogeneous ring. An element f of R is called a *superficial element* of R if $f \in R_1$ and if there is an m such that $(0:fR) \cap R_n = 0$ for any $n \geq m$.

(22.1) *Assume that R_0 is a semi-local ring with maximal ideals*

$\mathfrak{m}_1, \ldots, \mathfrak{m}_u$, *that every* $R/\mathfrak{m}_i$ *contains infinitely many elements and that* R_1 *is a finite* R_0*-module. Let* $\mathfrak{n}_1, \ldots, \mathfrak{n}_t$ *be proper submodules of* R_1. *Then there is a superficial element* f *of* R *which is not in any of the* $\mathfrak{n}_i$.

Proof: Consider all of the prime divisors of zero which do not contain R_1; let them be $\mathfrak{p}_1, \ldots, \mathfrak{p}_u$. Set $\mathfrak{n}_{t+i} = \mathfrak{p}_i \cap R_1$. Then, by the lemma of Krull-Azumaya, we see that $\mathfrak{n}_j + \mathfrak{T}R_1 \neq R_1$ for any $j = 1, \ldots, t+u$, $\mathfrak{T}$ being the Jacobson radical of R_0 ($\mathfrak{T} = \bigcap_i \mathfrak{m}_i$). Hence $N_j = (\mathfrak{n}_j + \mathfrak{T}R_1)/\mathfrak{T}R_1$ is a proper submodule of $M = R_1/\mathfrak{T}R_1$. We shall show that there is an element g of M which is not in any of the N_j. M is the direct sum of $M_i = R_1/\mathfrak{m}_iR_1$, which have free bases $m_{i,1}, \ldots, m_{i,n(i)}$ over the fields $R_0/\mathfrak{m}_i$. We prove the existence of g by induction on $\sum n(i)$. Set $N_j^* = m_{1,1}R + N_j$. We may assume that $N_j^* = M$ if and only if $j > v$. Applying the induction assumption to $N_j^*/m_{1,1}R$ in $M/m_{1,1}R$, we see that there is an element g^* of $M/m_{1,1}R$ which is not in any of the $N_j^*/m_{1,1}R$ for $j = 1, \ldots, v$. Let g' and g'' be two different elements of M whose residue classes modulo $m_{1,1}R$ are the same g^*. If both g' and g'' are in the same N_j, then N_j contains $m_{1,1}$, which cannot happen for $j > v$. Therefore, if we take different $g^{(1)}, \ldots, g^{(r)}$ of M whose residue classes are all the same g^* and if $r > t + u - v$, then at least one of $g^{(i)}$ is not in any of the N_j for $j > v$. By the choice of g^*, we see that the element is not in any of the N_j for $j = 1, \ldots, t+u$. Thus the existence of g is proved. Now let f be an element of R such that f modulo $\mathfrak{T}R = g$. Since $f \notin \mathfrak{p}_i$ for any i by our choice, $0{:}fR$ coincides with 0 up to primary components whose prime divisors contain R_1; namely, there is an ideal $\mathfrak{b}$ which contains a power R_1^m of R_1 such that $\mathfrak{b} \cap (0{:}fR) = 0$, whence $(0{:}fR) \cap R_n \subseteq (0{:}fR) \cap \mathfrak{b} = 0$ for $n \geq m$, and f is superficial.

When $\mathfrak{a}$ is an ideal of a Noetherian ring R, an element a of $\mathfrak{a}$ is called a *superficial element* of $\mathfrak{a}$ if there exists a natural number c such that $(\mathfrak{a}^n{:}aR) \cap \mathfrak{a}^c = \mathfrak{a}^{n-1}$ for any natural number $n > c$.

(22.2) *With the notation as above,* $a \in \mathfrak{a}$ *is a superficial element of* $\mathfrak{a}$ *if* a *modulo* $\mathfrak{a}^2$ *is a superficial element of the form ring* $F = \sum F_n$ *of* R *with respect to* $\mathfrak{a}$.

Proof: Set $a' = a$ modulo $\mathfrak{a}^2$. Let a natural number c be such that $(0{:}a'F) \cap F_n = 0$ for $n \geq c$. Let n be an arbitrary natural number such that $n > c$. It is obvious that $\mathfrak{a}^{n-1} \subseteq (\mathfrak{a}^n{:}aR) \cap \mathfrak{a}^c$. Let b be an arbitrary element of $(\mathfrak{a}^n{:}aR) \cap \mathfrak{a}^c$. Then $ab \in \mathfrak{a}^n$. Let m be such that $b \in \mathfrak{a}^{m-1}$ and that $b \notin \mathfrak{a}^m$. Set $b' = b$ modulo $\mathfrak{a}^m$. Then $b' \in F_{m-1}$.

Since $b \in \mathfrak{a}^n$, we have $m \geq l + c$, whence $(0{:}a'F) \cap F_{m-l} = 0$. If $m < n$, then $ab \in \mathfrak{a}^n$ implies that $a'b' = 0$, which is a contradiction. Therefore $m \geq n$, and $b \in \mathfrak{a}^{n-l}$. Thus the proof is complete.

(22.3) THEOREM: *Let $\mathfrak{a}$ be an ideal of depth zero in a Noetherian ring R, and let the prime divisors of $\mathfrak{a}$ be $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$. Let S be the intersection of the complements of $\mathfrak{m}_i$. Let $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ be ideals of R such that $\mathfrak{a}R_S$ is not contained in any $\mathfrak{b}_i R_S$. If $R/\mathfrak{m}_i$ contains infinitely many elements for every i, then there is a superficial element a of $\mathfrak{a}$ which is not in any of the $\mathfrak{b}_j$.*

Proof: Let $F = \sum F_n$ be the form ring of R with respect to $\mathfrak{a}$. Set $\mathfrak{n}_j = F_1 \cap ((\mathfrak{b}_j + \mathfrak{a}^2)/\mathfrak{a}^2)$. If $\mathfrak{n}_j = F_1$, then $\mathfrak{a} \subseteq \mathfrak{b}_j + \mathfrak{a}^2$, hence $\mathfrak{a} = (\mathfrak{b}_j \cap \mathfrak{a}) + \mathfrak{a}^2$, whence $\mathfrak{a}R_S = (\mathfrak{b}_j \cap \mathfrak{a})R_S$ by the lemma of Krull-Azumaya, and it is a contradiction. Thus $\mathfrak{n}_j \neq F_1$ for any j. Therefore there is a superficial element a' of F which is not in any of the $\mathfrak{n}_j$ by (22.1). An element a of $\mathfrak{a}$ such that $a' = a$ modulo $\mathfrak{a}$ is a superficial element of $\mathfrak{a}$ by (22.2). It is obvious that $a \notin \mathfrak{b}_j$, and the assertion is proved.

(22.4) *With the same R and $\mathfrak{a}$ as above, if $\mathfrak{a} = aR$, then a is a superficial element of $\mathfrak{a}$.*

Proof: It is sufficient to show that, in the form ring $F = \sum F_n$ of R with respect to $\mathfrak{a}$, $a' = a$ modulo $\mathfrak{a}^2$ is a superficial element of F. F is generated by a' over $F_0 = R/aR$. Therefore, if $\mathfrak{p}$ is a prime divisor of zero in F which does not contain F_1, then $a' \notin \mathfrak{p}$, hence $0{:}a'F$ coincides with 0 up to primary components whose prime divisors contain F_1. Therefore, a' is a superficial element of F, and a is a superficial element of $\mathfrak{a}$.

(22.5) *With the same notation as in* (21.2), *if $b \in R$, then*

$$\text{length}_{R'} R/(\mathfrak{a}^n + bR) = \text{length}_{R'} R/\mathfrak{a}^n - \text{length}_{R'} R/(\mathfrak{a}^n{:}bR).$$

This follows from (1.5).

(22.6) THEOREM: *With the same notation as above, assume that $a \in \mathfrak{a}$. Set $\mathfrak{a}' = \mathfrak{a}/aR$. Then $\lambda_{R'}(\mathfrak{a}'; n) \geq \lambda_{R'}(\mathfrak{a}; n) - \lambda_{R'}(\mathfrak{a}; n-1)$ for large n. If a is a superficial element of $\mathfrak{a}$, then, with the intersection S of the complements of the prime divisors of $\mathfrak{a}$, $\text{length}_{R'}(0{:}aR_S)$ is finite and $\lambda_{R'}(\mathfrak{a}'; x) = \lambda_{R'}(\mathfrak{a}; x) - \lambda_{R'}(\mathfrak{a}; x-1) + \text{length}_{R'}(0{:}aR_S)$.*

Proof: The first assertion is immediate from (22.5). Let c be a sufficiently large natural number which is fixed and let n be greater than c. Then $(\mathfrak{a}^n{:}aR) \cap \mathfrak{a}^c = \mathfrak{a}^{n-1}$. By (22.5), we have

$$\lambda_{R'}(\mathfrak{a}';\, n) \qquad \lambda_{R'}(\mathfrak{a};\, n) \qquad \lambda_{R'}(\mathfrak{a};\, n \qquad 1)$$

$$+ \operatorname{length}_{R'}(\mathfrak{a}^n{:}aR)/\mathfrak{a}^{n-1} \cdot \operatorname{length}_{R'}(\mathfrak{a}^n{:}aR)/\mathfrak{a}^{n-1}$$

$$= \operatorname{length}_{R'}(\mathfrak{a}^n{:}aR)/((\mathfrak{a}^n{:}aR) \cap \mathfrak{a}^r) \qquad \operatorname{length}_{R'}((\mathfrak{a}^n{:}aR) + \mathfrak{a}^r)/\mathfrak{a}^r.$$

Since the minimum condition holds in $R/\mathfrak{a}^r$, this length is a constant, say C, for large n. We have only to prove that $C = \operatorname{length}_{R'}(0{:}aR_S)$. Since $R/\mathfrak{a}^c = R_S/\mathfrak{a}^c R_S$ we may assume that $R = R_S$. Then $\mathfrak{a}^n{:}aR$ is contained in $(0{:}aR) + \mathfrak{a}^c$ by (3.12) for large n, whence $C = \operatorname{length}_{R'}(0{:}aR)/(0{:}aR) \cap \mathfrak{a}^c$. Since this C is independent of c (when c is large), $(0{:}aR) \cap \mathfrak{a}^c$ must be zero, and the assertion is proved.

(22.7) THEOREM: *With the same notation as in* (21.2), *the degree of* $\lambda_{R'}(\mathfrak{a};\, M;\, x)$ *is equal to* altitude $(\mathfrak{a} + (0{:}M))/(0{:}M)$ (*in the ring* $R/(0{:}M)$).

Proof: By virtue of (21.2), we may assume that $R = R'$ and furthermore that R is a local ring, with maximal ideal $\mathfrak{m} = \mathfrak{m}_1$. We may assume obviously that $0{:}M = 0$. Let $u_1, \ldots, u_t$ be a basis for M. We prove the assertion by induction on t. If $t = 1$, then M is isomorphic to R, and $\lambda(\mathfrak{a};\, M;\, n) = \lambda(\mathfrak{a};\, n)$. We prove this case by induction on altitude R. If altitude $R = 0$, then the assertion is obvious. Assume that altitude $R > 0$. Considering $R(X)$ if necessary (with a transcendental element X over R), we may assume that $R/\mathfrak{m}$ contains infinitely many elements by virtue of (21.4) and (9.10). (22.3) and (22.5) imply that there is a superficial element a of $\mathfrak{a}$ such that altitude R/aR = altitude $R - 1$ (by virtue of (9.7)). Then $\lambda(\mathfrak{a}/aR;\, x)$ is of degree (altitude $R - 1$) by our induction assumption. Therefore, we see that $\lambda(\mathfrak{a};\, x)$ is of degree (altitude R) by (22.6), which proves the assertion in this case. We consider now the general case. Since $0 = 0{:}M = \bigcap_i (0{:}u_iR)$, there is an u_i, say u_1, such that depth $(0{:}u_1R)$ = altitude R. Then, applying (21.5) with $N = u_1R$, $\deg(\lambda(\mathfrak{a};\, M;\, x)) = \max\{\deg \lambda(\mathfrak{a};\, N;\, x), \deg \lambda(\mathfrak{a};\, M/N;\, x)\}$. $\deg \lambda(\mathfrak{a};\, N;\, x)$ = altitude R by the case where $t = 1$ and $\deg \lambda(\mathfrak{a};\, M/N;\, x) \leq$ altitude R by induction, and thus we prove the assertion.

(22.8) COROLLARY. *With the same* $\mathfrak{a}$ *and* R *as above, if*

$$\text{altitude } \mathfrak{a} \geq 1$$

and if a *is a superficial element of* $\mathfrak{a}$, *then*

$$\text{altitude } \mathfrak{a}/aR = \text{altitude } \mathfrak{a} - 1.$$

(22.9) THEOREM: *Assume that the theorem of transition holds for Noetherian rings R and R^*. If $\mathfrak{p}$ is a prime ideal of R and if $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{p}R^*$, then* height $\mathfrak{p}$ = height $\mathfrak{p}^*$. *Consequently,* altitude R = altitude R^*. *Furthermore, if $\mathfrak{a}$ is an ideal of R, then* height $\mathfrak{a}$ = height $\mathfrak{a}R^*$ *and* altitude $\mathfrak{a}$ = altitude $\mathfrak{a}R^*$.

Proof: The theorem of transition holds for $R_{\mathfrak{p}}$ and $R^*_{\mathfrak{p}^*}$ by (19.2), whence $\lambda(\mathfrak{p}R^*_{\mathfrak{p}^*}\,;x)$ and $\lambda(\mathfrak{p}R_{\mathfrak{p}}\,;x)$ have the same degree, and we have height $\mathfrak{p}$ = height $\mathfrak{p}'$. Therefore, it is obvious that altitude R = altitude R^* because R^* dominates R. The last assertion follows from (18.11) and the above result (by virtue of (19.1)).

EXERCISES: *1.* Prove the converse of (22.2).

2. Let M be a finite module over a semi-local ring R and let $\mathfrak{a}$ be an ideal of R such that the radical of $\mathfrak{a}$ is the Jacobson radical of R. Prove that altitude R is equal to the altitude of the form ring F of R with respect to $\mathfrak{a}$ and that op. alt M is equal to the operator altitude of the form module of M with respect to $\mathfrak{a}$ (as an F-module).

3. With R, M and $\mathfrak{a}$ as above, let b be an element of R. Prove that

$$\lambda(\mathfrak{a};\, M/bM;\, n) = \lambda(\mathfrak{a};\, M;\, n) - \text{length}\ (M/(\mathfrak{a}^n M : bR))$$

for sufficiently large n.

23. Multiplicities

Let R, R', $\mathfrak{a}$, M, *etc.* be as in (21.2) throughout this section. Set r = altitude $\mathfrak{a}$. Then the degree of $\lambda_{R'}(\mathfrak{a};\, M;\, x)$ is at most equal to r by (22.7). Let a be the coefficient of x^r in this λ-polynomial. Then $(r!)a$ is an integer by (20.8). This integer is called the *multiplicity* of $\mathfrak{a}$ with respect to M over R' and is denoted by $\mu_{R'}(\mathfrak{a};\, M)$. R' may be dropped if $R' = R$. M may be dropped if $M = R$. Note that $\mu_{R'}(\mathfrak{a};\, M) = 0$ if and only if altitude $(\mathfrak{a} + (0:M))/(0:M) <$ altitude $\mathfrak{a}$. Note also that if M is a ring, then $\mu_{R'}(\mathfrak{a};\, M)$ is either $\mu_{R'}(\mathfrak{a}M)$ or zero according as altitude $\mathfrak{a}M$ is equal to altitude $\mathfrak{a}$ or not.

(21.2) implies that

(23.1) $\mu_{R'}(\mathfrak{a};\, M) = \sum_i \mu(\mathfrak{a}R_i\,;\, M \otimes R_i)\ [R/\mathfrak{m}_i : R'/\mathfrak{m}']$, *where i runs over those indices such that* height $\mathfrak{m}_i$ = altitude $\mathfrak{a}$.

(23.2) COROLLARY: *Let S be the intersection of the complements of the $\mathfrak{m}_i$ such that* height $\mathfrak{m}_i$ = altitude $\mathfrak{a}$. *Then* $\mu_{R'}(\mathfrak{a};\, M) = \mu_{R'}(\mathfrak{a}R_S\,;\, M \otimes R_S)$.

Note that one can reduce multiplicities to those of the case where $R = R'$ and where R is a local ring by (23.1).

As an immediate consequence of (21.5), we have an important

(23.3) THEOREM: *If N is a submodule of M, then*

$$\mu_{R'}(\mathfrak{a}; N) \mid \mu_{R'}(\mathfrak{a}; M/N) \quad \mu_{R'}(\mathfrak{a}; M),$$

and, in particular, if op. alt $M/N <$ altitude R, *then we have*

$$\mu_{R'}(\mathfrak{a}; N) = \mu_{R'}(\mathfrak{a}; M).$$

(23.4) COROLLARY: *If N has a free base $a_1, \ldots, a_f$ and if* op. alt M/N *is less than* altitude R, *then we have* $\mu_{R'}(\mathfrak{a}; M) = f \cdot \mu_{R'}(\mathfrak{a})$. *In particular, if the finite module M is a ring contained in the total quotient ring of R, then* $\mu_{R'}(\mathfrak{a}M) = \mu_{R'}(\mathfrak{a})$.

Next we prove

(23.5) THEOREM: *Letting $\mathfrak{p}$ run over all prime divisors of zero in R such that* depth $\mathfrak{p}$ = altitude R *and such that* $\mathfrak{a} + \mathfrak{p} \neq R$, *we have*

$$\mu_{R'}(\mathfrak{a}; M) = \sum_{\mathfrak{p}} \mu_{R'}((\mathfrak{a} + \mathfrak{p})/\mathfrak{p}) \cdot \text{length}_{R_{\mathfrak{p}}}(M \otimes R_{\mathfrak{p}}).$$

Proof: We note first that the vanishing of the right hand side implies that op. alt $M \otimes R_i <$ altitude R, and therefore that $\mu_{R'}(\mathfrak{a}; M) = 0$. Now we prove the assertion by induction on $t = \sum$ length $(M \otimes R_{\mathfrak{p}})$. Since the case where $t = 0$ is proved already, we assume that $t > 0$. Let m be an element of M such that $0{:}mR_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ for one $\mathfrak{p}$, say $\mathfrak{q}$. Then there is an element c of R which is not in $\mathfrak{q}$ such that $0{:}cmR = \mathfrak{q}$. Set $N = cmR$. Then N is isomorphic to $R/\mathfrak{q}$, and $\mu_{R'}(\mathfrak{a}; N) = \mu_{R'}(\mathfrak{a}; R/\mathfrak{q}) = \mu_{R'}((\mathfrak{a} + \mathfrak{q})/\mathfrak{q})$. This equality and our induction applied to M/N proves the assertion by virtue of (23.3).

The following lemma is immediate from the definition:

(23.6) *If $\mathfrak{b}$ is an ideal of R such that $\mathfrak{b} \subseteq \mathfrak{a}$ and if $\mathfrak{a}$ and $\mathfrak{b}$ have the same radical (or, more generally, if* altitude $\mathfrak{b}$ = altitude $\mathfrak{a}$), *then* $\mu_{R'}(\mathfrak{a}; M) \leq \mu_{R'}(\mathfrak{b}; M)$.

(23.7) THEOREM: *With $\mathfrak{b}$ as above, assume that $\mu(\mathfrak{a}) = \mu(\mathfrak{b})$. Then* $\mu_{R'}(\mathfrak{a}; M) = \mu_{R'}(\mathfrak{b}; M)$.

Proof: By the $\mathfrak{p}$ in (23.5), we have

$$\mu(\mathfrak{a}) = \sum_{\mathfrak{p}} \mu(\mathfrak{a} + \mathfrak{p}/\mathfrak{p}) \cdot \text{length } R_{\mathfrak{p}}\,, \quad \mu(\mathfrak{b}) = \sum_{\mathfrak{p}} \mu(\mathfrak{b} + \mathfrak{p}/\mathfrak{p}) \cdot \text{length } R_{\mathfrak{p}}\,.$$

Since $\mu(\mathfrak{b} + \mathfrak{p}/\mathfrak{p}) \geq \mu(\mathfrak{a} + \mathfrak{p}/\mathfrak{p})$ by (23.6), $\mu(\mathfrak{a}) = \mu(\mathfrak{b})$ implies that $\mu(\mathfrak{b} + \mathfrak{p}/\mathfrak{p}) = \mu(\mathfrak{a} + \mathfrak{p}/\mathfrak{p})$ for every $\mathfrak{p}$. By (23.1) we see, in the same way, that $\mu_{R'}(\mathfrak{b} + \mathfrak{p}/\mathfrak{p}) = \mu_{R'}(\mathfrak{a} + \mathfrak{p}/\mathfrak{p})$. Therefore, again by (23.5), we have the equality $\mu_{R'}(\mathfrak{a}; M) = \mu_{R'}(\mathfrak{b}; M)$.

We add here the following remark:

(23.8) *If* $F = \sum F_n$ *and* $G = \sum G_n$ *are the form ring of* R *and the form module of* M, *respectively, with respect to* $\mathfrak{a}$, *then* $\mu_{R'}(\mathfrak{a}; M) = \mu_{R'}(F_1F; G)$, op. alt. M = op. alt. G, *and in particular*, altitude $\mathfrak{a}$ = altitude F_1F.

The proof is immediate from (21.2) and (22.7).

EXERCISES: *1*. Let $\mathfrak{b}$ and $\mathfrak{c}$ be ideals of R such that depth $\mathfrak{b} >$ depth $\mathfrak{c}$ and such that $\mathfrak{a} + \mathfrak{b} \neq R$. Prove that $\mu_{R'}((\mathfrak{a} + \mathfrak{b})/\mathfrak{b}; M/\mathfrak{b}M) = \mu_{R'}((\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c})/(\mathfrak{b} \cap \mathfrak{c}); M/(\mathfrak{b} \cap \mathfrak{c})M) = \mu_{R'}((\mathfrak{a} + \mathfrak{b}\mathfrak{c})/\mathfrak{b}\mathfrak{c}; M/\mathfrak{b}\mathfrak{c}M)$.

2. Assume that M_i are finite R-modules and that $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ is exact (with suitable homomorphisms). Prove that

$$\sum_i (-1)^i \cdot \mu_{R'}(\mathfrak{a}; M_i) = 0.$$

3. Let R^* be the ring $R \oplus M$ in the principle of idealization. Prove that $\mu_{R'}(\mathfrak{a}; M) = \mu_{R'}(\mathfrak{a}R^*) - \mu_{R'}(\mathfrak{a})$.

24. System of parameters

We first generalize the notion of system of parameters: Let $\mathfrak{a}$ be an ideal of a Noetherian ring R such that depth $\mathfrak{a} = 0$. Set $r =$ altitude $\mathfrak{a}$. If there are r elements $a_1, \ldots, a_r$ of $\mathfrak{a}$ such that $\mathfrak{a}$ and $\sum a_iR$ have the same radical, then we call the set of the a_i a *system of parameters* of $\mathfrak{a}$. The set of r elements $b_1, \ldots, b_r$ is called a *system of parameters* of R if depth $\sum b_iR = 0$ and if altitude $\sum b_iR = r$. (9.6) shows that if R is a semi-local ring then the Jacobson radical of R has a system of parameters. On the other hand, (9.3) implies that if $\sum_1^s b_iR$ ($b_i \in R$) has the same radical with $\mathfrak{a}$, then $s \geq r$. Therefore, by virtue of the case of system of parameters of a local ring, if $x_1, \ldots, x_r$ is a system of parameters of $\mathfrak{a}$, then altitude $\mathfrak{a}/(x_1R + \cdots + x_tR) = r - t$. In this section, we mainly treat the case where $\mathfrak{a}$ is generated by a system of parameters of $\mathfrak{a}$. One should note that the general case may be reduced to such a case by virtue of (21.4), (23.2), (23.7) and the following:

(24.1) THEOREM: *If* $(R, \mathfrak{m}_1, \ldots, \mathfrak{m}_s)$ *is a semi-local ring of altitude* r, *if every* $R/\mathfrak{m}_i$ *contains infinitely many elements and if the radical of* $\mathfrak{a}$ *is the Jacobson radical* $\mathfrak{T} = \bigcap \mathfrak{m}_i$ *of* R, *then there is a system of parameters* $a_1, \ldots, a_r$ *of* $\mathfrak{a}$ *such that* $\mu(\mathfrak{a}) = \mu(\sum a_iR)$.

Before proving (24.1), we prove a lemma.

(24.2) *With the same* R, R', S, *and* $\mathfrak{a}$ *as in* (22.6), *we have the following*:

(1) *If* $a \in \mathfrak{a}^t$, *and if* altitude $\mathfrak{a}/aR$ = altitude $\mathfrak{a}$, *then* altitude $\mathfrak{a}/aR$ = altitude $\mathfrak{a} - 1$ *and* $\mu_{R'}(\mathfrak{a}/aR) = t \cdot \mu_{R'}(\mathfrak{a})$.

(2) *If* a *is a superficial element of* $\mathfrak{a}$ *and if* altitude $\mathfrak{a} > 1$, *then*

$$\text{length}_{R'} R/aR = \mu_{R'}(\mathfrak{a}) + \text{length}_{R'}(0 : aR_S).$$

(3) *If* a *is a superficial element of* $\mathfrak{a}$ *and if* altitude $\mathfrak{a} > 1$, *then*

$$\mu_{R'}(\mathfrak{a}/aR) = \mu_{R'}(\mathfrak{a}).$$

Proof: If $a \in \mathfrak{a}^t$, then $\mathfrak{a}^n : aR$ contains $\mathfrak{a}^{n-t}$ for $n > t$, and $\lambda_{R'}(\mathfrak{a}/aR; n) \geq \lambda_{R'}(\mathfrak{a}; n) - \lambda_{R'}(\mathfrak{a}; n - t)$ for sufficiently large n by (22.6), and we prove (1). (2) and (3) follow from the last assertion in (22.6).

We note, by the way, that if altitude $\mathfrak{a}/aR$ = altitude $\mathfrak{a}$, then $\mu_{R'}(\mathfrak{a}/aR) \leq \mu_{R'}(\mathfrak{a})$ by the definition of multiplicities (or by (23.3)).

Now we prove (24.1). We prove the assertion by induction on r. If $r = 0$, then the empty set is the required system of parameters. Assume that $r \geq 1$. Let a_1 be a superficial element of $\mathfrak{a}$; the existence follows from (22.3). Assume at first that $r = 1$. Applying (2) in (24.2), we have $\text{length}_{R'} R/a_1R = \mu_{R'}(\mathfrak{a}/a_1R) = \mu_{R'}(\mathfrak{a}) + \text{length}_{R'}(0 : a_1R)$. Since a_1 is a superficial element of a_1R by (22.4), we have by (22.6) that $\text{length}_{R'} R/a_1R = \mu_{R'}(a_1R) + \text{length}_{R'}(0 : a_1R)$, and we have $\mu_{R'}(\mathfrak{a}) = \mu_{R'}(a_1R)$. Assume now that $r > 1$. Then $\mu_{R'}(\mathfrak{a}/a_1R) = \mu_{R'}(\mathfrak{a})$ by (24.2). By induction, there is a system of parameters $a_2', \ldots, a_r'$ of $\mathfrak{a}/a_1R$ such that $\mu_{R'}(\mathfrak{a}/a_1R) = \mu_{R'}(\sum a_i'(R/a_1R))$. Let a_i be elements of $\mathfrak{a}$ such that $a_i' = a_i$ modulo a_1R. We are to prove that $a_1, \ldots, a_r$ are the required elements. Since $a_i \in \mathfrak{a}$, we have $\mu_{R'}(\sum a_iR) \geq \mu_{R'}(\mathfrak{a})$. On the other hand, by (1) in (24.2) we have $\mu_{R'}((\sum a_iR)/a_1R) \geq \mu_{R'}(\sum a_iR)$, whence $\mu_{R'}(\mathfrak{a}) = \mu_{R'}(\mathfrak{a}/a_1R) = \mu_{R'}(\sum a_i'(R/a_1R)) = \mu_{R'}((\sum a_iR)/a_1R) \geq \mu_{R'}(\sum a_iR)$, which implies that $\mu_{R'}(\sum a_iR) = \mu_{R'}(\mathfrak{a})$, and the proof is complete.

(24.3) *We use the same notation as in* (21.2). *If* $a \in \mathfrak{a}^t$ *and if altitude* $\mathfrak{a}/aR$ = *altitude* $\mathfrak{a} - 1$, *then* $\mu_{R'}(\mathfrak{a}/aR; M/aM) \geq t \cdot \mu_{R'}(\mathfrak{a}; M)$. *If* $a_1, \ldots, a_r$ *form a system of parameters of* $\mathfrak{a}$ *and if* $a_i \in \mathfrak{a}^{n_i}$, *then* $\text{length}_{R'} M/(\sum a_iM) \geq n_1 \cdots n_r \cdot \mu_{R'}(\mathfrak{a}; M)$.

Proof: (22.5) can be generalized to the case of modules by virtue of (1.6), and we have $\text{length}_{R'} M/(\mathfrak{a}^n + aR)M = \text{length}_{R'} M/\mathfrak{a}^nM - \text{length}_{R'} M/(\mathfrak{a}^nM : aR)$. Since $a \in \mathfrak{a}^t$, we have length $M/(\mathfrak{a}^nM : aR) \leq$ length $M/\mathfrak{a}^{n-t}M$, and $\lambda_{R'}(\mathfrak{a}/aR; M/aM; n) \geq \lambda_{R'}(\mathfrak{a}; M; n) - \lambda_{R'}(\mathfrak{a}; M; n - t)$, and we have the first result. By a repeated application of the first result, we see that $\text{length}_{R'} M/(\sum a_iM) = \mu_{R'}(0; M/(\sum a_iM)) \geq n_1 \cdots n_r \cdot \mu_{R'}(\mathfrak{a}; M)$, which proves the last assertion.

(24.4) *With the same R, R', $\mathfrak{a}$, and M as above, if $\mathfrak{a}$ is generated by a system of parameters $a_1, \ldots, a_r$, then* $\mu_{R'}(\mathfrak{a}; M) = \lim_{\min(n_i)\to\infty} (\text{length}_{R'} M/\sum a_i^{n_i} M)/(n_1 \cdots n_r)$. (LEMMA OF LECH)

Proof: That $\text{length}_{R'} M/\sum a_i^{n_i} M \geq n_1 \cdots n_r \cdot \mu_{R'}(\mathfrak{a}; M)$ follows from (24.3), and we have $\liminf (\text{length}_{R'} M/\sum a_i M)/n_1 \cdots n_r \geq \mu_{R'}(\mathfrak{a}; M)$. Therefore, we have only to show that

$$\limsup (\text{length}_{R'} M/(\sum a_i^n M))/n_1 \cdots n_r \leq \mu_{R'}(\mathfrak{a}; M).$$

Let $F = \sum F_n$ be the form ring of R with respect to $\mathfrak{a}$ and let $G = \sum G_n$ be the form module of M with respect to $\mathfrak{a}$. Set $x_i = a_i$ modulo $\mathfrak{a}^2$. Then the form module of $M/(\sum a_i^{n_i} M)$ is a homomorphic image of $G/(\sum x_i^{n_i} G)$, whence $\text{length}_{R'} G/(\sum x_i^{n_i} G) \geq \text{length}_{R'} M/(\sum a_i^{n_i} M)$, whence it is sufficient to show that

$$\limsup (\text{length}_{R'} G/(\sum x_i^{n_i} G))/n_1 \cdots n_r \leq \mu_{R'}(F_1 \cdot F; G),$$

because $\mu_{R'}(\mathfrak{a}; M) = \mu_{R'}(F_1 \cdot F; G)$ by (23.8). Thus we may assume that $F = R$, $M = G$, and $a_i = x_i$. R is then a homomorphic image of the polynomial ring in r indeterminates $X_1, \ldots, X_r$ over F_0. We prove the case where $M = mR$ ($m \in G_0$) by induction on length F_0. M is isomorphic to $R/(0:M)$. If $r = 0$, then the assertion is obvious, and we assume that $r > 0$. Assume that length $F_0 = 1$, *i.e.*, $\mathfrak{a}$ is maximal. Since F_0 is a field in this case, the x_i must be algebraically independent over F_0 because altitude $\mathfrak{a} = r$. If $0:M = 0$, then obviously M is isomorphic to the polynomial ring, $\mu_{R'}(\mathfrak{a}; M) = \text{length}_{R'} F_0$, and

$$\begin{aligned}\text{length}_{R'} M/(\sum x_i^{n_i} M) &= \text{length}_{R'} R/(\sum x_i^{n_i} R) \\ &= \text{length}_{R'} (F_0[x_1]/x_1^{n_1} F_0[x]) \otimes_{F_0} \cdots \otimes_{F_0} (F_0[x_r]/x_r^{n_r} F_0[x_r]) \\ &= n_1 \cdots n_r \cdot \text{length}_{R'} F_0,\end{aligned}$$

and we have the required equality in this case. Assume that $0:M \neq 0$, and let f be a homogeneous form of degree, say s, which is in $0:M$ ($f \neq 0$). Then M is a homomorphic image of R/fR. Then

$$\begin{aligned}&\text{length}_{R'} M/(\sum x_i^{n_i} M) \\ &\quad \leq \text{length}_{R'} R/(\sum x_i^{n_i} R) - \text{length}_{R'} (fR + \sum x_i^{n_i} R)/(\sum x_i^{n_i} R).\end{aligned}$$

$\text{length}_{R'} R/(\sum x_i^{n_i} R) = n_1 \cdots n_r \text{length}_{R'} F_0$ as was shown above, and $\text{length}_{R'} (fR + \sum x_i^{n_i} R)/(\sum x_i^{n_i} R) = \text{length}_{R'} R/((\sum x_i^{n_i} R):fR)$ by (1.5). Since F_0 is a field, $(\sum x_i^{n_i} R):fR \subseteq \sum x_i^{n_i - s} R$ and therefore $\text{length}_{R'} R/((\sum x_i^{n_i} R):fR)$ is not smaller than

$$\text{length}_{R'} R/(\sum x_i^{n_i} R) \quad (n_1 \quad s) \cdots (n_r \quad s) \cdot \text{length}_{R'} F_0 .$$

Thus

$$\limsup \ (\text{length } M/(\sum x_i^{n_i} M))/n_1 \cdots n_r$$
$$\leq \limsup \ (n_1 \cdots n_r - (n_1 - s) \cdots (n_r - s)) \cdot \text{length}_{R'} F_0/n_1 \cdots n_r$$
$$= 0,$$

and thus we prove this case. Now assume that length $F_0 > 1$, and let $a \in F_0$ be such that length $aF_0 = 1$. By induction,

$$\lim \ (\text{length}_{R'} M/(aM + \sum x_i^{n_i} M))/n_1 \cdots n_r = \mu_{R'}(\mathfrak{a};\ M/aM),$$

and

$$\lim \ (\text{length}_{R'} \cdot aM/a(\sum x_i^{n_i} M))/n_1 \cdots n_r = \mu_{R'}(\mathfrak{a};\ aM).$$

Now

$$\limsup \ (\text{length}_{R'} M/(\sum x_i^{n_i} M))/n_1 \cdots n_r$$
$$= \limsup \ [(\text{length}_{R'} M/(aM + \sum x_i^{n_i} M)$$
$$+ \text{length}_{R'} aM/(aM \cap \sum x_i^{n_i} M)]/n_1 \cdots n_r$$
$$\leq \mu_{R'}(\mathfrak{a}; M/aM) + \limsup \ (\text{length}_{R'} aM/a(\sum x_i^{n_i} M)/n_1 \cdots n_r$$
$$= \mu_{R'}(\mathfrak{a};\ M/aM) + \mu_{R'}(\mathfrak{a};\ aM),$$

this last sum is equal to $\mu_{R'}(\mathfrak{a};\ M)$ by (23.3). Thus the case where $M = mR$ is proved. Now we prove the general case. Let $m_1, \ldots, m_s$ be a basis for M which are homogeneous. We prove the assertion by induction on s. Set $N = \sum_1^{s-1} mR$.

$$\limsup \ (\text{length}_{R'} M/(\sum x_i^{n_i} M))/n_1 \cdots n_r$$
$$= \limsup \ (\text{length}_{R'} M/(N + \sum x_i^{n_i} M)$$
$$+ \text{length}_{R'} (N + \sum x_i^{n_i} M)/(\sum x_i^{n_i} M))/n_1 \cdots n_r$$
$$\leq \mu_{R'}(\mathfrak{a};\ M/N) + \limsup \ (\text{length}_{R'} N/(\sum x_i^{n_i} N))/n_1 \cdots n_r$$
$$= \mu_{R'}(\mathfrak{a};\ M/N) + \mu_{R'}(\mathfrak{a};\ N) = \mu_{R'}(\mathfrak{a};\ M),$$

and we have proved the assertion completely.

(24.5) COROLLARY: *With the same notation as above, we have* $\mu_{R'}(\sum a_i^{n_i} R; M) = n_1 \cdots n_r \cdot \mu_{R'}(\mathfrak{a};\ M)$.

Another corollary we should remark is the following

(24.6) COROLLARY: *With the notation as above, if we do not assume that* $\mathfrak{a}$ *is generated by a system of parameters but assume that* $\mathfrak{a}$ *is generated by* $a_1, \ldots, a_s$ *with* $s > r =$ altitude $\mathfrak{a}$. *Then*

$$\lim \ (\text{length}_{R'} M/(\sum a_i^{n_i} M))/n_1 \cdots n_s = 0.$$

Proof: Since we have only to show that lim sup (length $M/(\sum a_i^{n_i} M))/n_1 \cdots n_r \leq 0$, in the same way as in the proof of (24.4), we may assume that R is the form ring $F = \sum F_n$ of R with respect to $\mathfrak{a}$. Then M is a module over the polynomial ring $F_0[X_1, \ldots, X_s]$ in indeterminates X_i with operation such that $X_i m = a_i m$ for any $m \in M$, and in this sense, the multiplicity of M is zero, and thus we prove the assertion.

Now we prove an important result.

(24.7) THEOREM: *With the same* R, R', M, *and* $\mathfrak{a}$ *as above (which are the same as in* (21.2)), *assume that* $\mathfrak{a}$ *is generated by a system of parameters* $a_1, \ldots, a_r$. *For an arbitrarily fixed integer* s *such that* $0 \leq s \leq r$, *set* $\mathfrak{b} = \sum_1^s a_i R$. *Then, letting* $\mathfrak{p}$ *run over all minimal prime divisors of* $\mathfrak{b}$ *such that height* $\mathfrak{p} = s$ *and such that depth* $\mathfrak{p} = r - s$, *we have the following formula*: $\mu_{R'}(\mathfrak{a}; M) = \sum_{\mathfrak{p}} \mu_{R'}(\mathfrak{a} + \mathfrak{p}/\mathfrak{p}) \cdot \mu(\mathfrak{b}R_{\mathfrak{p}}; M \otimes R_{\mathfrak{p}})$. (ASSOCIATIVITY FORMULA)

Proof: For an arbitrary natural number t, set $\mathfrak{b}_t = \sum_1^s a_i^t R$, $a_{i,t} = a_i$ modulo $\mathfrak{b}_t$ and $\mathfrak{c}_t^* = \sum_i a_{i,t}(R/\mathfrak{b}_t)$. Then we see by (23.5) that $\mu_{R'}(\mathfrak{c}_t^*; M/\mathfrak{b}_t M) = \sum_{\mathfrak{p}}^* \mu_{R'}(\mathfrak{c}_t^* + \mathfrak{p}^*/\mathfrak{p}^*) \cdot \text{length } (M/\mathfrak{b}_t) \otimes (R/\mathfrak{b}_t)_{\mathfrak{p}^*}$, where $\mathfrak{p}^*$ runs over all prime divisors of zero in $R/\mathfrak{b}_t$ such that depth $\mathfrak{p}^* = r - s$. Therefore, letting $\mathfrak{p}'$ run over all minimal prime divisors of $\mathfrak{b}_t$ of depth $r - s$, we have

$$\mu_{R'}(\mathfrak{c}^*{}_t; M/\mathfrak{b}_t M) = \sum_{\mathfrak{p}'} \mu_{R'}(\mathfrak{a} + \mathfrak{p}'/\mathfrak{p}') \cdot \text{length } M \otimes (R_{\mathfrak{p}'}/\mathfrak{b}_t R_{\mathfrak{p}'}).$$

On the other hand by the lemma of Lech (24.4), we have $\lim_{n\to\infty} (\text{length}_{R'} M/(\mathfrak{b}_t + \sum_{s+1}^r a_i^n R)M)/n^{r-s} = \mu_{R'}(\mathfrak{c}^*; M/\mathfrak{b}_t M)$. Therefore, we have that

$$\begin{aligned}
\mu_{R'}(\mathfrak{a}; M) &= \lim_{t,n\to\infty} \text{length}_{R'} (M/(\mathfrak{b}_t + \textstyle\sum_{s+1}^r a_i^n R)M)/t^s n^{r-s} \\
&= \lim_{t\to\infty} (\lim_{n\to\infty} (\text{length}_{R'} M/(\mathfrak{b}_t + \textstyle\sum_{s+1}^r a_i^n R)M)/t^s n^{r-s}) \\
&= \lim_{t\to\infty} \textstyle\sum_{\mathfrak{p}'} \mu_{R'}(\mathfrak{a} + \mathfrak{p}'/\mathfrak{p}') \ (\text{length } M \otimes R_{\mathfrak{p}'}/\mathfrak{b}_t R_{\mathfrak{p}'})/t^s.
\end{aligned}$$

By (24.4) and (24.6), we see that lim (length $M \otimes R_{\mathfrak{p}'}/\mathfrak{b}_t R_{\mathfrak{p}'})/t^s$

is equal to either $\mu(\mathfrak{b}R_{\mathfrak{p}'}; M \otimes R_{\mathfrak{p}'})$ or zero according as height $\mathfrak{p}'$ is equal to s or not, and therefore we prove the assertion.

25. *Macaulay rings*

We say that an ideal $\mathfrak{a}$ of a ring is *isobathy* if every prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ has depth equal to depth $\mathfrak{a}$. It is obvious that an isobathy ideal cannot have any imbedded prime divisor. We say that a semi-local ring R is *unmixed* if the zero ideal in the completion of R is isobathy. It is known that there are local integral domains which are not unmixed; an example is given in the Appendix, Example 2.

(25.1) *Let R be a semi-local ring with Jacobson radical $\mathfrak{m}$. If there is an ideal $\mathfrak{a}$ of R such that the radical of $\mathfrak{a}$ is $\mathfrak{m}$ and such that the zero ideal in the form ring $F = \sum F_n$ of R with respect to $\mathfrak{a}$ is isobathy, then R is unmixed.*

Proof: Let R^* be the completion of R. Then F is the form ring of R^* with respect to $\mathfrak{a}R^*$. Assume that there is a prime divisor $\mathfrak{p}^*$ of zero in R^* such that depth $\mathfrak{p}^* <$ altitude $R =$ altitude R^* (by (17.12)). Set $\mathfrak{p}' = \sum (\mathfrak{p}^* \cap \mathfrak{a}^n)/(\mathfrak{p}^* \cap \mathfrak{a}^{n+1})$. Then $\mathfrak{p}'$ is an ideal of F and $F/\mathfrak{p}'$ is the form ring of $R^*/\mathfrak{p}^*$ with respect to $(\mathfrak{a}R^* + \mathfrak{p}^*)/\mathfrak{p}^*$. Therefore depth $\mathfrak{p}^*$ = altitude $(\mathfrak{a}R^* + \mathfrak{p}^*)/\mathfrak{p}^*$ = altitude $(F_1F + \mathfrak{p}')/\mathfrak{p}'$ by (23.8), and this altitude is equal to depth $\mathfrak{p}'$ by (14.5). Since $\mathfrak{p}^*$ is a prime divisor of zero, there is an element $a \neq 0$ of R^* such that $a\mathfrak{p}^* = 0$. Let a' be the $\mathfrak{a}$-form of a. Then we have $\mathfrak{p}'a' = 0$, whence $\mathfrak{p}'$ consists only of zero divisors, whence $\mathfrak{p}'$ is contained in a prime divisor $\mathfrak{q}'$ of zero in F, whence depth $\mathfrak{q}' \leq$ depth $\mathfrak{p}'$ = depth $\mathfrak{p}^* <$ altitude R, and the zero ideal of F is not isobathy. Therefore we complete the proof.

A system of parameters $a_1, \ldots, a_r$ of a Noetherian ring R is called a *distinct system of parameters* of R if $\mu(\sum a_iR) =$ length $R/(\sum a_iR)$. (Note the inequality $\mu(\sum a_iR) \leq$ length $R/\sum a_iR$, which was proved in (24.3).) A *Macaulay local ring* is a local ring which has a distinct system of parameters. A Noetherian ring R is called a *locally Macaulay ring* if $R_{\mathfrak{m}}$ is a Macaulay local ring for every maximal ideal $\mathfrak{m}$ of R. A Noetherian ring R is called a *Macaulay ring* if it is a locally Macaulay ring and if height $\mathfrak{m}$ = altitude R for every maximal ideal $\mathfrak{m}$ of R.

(25.2) THEOREM: *A system of parameters $a_1, \ldots, a_r$ of a Noetherian ring R is distinct if and only if, in the form ring $F = \sum F_n$ of R with*

respect to $\mathfrak{a} = \sum a_i R$, x_i (a_i *modulo* $\mathfrak{a}^2$) ($i = 1, \ldots, r$) *are algebraically independent over* R_0 = $R/\mathfrak{a}$.

Proof: Let $P = \sum P_n$ be the homogeneous polynomial ring in indeterminates $X_1, \ldots, X_n$ over $R/\mathfrak{a}$. Then $\mu(P_1P) =$ length $R/\mathfrak{a}$ by (20.4). Let ϕ be the homomorphism from P onto F such that $\phi(X_i) = x_i$, and let $\mathfrak{n}$ be the kernel of ϕ. We have length $R/\mathfrak{a} = \mu(P_1P) = \mu(P_1P; \mathfrak{n}) + \mu(P_1P; F)$ by (23.3). Obviously, $\mu(P_1P; F)$ is equal to $\mu(\sum x_iF)$, which is equal to $\mu(\mathfrak{a})$ by (23.8). Therefore length $R/\mathfrak{a} = \mu(\mathfrak{a})$ if and only if $\mu(P_1P; \mathfrak{n}) = 0$. Assume that $\mathfrak{n} \neq 0$ and let f be a homogeneous element of $\mathfrak{n}$. Multiplying a suitable element of P_0 if necessary, we may assume that $f\mathfrak{m} = 0$ with a maximal ideal $\mathfrak{m}$ of P_0. Then $0{:}fP = \mathfrak{m}P$, and fP is isomorphic to $P/\mathfrak{m}P$, whence $\mu(P_1P; \mathfrak{n}) \geq \mu(P_1P; fP) = \mu(P_1P; (P_0/\mathfrak{m})[X_1, \ldots, X_r]) = 1$. Therefore, $\mu(P_1P; \mathfrak{n}) = 0$ if and only if $\mathfrak{n} = 0$, and the assertion is proved.

We have by (25.1) and (25.2) the following:

(25.3) COROLLARY: *If a semi-local ring R has a distinct system of parameters $a_1, \ldots, a_r$ of the Jacobson radical of R, then R is unmixed.*

(25.4) THEOREM: *A system of parameters $a_1, \ldots, a_r$ of the Jacobson radical of a semi-local ring R is distinct if and only if a_i is not a zero divisor modulo $\sum_1^{i-1} a_jR$ for each $i = 1, 2, \ldots, r$.*

Proof: Set $\mathfrak{a} = \sum_1^r a_iR$. We prove the assertion by induction on r. If $r = 0$, then the assertion is obvious because the empty set is a distinct system of parameters of a ring of altitude zero. Assume that $r \geq 1$. Assume at first that the a_i form a distinct system of parameters. Then, length $R/\mathfrak{a} \geq \mu(\mathfrak{a}/a_1R) \geq \mu(\mathfrak{a})$ by (24.3), whence the equalities hold, and the a_i modulo a_1R ($i = 2, \ldots, r$) form a distinct system of parameters of R/a_1R. Therefore, by induction, a_i is not a zero divisor modulo $\sum_1^{i-1} a_jR$ for each $i = 2, \ldots, r$. Thus it is sufficient to show that a_1 is not a zero divisor, which is obvious by virtue of (25.2). Conversely, assume that each a_i is not a zero divisor modulo $\sum_1^{i-1} a_jR$. Then a_1 is not a zero divisor and, by induction, the a_i modulo a_1R ($i \geq 2$) form a distinct system of parameters of R/a_1R. Let $F = \sum F_n$ be the form ring of R with respect to $\mathfrak{a}$, let $X_1, \ldots, X_r$ be indeterminates and let ϕ be the homomorphism from $P = (R/\mathfrak{a})[X]$ onto F such that $\phi(X_i) = a_i$ modulo $\mathfrak{a}^2$. Since the a_i modulo a_1R ($i \geq 2$) form a distinct system of parameters of R/a_1R, the form ring F^* of R/a_1R with respect to $\mathfrak{a}/a_1R$ may be identified with P/X_1P,

which shows that the kernel $\mathfrak{n}$ of ϕ is contained in X_1P and that F^* is identified with $F/\phi(X_1P)$. We have only to prove that $\mathfrak{n} = 0$. Assuming the contrary, let f be a homogeneous element of $\mathfrak{n} : X_1P$ which is not in $\mathfrak{n}$; such an f exists, because, otherwise $\mathfrak{n} = X_1\mathfrak{n}$ by (8.4), whence $\mathfrak{n} = 0$ by (3.10). Let d be the degree of f and let b be an element of $\mathfrak{a}^d$ such that $\phi(f) = b$ modulo $\mathfrak{a}^{d+1}$. $X_1f \in \mathfrak{n}$ implies that $a_1b \in \mathfrak{a}^{d+2}$. Starting with $b = b_1$, we construct a Cauchy sequence (b_n) such that $b_i - b_{i+1} \in \mathfrak{a}^{d+i}$ and such that $a_1b_i \in \mathfrak{a}^{d+i+1}$ as follows: When b_i is defined, let $g \in P$ be a homogeneous form of degree $d + i + 1$ such that $\phi(g) = a_1b_i$ modulo $\mathfrak{a}^{d+i+2}$. Since the kernel of the natural map from F onto F^* is $\phi(X_1P)$, we see that $g \in X_1P$, whence there is a homogeneous form g' of degree $d + i$ such that $g = X_1g'$. Let c be an element of $\mathfrak{a}^{d+i}$ such that $\phi(g') = c$ modulo $\mathfrak{a}^{d+i+1}$. Then $a_1b_i \equiv a_1c$ modulo $\mathfrak{a}^{d+i+2}$. Set $b_{i+1} = b_i - c$. Then $b_i - b_{i+1} = c \in \mathfrak{a}^{d+i}$, $a_1b_{i+1} = a_1b_i - a_1c \in \mathfrak{a}^{d+i+2}$, and b_{i+1} is defined. Now, let b^* be the limit of the sequence (b_i) in the completion R^* of R. Then we have $a_1b^* = 0$. Since a_1 is not a zero divisor in R hence in R^* by (18.1), we have $b^* = 0$, which is a contradiction to $b_i \notin \mathfrak{a}^{d+1}$, and the assertion that $\mathfrak{n} = 0$ is proved, whence the a_i form a distinct system of parameters.

(25.5) THEOREM: *If $a_1, \ldots, a_r$ form a distinct system of parameters of a Noetherian ring R and if a system of parameters $b_1, \ldots, b_r$ of R generate an ideal $\mathfrak{b}$ which has the same radical as $\mathfrak{a} = \sum a_iR$, then the b_i form a distinct system of parameters.*

Proof: By the nature of multiplicities, we may assume that R is a semi-local ring, and that the radical $\mathfrak{m}$ of $\mathfrak{a}$ is the Jacobson radical of R. Note that every maximal ideal of R has height r by (25.3). We note also that the distinctness is not the property of the members of system of parameters but is the property of the ideals generated by them. We prove the assertion by induction on r. If $r = 0$, then $\mathfrak{a} = \mathfrak{b} = 0$ and the assertion is obvious; if $r = 1$, then, since R is unmixed, b_1 is not a zero divisor, which proves the assertion by (25.4). Assume that $r > 1$. By the above remark, we may assume that $a_1R + b_1R$ has height 2. By (25.4), the a_i modulo $a_1R (i \geq 2)$ form a distinct system of parameters, whence by induction, every system of parameters of $\mathfrak{m}/a_1R$ is distinct, which means that every system of parameters of $\mathfrak{m}$ which has a_1 as a member is distinct. Since height $a_1R + b_1R = 2$, there is a system of parameters of $\mathfrak{m}$ having a_1 and b_1 as members, and it is distinct by the above result. Hence, applying

the above to b_1 and to this last system of parameters, we see that any system of parameters of $\mathfrak{m}$ which has b_1 as a member is distinct, and in particular the b_i form a distinct system of parameters.

We say that the *unmixedness theorem* holds in a Noetherian ring R if the following is true: If an ideal $\mathfrak{a}$ of R is generated by s elements and if height $\mathfrak{a} = s$ (s can be any non-negative integer) then every prime divisor of $\mathfrak{a}$ is of height s.

Under this terminology, we can state the following characterization of locally Macaulay rings.

(25.6) THEOREM: *A Noetherian ring R is a locally Macaulay ring if and only if the unmixedness theorem holds in R.*

Proof: Assume first that the unmixedness theorem holds in R, and let $\mathfrak{m}$ be an arbitrary maximal ideal of R. Let $a_1, \ldots, a_r$ ($r =$ height $\mathfrak{m}$) be elements of $\mathfrak{m}$ such that height $\sum_1^s a_i R = s$ for any $s \leq r$; the existence follows from (9.5). The validity of the unmixedness theorem implies that each a_i is not a zero divisor modulo $\sum_1^i a_j R$, whence modulo $\sum_1^i a_j R_{\mathfrak{m}}$, too. Therefore the a_i form a distinct system of parameters of $R_{\mathfrak{m}}$, and R is a locally Macaulay ring. Conversely, assume that R is a locally Macaulay ring, and assume that an ideal $\mathfrak{a}$ is generated by s elements $a_1, \ldots, a_s$ and that height $\mathfrak{a} = s$. Let $\mathfrak{m}$ be an arbitrary maximal ideal of R such that $\mathfrak{a} \subseteq \mathfrak{m}$. Then there is a system of parameters of $R_{\mathfrak{m}}$ which contains the a_i as a subset. By (25.5), we see that such a system of parameters is necessarily distinct, whence $R_{\mathfrak{m}}/\mathfrak{a}R_{\mathfrak{m}}$ has a distinct system of parameters by (25.4). It follows that $R_{\mathfrak{m}}/\mathfrak{a}R_{\mathfrak{m}}$ is unmixed by (25.3), whence $\mathfrak{a}R_{\mathfrak{m}}$ has no imbedded prime divisors. Since this is true for any $\mathfrak{m}$ containing $\mathfrak{a}$, we see that every prime divisor of $\mathfrak{a}$ is of height s by virtue of (9.3), and the unmixedness theorem holds in R; and the proof is complete.

Next we prove a characterization of Macaulay rings.

(25.7) THEOREM: *A Noetherian ring R is a Macaulay ring if and only if one of the following conditions is satisfied*:

(1) *Every system of parameters $a_1, \ldots, a_r$ of R is distinct.*

(2) *If maximal ideals $\mathfrak{m}$, $\mathfrak{m}'$ ($\mathfrak{m}$ may be equal to $\mathfrak{m}'$ if R is a local ring) of R are given, then there is a distinct system of parameters $a_1, \ldots, \ldots, a_r$ of R such that every a_i is in $\mathfrak{m} \cap \mathfrak{m}'$.*

Proof: Assume at first that R is a Macaulay ring. Let $a_1, \ldots, a_r$ be a system of parameters of R and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be all of the prime

divisors of $\mathfrak{a}$ $\sum a_i R$. Since R is a Macaulay ring, height $\mathfrak{m}_i$ multitude R, whence the a_i form a distinct system of parameters in each $R_{\mathfrak{m}_i}$, whence by (23.1)

$$\mu(\mathfrak{a}) = \sum_i \mu(\mathfrak{a}R_{\mathfrak{m}_i}) = \sum \text{length } R_{\mathfrak{m}_i}/\mathfrak{a}R_{\mathfrak{m}_i} = \text{length } R/\mathfrak{a},$$

and (1) is proved. It is obvious that (1) implies (2). Assume that (2) holds good. It is sufficient to show that R is a Macaulay ring. Let $\{a_1, \ldots, a_r\}$ be a distinct system of parameters and set $\mathfrak{a} = \sum a_i R$. Then $\mu(\mathfrak{a}) = \text{length } R/\mathfrak{a} = \sum \text{length } R_{\mathfrak{n}}/\mathfrak{a}R_{\mathfrak{n}}$, where $\mathfrak{n}$ runs through all prime divisors of $\mathfrak{a}$. On the other hand, by (23.1), $\mu(\mathfrak{a}) = \sum \mu(\mathfrak{a}R_{\mathfrak{n}'})$, where $\mathfrak{n}'$ runs through all prime divisors of $\mathfrak{a}$ such that height $\mathfrak{n}' = r$. Since length $R_{\mathfrak{n}'}/\mathfrak{a}R_{\mathfrak{n}'} \geq \mu(\mathfrak{a}R_{\mathfrak{n}'})$ by (24.3), we see that height $\mathfrak{n} = r$ for any $\mathfrak{n}$ and that the a_i form a distinct system of parameters of $R_{\mathfrak{n}}$. Hence (2) implies that height $\mathfrak{m}$ = height $\mathfrak{m}'$ and that $R_{\mathfrak{m}}$, $R_{\mathfrak{m}'}$ are Macaulay local rings for any two maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$, whence R is a Macaulay ring. Thus the proof is completed.

The following remark is immediate from the definition:

(25.8) *A semi-local ring R is a Macaulay ring or a locally Macaulay ring if and only if so is the completion of R.*

On the other hand:

(25.9) *If R is a locally Macaulay ring, then every ring of quotients of R is also a locally Macaulay ring.*

Proof: By the definition, it is sufficient to prove that $R_{\mathfrak{p}}$ is a Macaulay ring for any prime ideal $\mathfrak{p}$ of R. Let r be the height of $\mathfrak{p}$ and let $a_1, \ldots, a_r$ be elements of $\mathfrak{p}$ such that $\sum_1^s a_j R$ is of height s for any $s \leq r$ (by (9.5)). Since the unmixedness theorem holds in R, a_i is not a zero divisor modulo $\sum_1^{i-1} a_j R$ for each i, and therefore the a_i form a distinct system of parameters of $R_{\mathfrak{p}}$ by virtue of (25.4), which proves the assertion.

The following is a generalization of the classical unmixedness theorem, because a field is obviously a Macaulay ring:

(25.10) THEOREM: *Let $x_1, \ldots, x_n$ be algebraically independent elements over a Noetherian ring R. If R is a locally Macaulay ring then so is the polynomial ring $R[x]$.*

Proof: The general case follows easily from the case where $n = 1$, and we assume that $n = 1$. x_1 is denoted by x. It is sufficient to prove that if $\mathfrak{m}$ is a maximal ideal of $R[x]$, then $R[x]_{\mathfrak{m}}$ is a Macaulay local ring. Set $\mathfrak{p} = \mathfrak{m} \cap R$. Then $R_{\mathfrak{p}}$ is a Macaulay local ring. In order to

prove the assertion for $R[x]_{\mathfrak{m}}$, we may assume that $R = R_{\mathfrak{p}}$. $\mathfrak{m}/\mathfrak{p}R[x]$ is a maximal ideal of $(R/\mathfrak{p})[x]$, whence $\mathfrak{m}/\mathfrak{p}R[x]$ is generated by one element, say f'. Let f be an element of $\mathfrak{m}$ such that $f' = f$ modulo $\mathfrak{p}R[x]$. Let $a_1, \ldots, a_r$ be a distinct system of parameters of $R = R_{\mathfrak{p}}$. By (6.13) and (25.4), we see that $a_1, \ldots, a_r, f$ form a distinct system of parameters of $R[x]_{\mathfrak{m}}$, and the assertion is proved.

(25.11) COROLLARY: *Let $x_1, \ldots, x_n$ be algebraically independent elements over a Macaulay ring R. Then $R[x_1, \ldots, x_n]$ is again a Macaulay ring if and only if there is no prime ideal $\mathfrak{p}$ of R such that* (1) *$\mathfrak{p}$ is not maximal and* (2) *there is an element $a \notin \mathfrak{p}$ such that*

$$(R/\mathfrak{p})[1/(a \text{ modulo } \mathfrak{p})]$$

is the field of quotients of $R/\mathfrak{p}$.

Proof: The non-existence of $\mathfrak{p}$ as above is equivalent to the statement that every maximal ideal $\mathfrak{m}$ of the polynomial ring $R[x]$ lies over a maximal ideal $\mathfrak{n}$ of R, by virtue of (14.10). The proof of the *if* part: Since height $\mathfrak{m}/\mathfrak{n} = n$ by (14.5), we see that height $\mathfrak{m} \geq n +$ height $\mathfrak{n} = n +$ altitude R. Since altitude $R[x] = n +$ altitude R by (9.10), we see that height $\mathfrak{m}$ = altitude $R[x]$ for every maximal ideal $\mathfrak{m}$ of $R[x]$, and the assertion is proved by (25.10). The proof of the *only if* part: Assume the existence of such a $\mathfrak{p}$. Hence if follows that there is a maximal ideal $\mathfrak{m}$ of $R[x]$ such that $\mathfrak{n} = \mathfrak{m} \cap R$ is not maximal. Applying the above observation to $\mathfrak{m}(R_{\mathfrak{n}})[x]$, we see that height $\mathfrak{m}$ = height $\mathfrak{n} + n$. Therefore height $\mathfrak{m} <$ altitude $R + n =$ altitude $R[x]$, whence $R[x]$ is not a Macaulay ring.

The following two remarks are obvious by (25.4) and (12.9).

(25.12) *A Notherian ring R of altitude 1 is a Macaulay ring if and only if no maximal ideal is a prime divisor of zero. Any Noetherian ring of altitude zero is a Macaulay ring.*

(25.13) *A normal Noetherian ring R is a Macaulay ring if every maximal ideal of R is of height 2.*

We prove furthermore that:

(25.14) THEOREM: *A regular local ring is a normal Macaulay ring.*

Proof: Let $(R, \mathfrak{m})$ be a regular local ring and let $x_1, \ldots, x_r$ be a regular system of parameters of R. Then the form ring $F = \sum F_n$ is generated by r elements over the field $F_0 = R/\mathfrak{m}$, and altitude $F = r$ by (23.8). Therefore the r generators must be algebraically independent, whence R is a Macaulay ring. That R is a normal ring follows from the following lemma:

(25.15) *Let $(R, \mathfrak{m})$ be a local ring. If the form ring $F = \sum F_n$ of R with respect to $\mathfrak{m}$ is an integral domain, then R is an integral domain. If F is a normal ring, then R is a normal ring.*

Proof: $ab = 0$ $(a, b \in R)$ implies $a'b' = 0$ if a' and b' are $\mathfrak{m}$-forms of a and b. Therefore we have proved the first assertion. Next we assume that F is normal. Assume that a/b $(a, b \in R)$ is integral over R and let $c \neq 0$ be an element of the conductor $\mathfrak{c}$ of R in $R[a/b]$. We are to prove that $a \in bR + \mathfrak{m}^n$ for any n, by induction on n. We may assume that a, b are in $\mathfrak{m}$. Then the above is true for $n = 1$. Assume that $a \in bR + \mathfrak{m}^n$, *i.e.*, $a = bq + r$ with $q \in R, r \in \mathfrak{m}^n$. It is sufficient to show that $a \in bR + \mathfrak{m}^{n+1}$. If $r \in \mathfrak{m}^{n+1}$, then there is nothing to prove, and we assume that $r \notin \mathfrak{m}^{n+1}$. Since $a/b = q + (r/b)$, we have $c(r/b)^m \in R$ for any m, *i.e.*, $cr^m = b^m d_m$ with $d_m \in R$. Let c', r', b' and d_m' be $\mathfrak{m}$-forms of c, r, b, d_m respectively. Then $cr^m = b^m d_m$ implies that $c'r'^m = b'^m d_m'$ or $c'r'^m = 0$ or $b'^m d_m' = 0$. Since F is an integral domain, we see that $c'r'^m = b'^m d_m'$, whence $c'(r'/b')^m \in F$. Since this is true for any natural number m and since F is a normal Noetherian ring, we have $r'/b' \in F$. Then there is an element e of R such that the $\mathfrak{m}$-form of e is r'/b', which means that eb modulo $\mathfrak{m}^{n+1} = r'$, whence $r - eb \in \mathfrak{m}^{n+1}$, and, since $a = b(q + e) + (r - eb)$, we get $a \in bR + \mathfrak{m}^{n+1}$. Thus $a \in bR + \mathfrak{m}^n$ for any n, and $a \in \bigcap_n (bR + \mathfrak{m}^n) = bR$ (by 16.7)), whence $a/b \in R$. Thus the normality is proved.

Another interesting result on regular local ring is the following

(25.16) THEOREM: *Assume that $(R, \mathfrak{m})$ is a regular local ring and that a ring R' is a finite R-module and furthermore that R is a subring of R'. Then R' is a free module over R if and only if R' is a Macaulay ring.*

Proof: Let $y_1, \ldots, y_s$ be elements of R' whose residue classes modulo $\mathfrak{m}R'$ form a linearly independent base of $R'/\mathfrak{m}R'$ over $R/\mathfrak{m}$. Then $R' = \sum Ry_i$ by the lemma of Krull-Azumaya. Let $x_1, \ldots, x_r$ be a regular system of parameters of R. R' is a Macaulay ring if and only if the x_i form a distinct system of parameters of R', or equivalently $\mu(\mathfrak{m}R') = \text{length } R'/\mathfrak{m}R'$ namely

$$\mu_R(\mathfrak{m}R') = \text{length}_R R'/\mathfrak{m}R' = s.$$

Let F be a free R-module with free base $Y_1, \ldots, Y_s$ and let $\mathfrak{n}$ be the kernel of the homomorphism ϕ such that $\phi(Y_i) = y_i$. If $\mathfrak{n} \neq 0$, $\mathfrak{n}$ contains a free module. Therefore

$$\mu_R(\mathfrak{m}R') = \mu_R(\mathfrak{m}; F) - \mu_R(\mathfrak{m}; \mathfrak{n}) \leq s$$

and the equality holds if and only if $\mathfrak{u} = 0$, *i.e.*, R' is free. Thus the proof is complete.

On the other hand, the following is obvious from the definition:

(25.17) *Assume that the theorem of transition holds for the Noetherian rings R and R'. Then R is a Macaulay ring if and only if so is R'.*

We add here the following theorem, which is a corollary to (25.15):

(25.18) THEOREM: *Let R be a regular local ring. For an ideal $\mathfrak{a}$ of R, the ring $R/\mathfrak{a}$ is again regular if and only if $\mathfrak{a}$ is generated by a subset of a regular system of parameters of R.*

Proof: The *if* part is obvious. Assume that $R/\mathfrak{a}$ is regular. Then there is a regular system of parameters $x_1, \ldots, x_r$ of R such that

$$x_1, \ldots, x_s \in \mathfrak{a}$$

and such that the residue classes of $x_{s+1}, \ldots, x_r$ modulo $\mathfrak{a}$ form a regular system of parameters of $R/\mathfrak{a}$. Since $\sum_1^s x_i R$ is a prime ideal by (25.14) or (25.15), we see that $\mathfrak{a} = \sum_1^s x_i R$, which completes the proof.

EXERCISE: Assume that an ideal $\mathfrak{a}$ of a Macaulay ring R is generated by r elements and that height $\mathfrak{a} = r$. Prove that $R/\mathfrak{a}$ is a Macaulay ring.

CHAPTER IV

The Theory of Syzygies

26. Definition of syzygies

Let R be a Noetherian ring, usually a local ring, throughout this section.

Let $u_1, \ldots, u_n$ be elements of an R-module M and let $U_1, \ldots, U_n$ be indeterminates. The set N of elements $\sum a_i U_i$ $(a_i \in R)$ of the free module generated by the U_i such that $\sum a_i u_i = 0$ is an R-module, whence it is a finite R-module. This last R-module N is called the *relation module* of the elements u_i. Note that $(\sum RU_i)/N$ is naturally isomorphic to $\sum Ru_i$. When the u_i form a minimal basis for M, the relation module N of the u_i is called a *relation module* of M. Note that, in this last case, if R is a local ring with maximal ideal $\mathfrak{m}$, then $N \subseteq \sum \mathfrak{m}U_i$ as is easily seen by virtue of (5.3).

(26.1) THEOREM: *If R is a local ring, then a relation module of a given finite R-module M is unique up to isomorphism. If $v_1, \ldots, v_n$ is a basis for M, then the relation module N of the v_i is the direct sum of the relation module of M and a free module.*

Proof: The uniqueness of the relation module of M is an immediate consequence of (5.3). As for the last assertion, we may assume by virtue of (5.3) that $v_1, \ldots, v_m$ is a minimal basis for M. Let $V_1, \ldots, \ldots, V_n$ be indeterminates. For each $i > m$, there is a relation $v_i = \sum_{j=1}^{m} a_{ij} v_j$, whence the relation module N of the v_i contains an element $f_i = V_i - \sum_1^m a_{ij} V_j$. Since the V_i are free, we see that $f_{m+1}, \ldots, f_n$ generate a free submodule N^* of N. On the other hand, N contains the relation module N^{**} of $v_1, \ldots, v_m$, and N^{**} is the relation module of M. We are to prove that N is the direct sum of N^{**} and N^*. It is obvious that $N^* \cap N^{**} = 0$. Therefore it is sufficient to show that N is generated by N^* and N^{**}. Let $g = \sum b_i V_i$ be an arbitrary element of N. Then $g - \sum_{m+1}^{n} b_i f_i$ is in $RV_1 + \cdots + RV_m$, whence the element is in N^{**}. Thus $N = N^* + N^{**}$ and the assertion is proved.

By virtue of (26.1), when R is a local ring we can define the notion of *syzygies* of finite module as follows:

Let R be a local ring and let M be a finite R-module. The 0th syzygy of M is M itself; when the ith syzygy Z_i of M is defined, the $(i+1)$th syzygy of M is the relation module of Z_i. The ith syzygy of M is denoted by $\operatorname{syz}^i M$; if we want to express that M is an R-module, we write $\operatorname{syz}_R^i M$.

Even if R is not a local ring, we can give the following notion of a *weak syzygy sequence* of a finite R-module M: A sequence of finite R-modules Z_i $(i = 0, 1, 2, \dots)$ is a weak syzygy sequence of M if $Z_0 = M$ and if each $Z_i (i \geq 1)$ is the relation module of a finite basis for Z_{i-1}. Z_i is called a weak ith syzygy of M.

(26.2) *If $M = Z_0, Z_1, \dots, Z_n, \dots$ is a weak syzygy sequence of a finite module M, then, with an arbitrary, multiplicatively closed subset S of R such that $0 \notin S$, $Z_0 \otimes R_S, Z_1 \otimes R_S, \dots, Z_n \otimes R_S, \dots$ is a weak syzygy sequence of $M \otimes R_S$ over R_S.*

Proof: Let $u_1, \dots, u_n$ be a basis for Z_m such that the relation module of the u_j is Z_{m+1}. Let N be the relation module of the

$$u_i \otimes 1 \qquad (1 \in R_S).$$

It is obvious that $Z_{m+1} \otimes R_S$ is contained in N. In order to prove the converse inclusion, let $\sum a_i' U_i$ be an element of N, i.e.,

$$\sum a_i'(u_i \otimes 1) = 0.$$

Since the elements of S are mapped to units, we may assume that a_i' are images of elements a_i of R. Then $\sum a_i'(u \otimes 1) = 0$ implies that $\sum a_i u_i$ is in the kernel K of the natural map from M into $M \otimes R_s$, whence there is an element s of S such that $\sum a_i' s u_i = 0$, and $\sum a_i' U_i \in Z_{m+1} \otimes R_S$. Thus $N = Z_{m+1} \otimes R_S$, and the assertion is proved.

(26.3) *When R is a local ring, any weak ith syzygy Z of a finite module M is the direct sum of the ith syzygy of M and a free module, hence the relation module of Z coincides with* $\operatorname{syz}^{i+1} M$.

The proof is immediate from (26.1).

From now on, let R be a local ring. A finite module M is said to be of *homological dimension n* (over R) if $n+1$ is the smallest i such that $\operatorname{syz}^i M = 0$. In symbols, we write $\operatorname{hd} M = n$; when we want to express "over R" explicitly, we write hd_R. The definition implies that:

(26.4) *Let M be a finite module over the local ring R. Then*: (1)

hd M $\quad$ 1 *if and only if* $M \neq 0$, (2) hd $M = 0$ *if and only if* M *is a free module different from zero*, (3) *if* $M \neq 0$ *and if* F *is a free module, then* hd $M = \mathrm{hd}(M \oplus F)$, (4) $\mathrm{hd}(\mathrm{syz}^i M) = \max(-1, \mathrm{hd}\ M - i)$ *and* (5) *if* Z *is a weak* i*th syzygy of* M *then* hd Z *is equal to* hd $M - i$ *for* $i \leq$ hd M; *it is equal to either* 0 *or* -1 *for other* i.

(26.5) THEOREM: *If a submodule* N *of a finite module* M *is given, then, for each* n, *there is a weak* n*th syzygy* Z_n *of* M *and an isomorphism* σ *from* $\mathrm{syz}^n N$ *into* Z_n *such that* $Z_n/\sigma(\mathrm{syz}^n N)$ *is isomorphic to*

$$\mathrm{syz}^n (M/N).$$

Proof: By the definition of syzygies, we have only to prove the case where $n = 1$. Let $n_1, \ldots, n_r$ be a minimal base of N and let $m_1', \ldots, \ldots, m_s'$ be a minimal base of M/N. Let m_i be an element of M such that $m_i' = m_i$ modulo N. Let Z_1 be the relation module of the base $n_1, \ldots, n_r, m_1, \ldots, m_s$ of M. $\sum a_i M_i \in \mathrm{syz}^1 (M/N)$ if and only if $\sum a_i m_i' = 0$, that is, $\sum a_i m_i \in N$, or equivalently, $\sum a_i m_i + \sum b_j n_j = 0$ with some $b_j \in R$, whence $\mathrm{syz}^1 (M/N)$ is the image of Z_1 by the map ϕ such that $\phi(\sum a_i M_i + \sum b_j N_j) = \sum a_i M_i$. The kernel of ϕ is the set of elements of Z_1 of the form $\sum b_j N_j$, which is obviously the relation module of N, i.e., $\mathrm{syz}^1 N$. Thus the proof is complete.

(26.6) COROLLARY: *Among the homological dimensions of* N, M, *and* M/N, *one of the following must hold*: (1) hd $N \leq$ hd $M = \mathrm{hd}(M/N)$, (2) hd $M \leq$ hd $N = \mathrm{hd}(M/N) - 1$, or (3) $\mathrm{hd}(M/N) <$ hd $M =$ hd N.

Proof: Let Z_n be a weak syzygy of M such that $Z_n/\mathrm{syz}^n N = \mathrm{syz}^n (M/N)$. Case I: Assume that hd N is minimal among homological dimensions of M, N, M/N, and let n be hd N. Then Z_{n+1} is isomorphic to $\mathrm{syz}^{n+1} (M/N)$. Therefore, either hd $M =$ hd (M/N) or $\mathrm{syz}^{n+1} M = 0$. In the latter case Z_{n+1} is a free module, and therefore we see that, in case I, either (1) or (2) holds. Case II: Assume that hd M is minimal among the homological dimensions of M, N, M/N, and set $m =$ hd M. Since $\mathrm{syz}^m M$ is free, $\mathrm{syz}^m N$ is the relation module of a base of $\mathrm{syz}^m (M/N)$, hence either both $\mathrm{syz}^m (M/N)$ and $\mathrm{syz}^m N$ are free and different from zero or hd $(\mathrm{syz}^m N) =$ hd $(\mathrm{syz}^{m+1} (M/N))$, and therefore either (1) or (2) holds. Case III: The remaining case is where hd (M/N) is smaller than both hd N and hd M. Set $n' =$ hd (M/N). Then $Z_{n'+1}/\mathrm{syz}^{n'+1} N = 0$, i.e., $Z_{n'+1} = \mathrm{syz}^{n'+1} N$. By

our assumption that hd (M/N) is smaller than both hd N and hd M, we have (3). Thus the proof is complete.

EXERCISES: Let R be a Noetherian ring and consider finite modules over R.

We say that a module M is a *projective module* if $M \otimes R_{\mathfrak{m}}$ is free for any maximal ideal $\mathfrak{m}$ of R. The *homological dimension of* a module M is defined to be the maximum (or the supremum) of homological dimensions of $M \otimes R_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$.

1. Prove that hd $M \leq n (n \geq 0)$ if and only if an arbitrary weak nth syzygy of M is projective, or equivalently, if and only if a suitable weak nth syzygy of M is projective.

2. Prove that if Z and Z' are weak ith syzygies of the same module M, then there are free modules F and F' such that $Z \oplus F \cong Z' \oplus F'$.

3. Generalize (26.5) and (26.6) to our case.

4. In (26.2), assume that R' is a ring which is an R-module and such that $\otimes R'$ is exact. Prove that $Z_0 \otimes R', Z_1 \otimes R', \ldots, Z_n \otimes R', \ldots$ is a weak syzygy sequence of $M \otimes R'$.

27. *Change of Rings*

(27.1) THEOREM: *Let M be a finite module over a local ring $(R, \mathfrak{m})$ and let x be an element of $\mathfrak{m}$. Assume that x is not a zero divisor with respect to both R and M. Then for every natural number n, there is a natural isomorphism between* $(\mathrm{syz}^n M)/x(\mathrm{syz}^n M)$ and

$$\mathrm{syz}^n_{R/xR}\,(M/xM).$$

Proof: Using the induction on n, we have only to prove the case where $n = 1$. Let $u_1, \ldots, u_r$ be a minimal base of M. Then $u' = u_i$ modulo xM form a minimal base of M/xM. $\sum a_i' U_i \in \mathrm{syz}^1 (M/xM)$ if and only if $\sum a_i' u_i' = 0$, i.e., $\sum a_i u_i \in xM$ with a_i such that $a_i' = a_i$ modulo xR, namely $\sum a_i u_i = \sum x b_i u_i$. Thus the map ϕ such that $\phi(\sum a_i U_i) = \sum (a_i \text{ modulo } xR) U_i$ is a homomorphism from $\mathrm{syz}^1 M$ onto $\mathrm{syz}^1_{R/xR} M/xM$. The kernel of ϕ is the set of elements $\sum x a_i U_i$ such that $\sum x a_i u_i = 0$, whence $\sum a_i u_i = 0$ because x is not a zero divisor with respect to M. Thus the kernel of ϕ is $x(\mathrm{syz}^1 M)$, and the assertion is proved.

We say that a sequence of elements $x_1, \ldots, x_r$ of the maximal ideal $\mathfrak{m}$ of a local ring R is an *M-sequence*, M being an R-module, if x_i is not a zero divisor with respect to $M/\sum_1^{i-1} x_j M$ for each $i = 1, \ldots, r$. Then we have:

(27.2) COROLLARY: *Let M be a finite module over a local ring $(R, \mathfrak{m})$. If $x_1, \ldots, x_s$ is an M-sequence and at the same time an R-sequence, then* $\mathrm{hd}_R M = \mathrm{hd}_{R/\mathfrak{a}} M/\mathfrak{a}M$ *with* $\mathfrak{a} = \sum x_i R$.

(27.3) THEOREM: *Let M be a finite module over a local ring $(R, \mathfrak{m})$ and let x be an element of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$. Assume furthermore that x is not a zero divisor in R, that M is contained in a free module $F = \sum RU_i$ ($U_1, \ldots, U_r$ being a free base of F) and that $xF \subseteq M \subseteq \mathfrak{m}F$. Then, for each natural number n, $\operatorname{syz}^n M$ can be imbedded in a free module F_n in such a way that $xF_n \subseteq \operatorname{syz}^n M \subseteq \mathfrak{m}F_n$ and such that $(\operatorname{syz}^n M)/xF_n$ is naturally isomorphic to $\operatorname{syz}^n_{R/xR}(M/xF)$.*

Proof: Using induction on n, we have only to prove the case where $n = 1$. Let $a_1', \ldots, a_s'$ be a minimal basis for M/xF and let $a_1, \ldots, a_s$ be elements of M such that $a_i' = a_i$ modulo xF. Then $a_1, \ldots, a_s, xU_1, \ldots, xU_r$ is a basis for M. They really form a minimal basis for M, since otherwise there would be a relation $c_1a_1 + \cdots + c_sa_s + d_1xU_1 + \cdots + d_rxU_r = 0$ with some $c_i \notin \mathfrak{m}$ or some $d_j \notin \mathfrak{m}$. If some $c_i \notin \mathfrak{m}$, then this contradicts the fact that the a_i' form a minimal basis for M/xF; if some $d_j \notin \mathfrak{m}$, then the coefficient of U_j in $\sum c_ia_i$ is not in $\mathfrak{m}^2$, whence some $c_i \notin \mathfrak{m}$ (because $M \subseteq \mathfrak{m}F$) which is not the case. Thus the a_i and the xU_j form a minimal basis for M. $\operatorname{syz}^1 M$ is therefore the relation module of $a_1, \ldots, a_r, xU_1, \ldots, xU_s$. $\sum c_iA_i + \sum b_jV_j \in \operatorname{syz}^1 M$ if and only if $\sum c_ia_i + \sum b_jxU_j = 0$. Let σ be the map from $\operatorname{syz}^1 M$ into $F_1 = \sum RA_i$ such that $\sigma(\sum c_iA_i + \sum b_jV_j) = \sum c_iA_i$. This σ is obviously a homomorphism. Element of the kernel of σ is $\sum b_jV_j$ with $\sum b_jxU_j = 0$. Since x is not a zero divisor and since U_j are free, we have $b_j = 0$ and therefore σ is an isomorphism. Since the a_i and the xU_j form a minimal basis, we have $\sigma(\operatorname{syz}^1 M) \subseteq \mathfrak{m}F_1$. Since $xa_i \in xF$, we have $xA_i \in \sigma(\operatorname{syz}^1 M)$. Thus $xF_1 \subseteq \sigma(\operatorname{syz}^1 M) \subseteq \mathfrak{m}F_1$. $\sum c_i'A_i \in \operatorname{syz}^1_{R/xR}(M/xF)$ if and only if $\sum c_iA_i \in xF$ with c_i such that $c_i' = c_i$ modulo xR, or equivalently $\sum c_iA_i \in \sigma(\operatorname{syz}^1 M)$. Thus we see that

$$\operatorname{syz}^1_{R/xR}(M/xF) = \sigma(\operatorname{syz}^1 M)/xF_1,$$

and the assertion is proved completely.

(27.4) COROLLARY: *With the same notation and assumptions as in (27.3) above, we have* $\operatorname{hd}_R M = 1 + \operatorname{hd}_{R/xR} M/xF$, *except for the case where* $F = 0$.

Proof: If both $\operatorname{hd} M$ and $\operatorname{hd} M/xF$ are infinite, then the assertion is obvious. Therefore, we assume that one of them is finite and we prove the corollary by induction on the finite homological dimension. $\operatorname{hd}_{R/xR} M/xF = -1$ if and only if $M/xF = 0$, i.e., $M = xF$, or equivalently $\operatorname{hd} M = 0$ because, in the notation in the proof of (27.3) the

a_i and xU_i form a minimal basis for M. Since the assumption in (27.3) holds for $\mathrm{syz}^1 M$ and since $\mathrm{syz}^1_{R/xR}(M/xM) \cong \mathrm{syz}^1(M/xF_1)$, we prove the assertion by induction.

(27.5) COROLLARY: *With the same* R, $\mathfrak{m}$, *and* x *as above, let* M *be a finite* R*-module such that* $xM = 0$. *Then* $\mathrm{hd}_R M = 1 + \mathrm{hd}_{R/xR} M$, *except for the case where* $M = 0$.

Proof: Let $u_1, \ldots, u_r$ be a minimal base of M. $\sum c_i U_i \in \mathrm{syz}^1_R M$ if and only if $\sum c_i u_i = 0$. Then with $F = \sum RU_i$, we have $xF \subseteq \mathrm{syz}^1_R M \subseteq \mathfrak{m}F$, and $\mathrm{syz}^1_{R/xR} M = (\mathrm{syz}^1_R M)/xF$. Therefore, we can prove the assertion, using (27.4).

We give, by the way, some results on M-sequences.

Let $(R, \mathfrak{m})$ be a local ring and let M be a finite R-module. For an M-sequence $x_1, \ldots, x_r$ the number r is called the *length* of the M-sequence. An M-sequence $x_1, \ldots, x_r$ is called a *maximal* M-sequence if there is no element $y \in \mathfrak{m}$ such that $x_1, \ldots, x_r, y$ is an M-sequence.

(27.6) *With the notation as above, if* $x_1, \ldots, x_r$ *is an* M*-sequence, then any permutation of the* x_i *is an* M*-sequence.*

Proof: If we show that x_1 and x_2 permute with each other, then the general case follows immediately, using the induction on r from the fact that $x_2, \ldots, x_r$ is an (M/x_1M)-sequence. Thus we are to prove the permutability of x_1 and x_2. Assume that $x_2 m = 0 \, (m \in M)$. Then, since $x_2 m \in x_1 M$, we have $m \in x_1 M : x_2 R = x_1 M$, and $m = x_1 m'$ with $m' \in M$. Thus $x_1 x_2 m' = 0$. Since x_1 is not a zero divisor with respect to M, $x_2 m' = 0$. Thus we have $0 : x_2 R$ (in M) is contained in $x_1(0 : x_2 R)$, whence by the lemma of Krull-Azumaya, we have

$$0 : x_2 R = 0,$$

i.e., x_2 is not a zero divisor with respect to M. Assume that $m \in x_2 M : x_1 R$. Then $x_1 m = x_2 m'$ with $m' \in M$. Then $m' \in x_1 M : x_2 R = x_1 M$, i.e., $m' = x_1 m'' \, (m'' \in M)$. Then $x_1 m = x_1 x_2 m''$. Since x_1 is not a zero divisor with respect to M, we have $m = x_2 m''$, and $x_2 M : x_1 R \subseteq x_2 M$. Thus $x_2, x_1, x_3, \ldots, x_r$ is an M-sequence.

(27.7) *With the same notation as above, if there is an* M*-sequence* $x_1, \ldots, x_r$, *then there is an* M*-sequence* $y_1, \ldots, y_r$ *such that their residue classes modulo* $\mathfrak{m}^2$ *are linearly independent over the field* $R/\mathfrak{m}$; *if the* x_i *form a maximal* M*-sequence, then so do the* y_i.

Proof: Assume that $x_1, \ldots, x_s$ (s may be zero) modulo $\mathfrak{m}^2$ are linearly independent. In that case, let $y_1, \ldots, y_s$ be the $x_1, \ldots, x_s$.

We prove the assertion by induction on such an s. If $s = r$, then there is nothing to prove. Assume therefore $s > r$. Set $\mathfrak{a} = \sum_1^r x_i R$. Since x_r is not a zero divisor with respect to $M/\mathfrak{a}M$, there is an element y of $\mathfrak{m}$ which is not in $\mathfrak{a} + \mathfrak{m}^2$ (or rather, $(\mathfrak{a}M:M) + \mathfrak{m}^2$) such that y is not a zero divisor with respect to $M/\mathfrak{a}M$, because of the fact that the set of zero divisors with respect to $M/\mathfrak{a}M$ is the union of a finite number of prime ideals (see Exercise 1 in §8). Then $x_1, \ldots, x_{r-1}, y$ is an M-sequence, and we are reduced to the case of greater s (by (27.6)). Thus it remains only to prove that if the x_i form a maximal M-sequence, then so do $x_1, \ldots, x_{r-1}, y$. Considering $M/\mathfrak{a}M$ and $R/(\mathfrak{a}M:M)$, we may assume that $r = 1$ and that M is faithful. That x_1 is a maximal M-sequence implies that every element of $\mathfrak{m}$ is a zero divisor with respect to M/x_1M, whence there is an element m of M which is not in x_1M but is in $x_1M:\mathfrak{m}$ (cf. Exercise 1 in §8). Then $ym = x_1m'$ for an $m' \in M$. If $m' = ym^*$ for an $m^* \in M$, then $m = xm^*$ which is not the case. Therefore $m' \notin yM$. Let z be an arbitrary element of $\mathfrak{m}$. Then $zm = xm''$ for an $m'' \in M$, whence $xym'' = yzm = xzm'$, and $ym'' = zm'$. Thus $z \in yM:m'R$. Thus every element of $\mathfrak{m}$ is a zero divisor with respect to M/yM, and the maximality of y is proved. Thus (27.7) is proved completely.

(27.8) COROLLARY: *Maximal M-sequences have the same length.*

Proof: Assume that $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ are maximal M-sequences. We prove that $r = s$ by induction on r. If $r = 0$, then the assertion is obvious; if $r = 1$, this has been proved in the last step of the proof of (27.7). Assume now that $r > 1$. Then the union of the sets of zero divisors with respect to M/x_1M and M/y_1M does not cover $\mathfrak{m}$, whence there is an element z such that both x_1, z and y_1, z form M-sequences. Let $x_1, z, z_3, \ldots, z_t$ and $y_1, z, w_3, \ldots, w_u$ be maximal M-sequences. Considering M/x_1M, we have $r = t$ by induction. Considering M/zM, we have $t = u$, and, considering M/y_1M, we have $u = s$. Thus $r = s$, which completes the proof.

EXERCISES: Let M be a finite module over a Noetherian ring and let $\mathfrak{a}$ be an ideal of R. Then the notion of *M-sequence* in $\mathfrak{a}$ is defined similarly using $\mathfrak{a}$ instead of $\mathfrak{m}$ in the previous definition.

1. Confirm that, under the assumption that $M/\mathfrak{a}M \neq 0$, (27.6) and (27.8) can be generalized to such a case.

2. Prove (27.2) when R is a semi-local ring and when the x_i are in the Jacobson radical.

3. Adapt (27.4) to the case of semi-local rings.

28. Regular local rings

We begin with a lemma:

(28.1) *Let* $(R, \mathfrak{m})$ *be a local ring. If* $0 : \mathfrak{m} \neq 0$, *then* hd $M = \infty$ *for every finite module* M *which is not free.*

Proof: Assume that hd $M = n < \infty$ and that $n \geq 1$. Then syz^n M is free and different from zero. Since syz^n M is the relation module of syz^{n-1} M, there is a free module F such that syz^n $M \subseteq \mathfrak{m}F$, whence $(0 : \mathfrak{m})(\text{syz}^n\ M) = 0$, which is a contradiction.

Now we prove:

(28.2) Theorem: *Let* $(R, \mathfrak{m})$ *be a local ring. If* hd $\mathfrak{m}$ *is finite, then* R *is regular. Conversely, if* R *is a regular local ring, then for every finite* R*-module* M *different from zero, we have* hd M = altitude $R - s$, *where* s *is the length of a maximal* M*-sequence.*

Proof: Assume that hd $\mathfrak{m}$ is finite. We prove the regularity of R by induction on r = altitude R. We begin with the following remark: If $0 : \mathfrak{m} \neq 0$, then $\mathfrak{m}$ must be free by (28.1), whence $\mathfrak{m} = 0$ because $0 : \mathfrak{m} \neq 0$. Therefore, R is a field in this case. Now, if $r = 0$, then $0 : \mathfrak{m} \neq 0$, and the assertion is proved already. Assume that $r > 0$. Then by the above remark, we have $0 : \mathfrak{m} = 0$. Therefore, there is an element x of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$ such that x is not a zero divisor. Then hd $\mathfrak{m} = \text{hd}_{R/xR}\ \mathfrak{m}/xR + 1$ by (27.4), whence R/xR is regular by induction. Therefore we see that R is also a regular local ring by (9.11). Conversely, assume that R is a regular local ring and let M be a finite R-module different from zero. Let $x_1, \ldots, x_s$ be a maximal M-sequence. We may assume, by (27.7), that $x_s \notin \mathfrak{m}^2$ if $s \geq 1$. We prove the equality hd $M = r - s$ (r = altitude R) by induction on r. If $r = 0$, then R is a field, and M is free (s is obviously zero). Thus this case is obvious. Assume that $r \geq 1$. If $s \geq 1$, then hd M = $\text{hd}_{R/x_sR}\ M/x_sM$ by (27.2), whence by induction hd $M = (r - 1) - (s - 1) = r - s$. If $s = 0$, then M is not free, whence syz^1 $M \neq 0$ and hd $M = 1 +$ hd syz^1 M. Since syz^1 M is contained in a free module, $y \in \mathfrak{m}$ $(y \neq 0)$ forms an (syz^1 M)-sequence; if it is maximal, then by the above proof, we have hd (syz^1 M) $= r - 1$, and hd $M = r$. Thus, it is sufficient to prove that every element z of $\mathfrak{m}$ is a zero divisor with respect to (syz^1 M)/y(syz^1 M). Let F be a free module such that F/(syz^1 M) $\cong M$. Since z is a zero divisor with respect to M, there is an element a of F which is not in syz^1 M such that $za \in$ syz^1 M, whence $yza \in y$(syz^1 M). But $ya \notin y$(syz^1 M) because y is

not a zero divisor and because $a \notin \mathrm{syz}^1 M$. Therefore, z is a zero divisor with respect to $(\mathrm{syz}^1 M)/y(\mathrm{syz}^1 M)$, and the proof is complete.

(28.3) COROLLARY: *If* $\mathfrak{p}$ *is a prime ideal of a regular local ring* R, *then* $R_{\mathfrak{p}}$ *is a regular local ring.*

Proof: $\mathrm{hd}\ \mathfrak{p}$ is finite, whence $\mathrm{hd}_{R_{\mathfrak{p}}}\ \mathfrak{p}R_{\mathfrak{p}}$ is finite by (26.2), which proves the assertion.

Let $(R, \mathfrak{m})$ be a regular local ring and let p be the characteristic of $R/\mathfrak{m}$. R is called an *unramified regular local ring* if either R contains a field or $p \notin \mathfrak{m}^2$. Namely, R is unramified if and only if R/pR is regular. Now we have:

(28.4) *If* $\mathfrak{p}$ *is a prime ideal of an unramified regular local ring* R, *then* $R_{\mathfrak{p}}$ *is an unramified regular local ring.*

Proof: Let p be the characteristic of the residue class field of R. If $pR \nsubseteq \mathfrak{p}$, then $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is of characteristic zero, whence $R_{\mathfrak{p}}$ contains the rational number field, and $R_{\mathfrak{p}}$ is unramified in this case. Assume that $pR \subseteq \mathfrak{p}$. Since R/pR is regular, we see that $(R/pR)_{\mathfrak{p}/pR} = R_{\mathfrak{p}}/pR_{\mathfrak{p}}$ is regular by (28.3), and the assertion is proved.

(28.5) *Let* $(R, \mathfrak{m})$ *be a local ring and let* $\mathfrak{a}$ *be an ideal of* R. *Assume that* $\mathfrak{a} = xR{:}yR$ $(x \in \mathfrak{a},\ y \in R)$ *and that* $x \notin \mathfrak{a}\mathfrak{m}$. *If* $\mathrm{hd}\ \mathfrak{a} \leq 1$, *then* $\mathfrak{a} = xR$.

Proof: Assume the contrary. Since $x \notin \mathfrak{a}\mathfrak{m}$, there is a minimal basis $x, a_1, \ldots, a_n$ for $\mathfrak{a}$. Let b be such that $xb = ya_1$. By the assumption $\mathrm{syz}^1\ \mathfrak{a} = \{cX + \sum c_iA_i \mid cx + \sum c_ia_i = 0\}$ is a free module. Let $f_1, \ldots, f_m$ be a free basis for $\mathrm{syz}^1\ \mathfrak{a}$. $\mathrm{syz}^1\ \mathfrak{a}$ contains elements $a_1X - xA_1$ and $bX - yA_1$, whence there are elements d_{ij} such that $a_1X - xA_1 = \sum_j d_{1j}f_j$ and $bX - yA_1 = \sum_j d_{2j}f_j$. $y(a_1X - xA_1) = xbX - xyA = x(bX - yA)$, whence we have $yd_{1j} = xd_{2j}$ for any j, which implies that $d_{1j} \in xR{:}y = \mathfrak{a}$, whence the coefficients of $d_{1j}f_j$ are in $\mathfrak{a}\mathfrak{m}$, which implies that x is in $\mathfrak{a}\mathfrak{m}$ because $a_1X - xA_1 = \sum d_{1j}f_j$, which is a contradiction and we prove the assertion.

(28.6) *Let* x *and* y *be elements of a ring* R. *If* x *is not a zero divisor, then either* $xR + yR$ *is principal or* $\mathrm{hd}\ (xR + yR) = 1 + \mathrm{hd}\ (xR{:}yR)$.

Proof: Assume that $xR + yR$ is not principal, then, since $\mathrm{hd}\ xR = 0$, we have by (26.6) that $\mathrm{hd}\ (xR + yR) = \mathrm{hd}\ (xR + yR)/xR$, whence it is equal to $\mathrm{hd}\ R/(xR{:}yR)$ by (1.5), and the assertion is proved by the fact that $xR{:}yR = \mathrm{syz}^1\ R/(xR{:}yR)$.

(28.7) THEOREM: *An arbitrary regular local ring* $(R, \mathfrak{m})$ *is a unique factorization ring.*

Proof: Let r be the altitude of R and let $\mathfrak{p}$ be an arbitrary prime ideal of height 1 in R. We have only to prove that $\mathfrak{p}$ is principal. If $r \leq 1$, then the assertion is obvious. Assume that $r \geq 2$. If $z \in \mathfrak{m}$ is not in $\mathfrak{p}$, then z forms an $R/\mathfrak{p}$-sequence, which implies that $\operatorname{hd} R/\mathfrak{p} \leq r - 1$, hence $\operatorname{hd} \mathfrak{p} \leq r - 2$ because $\mathfrak{p} = \operatorname{syz}^1 R/\mathfrak{p}$. If $r = 2$, then $\operatorname{hd} \mathfrak{p} = 0$ and $\mathfrak{p}$ is principal. Assume that $r \geq 3$. Let x be an element of $\mathfrak{p}$ which is not in $\mathfrak{p}\mathfrak{m}$. Since $\mathfrak{p}$ is a minimal prime divisor of xR, there is an element $y \in R$ such that $xR:yR = \mathfrak{p}$. Therefore, if $r = 3$, we see that $\mathfrak{p}$ is principal by (28.5). Thus we assume that $r \geq 4$, and we use induction on r. Set $\mathfrak{a} = xR + yR$. Since x is irreducible, if $\mathfrak{a}$ is principal, then $yR = R$, and $\mathfrak{p}$ is principal. Therefore, we assume that $\mathfrak{a}$ is not principal. Let t be so large that $\mathfrak{a}':\mathfrak{m} = \mathfrak{a}'$ with $\mathfrak{a}' = \mathfrak{a}:\mathfrak{m}^t$. Let z be an element of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$ such that $\mathfrak{a}':zR = \mathfrak{a}'$. $R' = R/zR$ is regular, hence it is a unique factorization ring by induction. Therefore $\operatorname{hd}_{R'} (\mathfrak{a} + zR)/zR \leq 1$ by (28.6), whence $\operatorname{hd}_{R'} (R/\mathfrak{a} + zR) \leq 2 <$ altitude R', which implies in particular that

$$(\mathfrak{a} + zR)/zR:\mathfrak{m}/zR = (\mathfrak{a} + zR)/zR,$$

by (28.2), whence $(\mathfrak{a} + zR):\mathfrak{m} = \mathfrak{a} + zR$. Therefore $\mathfrak{a}' = \mathfrak{a}:\mathfrak{m}^t \subseteq (\mathfrak{a} + zR):\mathfrak{m}^t = \mathfrak{a} + zR$. Since $\mathfrak{a}':zR = \mathfrak{a}'$, $\mathfrak{a}' \subseteq \mathfrak{a} + zR$ implies that $\mathfrak{a}' = \mathfrak{a}$ by (4.3). Therefore, there is a maximal $R/\mathfrak{a}$-sequence $x_0, \ldots, x_s$ such that $x_0 = z$. Then $x_1, \ldots, x_s$ is a maximal $R/(\mathfrak{a} + zR)$-sequence. Since $\operatorname{hd}_{R'} R/(\mathfrak{a} + zR) \leq 2$, we have $s \geq r - 1 - 2 = r - 3$, whence $\operatorname{hd}_R R/\mathfrak{a} \leq 2$, and $\operatorname{hd} \mathfrak{a} \leq 1$. Since we assumed that $\mathfrak{a}$ is not principal, we have $\operatorname{hd} \mathfrak{a} = 1$, whence $\operatorname{hd} \mathfrak{p} = 0$ by (28.6) and $\mathfrak{p}$ is principal. Thus the proof is complete.

We say that a Noetherian ring R is a *regular ring* if $R_{\mathfrak{m}}$ is a regular local ring for every maximal ideal $\mathfrak{m}$ of R. Under this definition, one can assert the following corollary:

(28.8) COROLLARY: *A regular semi-local integral domain is a unique factorization ring.*

This follows immediately from the following lemma:

(28.9) *Let $(R, \mathfrak{m}_1, \ldots, \mathfrak{m}_n)$ be a semi-local integral domain. If every $R_i = R_{\mathfrak{m}_i} (i = 1, \ldots, n)$ is a unique factorization ring, then R is a unique factorization ring.*

Proof: Let $\mathfrak{p}$ be an arbitrary prime ideal of height 1 in R. Then $\mathfrak{p}R_i$ is generated by an element p_i of $\mathfrak{p}$. Let a_i be an element of $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{i-1} \cap \mathfrak{m}_{i+1} \cap \cdots \cap \mathfrak{m}_n$ which is not in $\mathfrak{m}_i$. Then $\mathfrak{p}R_i$ is generated by $p_i a_i$. Set $p = \sum p_i a_i$. Then since $p_j a_j \in \mathfrak{p}\mathfrak{m}_i R_i$ for $i \neq j$,

we see that p generates pR_i for every i, whence $\mathfrak{p} = pR$ by (8.9), and the assertion is proved.

We add, here, some remarks on non-regular local rings.

(28.10) *Let $(R, \mathfrak{m})$ be a local ring. Assume that an $x \in \mathfrak{m}$ is not a zero divisor. Then for a finite module $M \neq 0$, it holds that* $\operatorname{hd}_R M = 1 + \operatorname{hd}_{R/xR}(\operatorname{syz}^1 M)/x(\operatorname{syz}^1 M)$.

Proof: $\operatorname{hd}_R M = 1 + \operatorname{hd}_R \operatorname{syz}^1 M$. Since x is not a zero divisor and since $\operatorname{syz}^1 M$ is a submodule of a free module, we see that $\operatorname{hd}_R \operatorname{syz}^1 M = \operatorname{hd}_{R/xR}(\operatorname{syz}^1 M)/x(\operatorname{syz}^1 M)$ by (27.2), and the assertion is proved.

(28.11) THEOREM: *Let $(R, \mathfrak{m})$ be a local ring and let $M(\neq 0)$ be a finite R-module. Let s be the length of a maximal M-sequence. If* hd M *is finite, then* hd $M + s$ *is equal to the length t of a maximal R-sequence.*

Proof: We prove the assertion by induction on t. If $t = 0$, then $0 : \mathfrak{m} \neq 0$, and the assertion is true by (28.1). Assume that $t > 0$, and let $x_1, \ldots, x_t$ be a maximal R-sequence. If $s \neq 0$, then we may assume that x_1 is not a zero divisor with respect to M by virtue of (27.8). Then $\operatorname{hd}_R M = \operatorname{hd}_{R/x_1R} M/x_1M$. $(x_2 \text{ modulo } x_1R), \ldots, (x_t \text{ modulo } x_1R)$ is a maximal R/x_1R-sequence, and if $x_1, y_2, \ldots, y_s$ is a maximal M-sequence, then $(y_2 \text{ modulo } x_1R), \ldots, (y_s \text{ modulo } x_1R)$ is a maximal M/x_1M-sequence by definition. Thus we have settled this case. Assume that $s = 0$. We can prove that x_1 forms a maximal $(\operatorname{syz}^1 M)$-sequence, in the same way as in the last step of the proof of (28.2) (with $y = x_1$). Therefore, by the case where $s > 0$, we see that hd $\operatorname{syz}^1 M + 1 = t$, and hd $M = t$, which completes the proof.

EXERCISES: *1.* Let $\mathfrak{a}$ be an ideal of a regular local ring R. Prove that if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are all of the prime divisors of $\mathfrak{a}$, then *hd* $\mathfrak{a}$ is not greater than the maximum of the depth $\mathfrak{p}_i + 1$.

2. Let R be a Noetherian ring. Prove the equivalence of the following conditions: (1) hd $M \leq n$ for every finite module M, (2) R is a regular ring such that altitude $R \leq n$.

3. Assume that M is a finite $R/\mathfrak{a}$-module ($\mathfrak{a}$ being an ideal of a local ring R). Prove that $\operatorname{hd}_{R/\mathfrak{a}} M + \operatorname{hd}_R R/\mathfrak{a} = \operatorname{hd}_R M$, provided that each of them is finite.

29. *Syzygies of graded modules*

Since there is a very close relation between graded rings and semi-local rings or between graded rings over local rings and local rings, we add some remarks on syzygies of graded modules.

Let $R = \sum R_n$ be a graded Noetherian ring such that R_0 is a local

ring with maximal ideal $\mathfrak{m}_0$. Set $\mathfrak{m} = \mathfrak{m}_0 + \sum_{n>0} R_n$. $\mathfrak{m}$ is obviously a maximal ideal. Let M be a finite graded module.

We define a *syzygy sequence* of M as follows: The first member, which may be denoted by $\mathrm{syz}^0 M$, is M itself. When the nth member $\mathrm{syz}^{n-1} M$, which is a graded finite module, is defined, we define the $(n+1)$st member $\mathrm{syz}^n M$ as follows: Let $u_1, \ldots, u_r$ be a minimal basis for $\mathrm{syz}^{n-1} M$ consisting only of homogeneous elements, of degree, say, $d_1, \ldots, d_r$. Let $U_1, \ldots, U_r$ be indeterminates and consider the relation module $N = \{\sum a_i U_i \mid \sum a_i u_i = 0\}$. If we regard U_i as an element of degree d_i, then N is a graded module. This graded module N is defined to be $\mathrm{syz}^n M$. Then:

(29.1) *Every* $\mathrm{syz}^n M$ *is unique up to isomorphism.*

Proof: If $v_1, \ldots, v_s$ is another similar basis for M and if $d_i' = \deg v_i$, then we see, first, that there is a linear transformation from the members of u_i with smallest d_i to such ones of the v_i, hence the same can be generalized to be the case of the u_i with d_i at most the second smallest and such ones of the v_i, and so on, and we see that $r = s$ and there is a linear transformation which maps the u_i onto the v_i, whence $\mathrm{syz}^n M$ is independent of the choice of bases.

Thus "syzygy sequence" is well defined, and therefore the same treatment as in the case of local rings can be applied. But we need not repeat the same again, because of the following theorem.

(29.2) THEOREM: *With the same notation as above, we set* $R^* = R_{\mathfrak{m}}$. *Then* $\mathrm{syz}^n_{R^*}(M \otimes R^*)$ *is naturally isomorphic to* $(\mathrm{syz}^n_R M) \otimes R^*$.

Proof: Since we are considering graded modules, any element a of R which is not in $\mathfrak{m}$ is not a zero divisor with respect to modules, whence M is naturally contained in $M \otimes R^*$. One can see easily that a minimal basis for M consisting of homogeneous elements becomes a minimal basis for $M \otimes R^*$, whence we see easily that $\mathrm{syz}^1_{R^*}(M \otimes R^*)$ is naturally isomorphic to $(\mathrm{syz}^1_R M) \otimes R^*$. Applying the same to $\mathrm{syz}^n_R M$ instead of M, we prove the assertion.

By virtue of the above results, one can state a generalization of the classical syzygy theorem of Hilbert as follows:

(29.3) THEOREM: *Let R be the homogeneous polynomial ring in algebraically independent elements $x_1, \ldots, x_n$ over a regular local ring R_0. Then for any finite graded module M over R,* hd M *is at most* $n +$ altitude R_0, *and with* $t = \mathrm{hd}\, M$, *we have* $\mathrm{syz}^{t+1} M = 0$.

CHAPTER V

Theory of Complete Local Rings and Its Application

30. Some properties of complete local rings

(30.1) THEOREM: *Let R be a complete semi-local ring with Jacobson radical $\mathfrak{m}$. If $\mathfrak{a}_n (n = 1, 2, 3, \dots)$ are ideals of R such that $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ for any n and such that $\bigcap_n \mathfrak{a}_n = 0$, then for any given natural number n, there exists a natural number $m(n)$ such that $\mathfrak{a}_{m(n)} \subseteq \mathfrak{m}^n$.*

Proof: Assume the contrary, namely, assume that there is a natural number r such that $\mathfrak{a}_m \nsubseteq \mathfrak{m}^r$ for any m. Then, for any $n \geq r$, $\mathfrak{a}_m \nsubseteq \mathfrak{m}^n$. Since altitude $R/\mathfrak{m}^n = 0$, the minimum condition for ideals holds in $R/\mathfrak{m}^n$, whence there is a natural number $t(n)$ such that $\mathfrak{a}_{t(n)} + \mathfrak{m}^n = \mathfrak{a}_m + \mathfrak{m}^n$ for any $m \geq t(n)$. We may assume that $t(n) < t(n+1)$ for any $n = r, r+1, \dots$. Then $\mathfrak{a}_{t(n)} \subseteq \mathfrak{a}_{t(n)} + \mathfrak{m}^n = \mathfrak{a}_{t(n+1)} + \mathfrak{m}^n$, and therefore for any given element x_n of $\mathfrak{a}_{t(n)}$ there is an element x_{n+1} of $\mathfrak{a}_{t(n+1)}$ such that $x_n - x_{n+1} \in \mathfrak{m}^n$. Starting with an $x_r \in \mathfrak{a}_{t(r)}$ which is not in $\mathfrak{m}^r$, we have a sequence of x_n as above. Then the x_n form a Cauchy sequence, which has a limit x^* in R. Since $x_n, x_{n+1}, \dots$ are in $\mathfrak{a}_{t(n)}$ and since x^* is the limit of the sequence, we have $x^* \in \mathfrak{a}_{t(n)}$ by the closedness of ideals. Hence $x^* \in \bigcap_n \mathfrak{a}_{t(n)} = 0$, and $x^* = 0$. On the other hand, since $x_n - x_r \in \mathfrak{m}^r$ for any n, we see that $x^* - x_r \in \mathfrak{m}^r$, whence $x_r \in \mathfrak{m}^r$, which is a contradiction.

(30.2) COROLLARY: *If a complete semi-local ring R is dominated by a semi-local ring R' which may not be Noetherian, then R is a subspace of R'.*

Proof: Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the Jacobson radicals of R and R', respectively. Then obviously $\mathfrak{m}^n \subseteq \mathfrak{m}'^n \cap R$. By (30.1), we have $\mathfrak{m}'^{m(n)} \cap R \subseteq \mathfrak{m}^n$, and the assertion is proved.

We say that a quasi-local ring $(R, \mathfrak{m})$ is a *Henselian ring* if the following is true: If a monic polynomial $f(x)$ over R is such that $f(x) \equiv g_0(x)h_0(x)$ modulo $\mathfrak{m}R[x]$ with monic polynomials g_0 and h_0 with the

properly that $g_0R[x] + h_0R[x] + \mathfrak{m}R[x] = R[x]$, then there are monic polynomials $g(x)$ and $h(x)$ such that $f(x) = g(x)h(x)$ and such that $g(x) - g_0(x), h(x) - h_0(x)$ are in $\mathfrak{m}R[x]$.

Under this terminology, we can assert that:

(30.3) THEOREM: *If $(R, \mathfrak{m})$ is a complete local ring which may not be Noetherian, then R is a Henselian ring.*

We prove this theorem in the following form, which is more general in appearance:

(30.4) *If $(R, \mathfrak{m})$ is a complete local ring which may not be Noetherian, if $f(x)$, $h_0(x)$ are polynomials in an indeterminate x over R and if $g_0(x)$ is a monic polynomial in x over R such that $f(x) - g_0(x)h_0(x) \in \mathfrak{m}R[x]$ and such that $g_0(x)R[x] + h_0(x)R[x] + \mathfrak{m}R[x] = R[x]$, then there are polynomials $g(x)$ and $h(x) (\in R[x])$ as follows: $f(x) = g(x)h(x)$, $g(x) - g_0(x) \in \mathfrak{m}R[x]$, $h(x) - h_0(x) \in \mathfrak{m}R[x]$ and $g(x)$ is a monic polynomial.*

Proof: We may assume that $\deg h_0 + \deg g_0 \leq \deg f$. Starting with g_0 and h_0, we construct sequences of polynomials $g_n(x)$ and $h_n(x)$ such that $f - g_nh_n \in \mathfrak{m}^{n+1}R[x]$, $g_n - g_{n-1} \in \mathfrak{m}^nR[x]$, $h_n - h_{n-1} \in \mathfrak{m}^nR[x]$, $\deg h_n + \deg g_n \leq \deg f$, and such that g_n is a monic polynomial (for every n): Namely, when g_n and h_n are already defined, then we define g_{n+1} and h_{n+1} as follows: Since $g_0 - g_n$ and $h_0 - h_n$ are in $\mathfrak{m}R[x]$, we see that g_n, h_n, and $\mathfrak{m}$ generate $R[x]$, whence there are polynomials $a_i(x)$, $b_i(x)$ and $m_i(x)$ such that $x^i = g_na_i + h_nb_i + m_i$ with $m_i \in \mathfrak{m}R[x]$. Since g_n is monic, we may assume that $\deg b_i < \deg g_n = \deg g_0$. By the existence of the term m_i, we may assume that the coefficients of a_i and b_i are units or zero. Then we see that $\deg a_i \leq \deg f - \deg g_n$ if $i \leq \deg f$. Now we write $f - g_nh_n = \sum c_ix^i (c_i \in \mathfrak{m}^{n+1})$. This last sum is taken up to the term whose degree is equal to $d = \deg f$. Therefore, $f - g_nh_n = g_n(\sum c_ia_i) + h_n(\sum c_ib_i) + \sum c_im_i$, and $\deg (\sum c_ia_i) \leq \deg f - \deg g_n$, $\deg (\sum c_ib_i) < \deg g_n$, $\sum c_im_i \in \mathfrak{m}^{n+2}R[x]$. Set $g_{n+1} = g_n + \sum c_ib_i$, $h_{n+1} = h_n + \sum c_ia_i$. Then $f - g_{n+1}h_{n+1} = \sum c_im_i - (\sum c_ib_i)(\sum c_ia_i) \in \mathfrak{m}^{n+2}R[x]$, and as is easily verified, g_{n+1} and h_{n+1} satisfy the requirements. Thus the existence of the sequences is proved. Since R is complete, we can consider the limits of $\{g_n(x)\}$ and $\{h_n(x)\}$; let them be $g(x)$ and $h(x)$. Then we see that $f - gh \in \mathfrak{m}^nR[x]$ for any n, and $f = gh$, and we prove easily that these g and h are the required elements.

Since some general properties of Henselian rings will be observed

later in Chapter VII, including the fact that the Hensel lemma of the form in (30.1) is a general property of Henselian rings, we shall not derive any of them at present, except for the following:

(30.5) *If R is a Henselian integral domain and if R' is an integral extension of R, then R' is quasi-local.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of R. Assume that R' has maximal ideals $\mathfrak{m}'$, $\mathfrak{m}''(\mathfrak{m}' \neq \mathfrak{m}'')$, and let a be an element of $\mathfrak{m}'$ which is not in $\mathfrak{m}''$. Set $R'' = R[a]$ and let

$$f(x) = x^n + c_1x^{n-1} + \cdots + c_n (c_i \in R)$$

be an irreducible monic polynomial over R which has a as a root. Since $a \in \mathfrak{m}'$, we have $c_n \in \mathfrak{m}$. Since $a \notin \mathfrak{m}''$, $a^n \notin \mathfrak{m}R[a]$, and there is a c_i which is not in $\mathfrak{m}$. Let j be such that $c_j \notin \mathfrak{m}$, $c_{j+s} \in \mathfrak{m}$ (for $s > 0$). Then $1 \leq j \leq n-1$, and $f(x) \equiv (x^j + c_1x^{j-1} + \cdots + c_j)x^{n-j}$ modulo $\mathfrak{m}R[x]$. Since R is Henselian, $f(x)$ must be reducible over R, which is a contradiction, and the assertion is proved.

(30.6) THEOREM: *Let R be a complete semi-local ring with Jacobson radical $\mathfrak{m}$. Let M be an R-module. If $M/\mathfrak{m}M$ is a finite R-module and if the $\mathfrak{m}$-adic topology of M is T_0, then M is a finite module*: *Let $u_1, \ldots, u_s$ be elements of M such that $M/\mathfrak{m}M$ is generated by their residue classes, then $M = \sum Ru_i$.*

Proof: Set $N = \sum_1^s Ru_i$. Let a be an arbitrary element of M. We want to show that there is a sequence of elements $a_1, \ldots, a_n, \ldots$ of N such that $a_n = \sum m_{ni}u_i$ with $m_{ni} \in \mathfrak{m}^{n-1}$ and such that

$$a - \textstyle\sum_1^n a_j \in \mathfrak{m}^nM.$$

We use induction on n. The case where $n = 1$ is immediate from the assumption. Assume that $a_1, \ldots, a_n$ are already defined. Then $a - \sum_1^n a_j = \sum m_ib_i$ with $m_i \in \mathfrak{m}^n$, $b_i \in M$. Let c_i be elements of N such that $b_i - c_i \in \mathfrak{m}M$, and set $a_{n+1} = \sum m_ic_i$. Then a_{n+1} is the required element, and the sequence is well defined. Set $m_i^* = \sum_n m_{ni}$ and $a^* = \sum m_i^*u_i$. Then $a - a^* \in \mathfrak{m}^nM$ for any n, whence $a = a^*$, which implies that $M \subseteq N$, and $M = N$.

EXERCISES: *1.* Assume that a local ring R, with principal maximal ideal pR, is dominated by a semi-local ring R' which may not be Noetherian. Prove that R is a subspace of R'.

2. Generalize (30.1) to the case of finite module over a complete semi-local ring.

31. The structure theorem of complete local rings

Let R be a semi-local ring with Jacobson radical $\mathfrak{m}$ and let $x_1, \ldots, \ldots, x_n$ be elements of $\mathfrak{m}$. Let I be a subring of R. Then power series in the x_i with coefficients in I has meaning in the completion R^* of R and the set of all such power series becomes a subring of R^*. This subring is denoted by $I[[x_1, \ldots, x_n]]$. Furthermore, if $X_1, \ldots, X_n$ are indeterminates, then there is a homomorphism ϕ from $I[[X_1, \ldots, X_n]]$ onto $I[[x_1, \ldots, x_n]]$ over I such that $\phi(X_i) = x_i$. If the homomorphism ϕ is an isomorphism, we say that $x_1, \ldots, x_n$ are *analytically independent* over I. We note that if I is Noetherian then $I[[x_1, \ldots, \ldots, x_n]]$ is Noetherian. If I is a semi-local ring or a local ring, then so is $I[[x_1, \ldots, x_n]]$. (The proof is immediate from (15.3) and (15.4).)

The main result in this section is the following:

(31.1) THEOREM: *If $(R, \mathfrak{m})$ is a complete local ring which may not be Noetherian, then R contains a ring I which satisfies the following condition: Let p be the characteristic of $R/\mathfrak{m}$. Then $\mathfrak{m} \cap I$ is generated by p (i.e., p-fold of the identity), I is a complete local ring and $R/\mathfrak{m}$ is naturally equal to $I/(\mathfrak{m} \cap I)$. Consequently, if $\{a_\lambda\}$ form a basis for $\mathfrak{m}$, then every element of R is expressed as a power series in the a_λ with coefficients in I.* (STRUCTURE THEOREM OF COMPLETE LOCAL RINGS)

Such a ring I, as above, is called a *coefficient ring* of R; if I is a field, then I is called a *coefficient field* of R. It is obvious that I is a field if and only if R contains some field.

Proof: We begin with the case where $p = 0$. Let I be a maximal subfield of R; the existence follows from Zorn's lemma. We want to show that this I is a coefficient field. Since $\mathfrak{m} \cap I = 0$, I is regarded as a subfield of $R/\mathfrak{m}$. If $x' \in R/\mathfrak{m}$ is transcendental over I, then with an x such that $x' = x$ modulo $\mathfrak{m}$, $I(x)$ is a subfield of R, which contradicts the maximality of I. Hence $R/\mathfrak{m}$ is algebraic over I. Assume that $R/\mathfrak{m}$ contains an element a' which is not in I and let $f(x)$ be the irreducible monic polynomial over I which has a' as a root. The same $f(x)$ is regarded as a polynomial over R. Since $p = 0$, a' is a simple root of $f(x)$ modulo $\mathfrak{m}R[x]$, whence $f(x) = (x - a)g(x)$ with an $a \in R$ such that $a' = a$ modulo $\mathfrak{m}$, by virtue of (30.3) or (30.4). This implies that $I(a)$ is a subfield of R, which contradicts the maximality of I, and $R/\mathfrak{m} = I$. Thus this case is proved. We consider the case $p \neq 0$. Before proceeding with the proof, we give some preliminaries.

When K is a field of characteristic $p \neq 0$, a subset B of K is called a

p base of K if B satisfies the following two conditions: (1)

$$K = K^p(B),$$

and (2) if $b_1, \ldots, b_r$ are mutually distinct elements of B, then $[K^p(b_1, \ldots, b_r):K^p] = p^r$.

Under this terminology, we have the following lemma:

(31.2) *An arbitrary field K of characteristic $p \neq 0$ has a p-base, say B. For any natural number n and for any mutually distinct elements $b_1, \ldots, b_r$ of B, we have that $K = K^{p^n}(B)$ and that*

$$[K^{p^n}(b_1, \ldots, b_r):K^{p^n}] = p^{nr}.$$

Proof: The existence of B is easy by virtue of Zorn's lemma, considering subsets of K satisfying the second condition in the definition. We prove the other assertions by induction on n. Since the map ϕ such that $\phi(a) = a^p$ is an isomorphism from K onto K^p, we have $K^p = K^{p^n}(B^p)$ by induction and therefore $K = K^{p^n}(B)$. $p^{nr} \geq [K^{p^n}(b_1, \ldots, \ldots, b_r):K^{p^n}] = [K^{p^n}(b_1, \ldots, b_r):K^{p^n}(b_1^p, \ldots, b_r^p)]\cdot[K^{p^n}(b_1^p, \ldots, \ldots, b_r^p):K^{p^n}] \geq p^r\cdot[K^{p^{n-1}}(b_1, \ldots, b_r):K^{p^{n-1}}] = p^r\cdot p^{(n-1)r}$. Thus we prove (31.2).

We note that (31.2) implies that every element of K is expressed as a polynomial in elements of B with coefficients in K^{p^n} in such a way that the degree of the expression is less than p^n for each member of B and that such an expression is uniquely determined by the element of K.

Next we prove another lemma:

(31.3) *Let p be a prime number and assume that an ideal $\mathfrak{m}$ of a ring R contains p (i.e., the p-fold of the identity). If $a - b \in \mathfrak{m}$, then $a^{p^n} - b^{p^n} \in \mathfrak{m}^{n+1}$. Consequently, if, furthermore, $\mathfrak{m}^t = 0$ and if $\mathfrak{m}$ is a maximal ideal, then the map ϕ such that $\phi(a) = a^{p^s}$ with $s + 1 \geq t$ induces a one-one map from the field $R/\mathfrak{m}$ into R.*

Proof: Set $c = b - a$, $q = p^n$. Then $b^q = a^q + qa^{q-1}c + \cdots + \binom{q}{r}a^{q-r}c^r + \cdots + c^q$. If $r = p^t r'$, $(p, r') = 1$, then a simple calculation shows that $\binom{q}{r}$ is a multiple of p^{n-t}, whence $\binom{q}{r} \in \mathfrak{m}^{n-t}$. Since $p^t > t$, $c^r \in \mathfrak{m}^{t+1}$, and therefore the assertion is proved.

Now we proceed with the proof of (31.1). Let B^* be a p-base of $K = R/\mathfrak{m}$ and fix a set B of representatives of B^* in R (i.e., we take only one $b \in R$ for each $b^* \in B^*$ such that $b^* = b$ modulo $\mathfrak{m}$, and B

is the set of such b). For each natural number n let ϕ_n be the map from $R/\mathfrak{m}^n$ into itself given by $\phi_n(a) \equiv a^{p^{2n}}$. Then ϕ_n induces a one one map from $R/\mathfrak{m}$ into $R/\mathfrak{m}^n$ by (31.3); this one one map is denoted by σ_n. We denote by A_n the image of $R/\mathfrak{m}$ by σ_n. Let S_n be the set of polynomials in elements of B taken modulo $\mathfrak{m}^n$ with coefficients in A_n such that the degree of the polynomial in each element of B is less than p^{2n}. Since ϕ_n induces on $K = R/\mathfrak{m}$ an isomorphism from K onto $K^{p^{2n}}$, there is a natural one-one map between elements of $K^{p^{2n}}$ and A_n (such that $(a \text{ modulo } \mathfrak{m})^{p^{2n}}$ corresponds to $(a \text{ modulo } \mathfrak{m}^n)^{p^{2n}}$). Therefore, we have a one-one map from K onto S_n, and S_n becomes a complete set of representatives of $R/\mathfrak{m}$ in $R/\mathfrak{m}^n$. Set $J_n = S_n + pS_n + \cdots + p^{n-1}S_n$ (this notation means that J_n is the set of elements of the form $\sum_{i=0}^{n-1} a_i p^i$ with $a_i \in S_n$. We want to show that J_n is a ring. If it is known that the sum of two elements of S_n is in J_n, then we see that the sum of two elements of J_n is in J_n, and furthermore, since the product of two elements of S_n which are monomials in the elements of B are in S_n, we see easily that the product of two elements of S_n is in J_n, whence the product of two elements of J_n is in J_n. Thus, in order to prove that J_n is a ring, we have only to show that the sum of two elements $\sum a_M M$ and $\sum b_M M$ ($a_M, b_M \in A_n$; $M = b_1^{e_1} \cdots b_r^{e_r}$ with $b_i \in B$, $0 \leq e_i < p^{2n}$) is in J_n. We prove it in the form that $p^i(\sum a_M M + \sum b_M M)$ is in $p^i J_n$ by induction on i starting with $i = n$ (until $i = 0$). This last assertion is obvious for $i = n$. Assume that $0 \leq i < n$. Set $q = p^{2n}$. For each M, a_M and b_M are in A_n and therefore they are qth powers of elements c_M and d_M of $R/\mathfrak{m}^n$. Since a_M and b_M are uniquely determined by the residue classes of c_M and d_M modulo $\mathfrak{m}$, we may assume that c_M and d_M are in S_n. Now, $a_M + b_M = (c_M + d_M)^q - \sum_1^{q-1} \binom{q}{r} c_M^{q-r} d_M^r$. Since $\binom{q}{r}$ are multiples of p, we see that $p^i(\sum_{r,M} \binom{q}{r} c_M^{q-r} d_M^r) M$ is in $p^{i+1} J_n$ by induction because c_M, d_M are in S_n. Therefore

$$\sum p^i (a_M + b_M) M = \sum p^i (c_M + d_M)^q M + p^i (\sum_{r,M} \binom{q}{r} c_M^{q-r} d_M^r) M$$

is in $p^i J_n$. Thus, the above assertion is proved, and we see that J_n is a ring. Obviously $J_n \cap \mathfrak{m}/\mathfrak{m}^n = pJ_n$, whence pJ_n is a maximal ideal of J_n. The one-one correspondence between S_n and $R/\mathfrak{m}$ now induces the natural isomorphism between J_n/pJ_n and $R/\mathfrak{m}$. We want to show

next that the natural homomorphism π_n from $R/\mathfrak{m}^n$ onto $R/\mathfrak{m}^{n-1}$ induces a natural homomorphism from J_n onto J_{n-1}. It is obvious that $\pi_n(M)$ becomes an element of S_{n-1}, hence $\pi_n(S_n) \subseteq J_{n-1}$, which implies that π_n is a homomorphism from J_n into J_{n-1}. On the other hand, it is obvious by the construction that each element of S_{n-1} is in $\pi_n(S_n)$, which implies that $\pi_n(J_n)$ contains J_{n-1}. Therefore π_n induces a natural homomorphism from J_n onto J_{n-1}. Now, let $\{a_n\}$ be a sequence of elements such that $a_n \in J_n$ and such that $\pi_n(a_n) = a_{n-1}$. For each such sequence $\{a_n\}$, let $\{b_n\}$ be a sequence of elements of R such that b_n modulo $\mathfrak{m}^n = a_n$. Then it is obvious that $\{b_n\}$ is a regular sequence, hence there is $\lim b_n$. This last limit depends only on the sequence $\{a_n\}$ as is easily seen. Let I be the set of such limits. Since each J_n is a ring, I is a ring. Furthermore, each regular sequence in I with pI-adic topology comes from such a sequence $\{a_n\}$ as above, whence I is complete in its pI-adic topology. Therefore we see easily as in the proof of (15.1) that I is a quasi-local ring with maximal ideal pI. Hence, in order to prove (31.1), it is sufficient to prove that I is Noetherian, which follows from the following two lemmas:

(31.4) *If a quasi-local ring* $(R, \mathfrak{m})$ *is dominated by a local ring* $(R', \mathfrak{m}')$ *which may not be Noetherian, then* R *is a local ring which may not be Noetherian.*

Proof: This is obvious because $\mathfrak{m} \subseteq \mathfrak{m}'$.

(31.5) *If a local ring* R *which may not be Noetherian has principal maximal ideal* pR, *then* R *is Noetherian.*

Proof: Let $\mathfrak{a}$ be an arbitrary ideal of R such that $R \neq \mathfrak{a} \neq 0$. Then there is a natural number n such that $\mathfrak{a} \subseteq p^nR$, $\mathfrak{a} \nsubseteq p^{n+1}R$. Then $\mathfrak{a}:p^nR$ is not contained in pR, whence $\mathfrak{a}:p^nR = R$, which implies that $\mathfrak{a} \supseteq p^nR$ and $\mathfrak{a} = p^nR$.

(31.6) COROLLARY: *If* R *is a complete local integral domain, then* R *contains a complete regular ring* S *such that* R *is a finite* S*-module and such that* $S = I[[x_1, \ldots, x_r]]$ *with a coefficient ring* I *of* R *and analytically independent elements* $x_1, \ldots, x_r$ *over* I.

Proof: When I is a field, let $x_1, \ldots, x_r$ be a system of parameters of R; when I is not a field and if the maximal ideal of I is pI, let $x_1, \ldots, x_r$ be such that $p, x_1, \ldots, x_r$ is a system of parameters of R. Set $S = I[[x_1, \ldots, x_r]]$. (30.6) implies that R is a finite S-module, whence altitude R = altitude S. Let $X_1, \ldots, X_r$ be indeterminates. Then since $X_1, \ldots, X_r$ or $p, X_1, \ldots, X_r$ form a regular system of parameters of $I[[X_1, \ldots, X_r]]$, we have altitude $I[[X_1, \ldots, X_r]] =$

altitude R. Therefore the natural mapping from $I/\|X\|$ onto $I/\|x\|$ must be an isomorphism, and the assertion is proved.

As another corollary to (31.1), we have the following result by virtue of (15.3):

(31.7) COROLLARY: *If R is a complete local ring which may not be Noetherian and if the maximal ideal $\mathfrak{m}$ of R has a finite basis, then R is Noetherian.*

As an application of (31.7), we prove the following:

(31.8) THEOREM: *A semi-local ring R which may not be Noetherian is really Noetherian if and only if*: (1) *every finitely generated ideal of R is a closed subset of R, and* (2) *the maximal ideals of R have finite bases.*

Proof: The only if part is obvious by (16.7). Assume that R is not Noetherian and that the maximal ideals have finite bases. Then there is an ideal which has no finite basis, whence there exists an ascending sequence $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \cdots$ of ideals $\mathfrak{a}_n$ of R such that each of the $\mathfrak{a}_n$ has a finite basis. Let R^* be the completion of R. Then R^* is Noetherian by (31.7) and (17.7). Therefore there is an n such that $\mathfrak{a}_m R^* = \mathfrak{a}_n R^*$ for any $m \geq n$, which implies that $\mathfrak{a}_n$ is not a closed subset of R, because $\mathfrak{a}_n R^* \cap R$, which contains $\mathfrak{a}_m$, is contained in the closure of $\mathfrak{a}_n$. Thus (31.8) is proved.

Next we give some remarks on the choice of coefficient rings. When $(R, \mathfrak{m})$ is a complete local ring which may not be Noetherian, such that $R/\mathfrak{m}$ is of characteristic $p \neq 0$, let K be the maximal perfect subfield of $R/\mathfrak{m}$. For each element a' of K, let b_n be a representative of $a'^{p^{-n}}$ in R and set $c_n = b_n^{p^n}$. Then since $b_{n+1}^p - b_n \in \mathfrak{m}$, we see by (31.3) that the c_n form a Cauchy sequence, whose limit a is uniquely determined by a' independently of the choice of the b_n. This a is called the *multiplicative representative* of a'. Note that a is a representative of a' and that if b is the multiplicative representative of an element b' of K, then ab is the multiplicative representative of $a'b'$, as is obviously seen by our definition; these are the reasons for calling a the multiplicative representatives of a'. Now we have:

(31.9) THEOREM: *Let $(R, \mathfrak{m})$ be a complete local ring which may not be Noetherian.* (1) *If $R/\mathfrak{m}$ is of characteristic zero, then a subring I is a coefficient ring of R if and only if I is a maximal subfield of R.* (2) *Assume that $R/\mathfrak{m}$ is of characteristic $p \neq 0$. Let B^* be a p-base of $R/\mathfrak{m}$, let B be a set of representatives of B^* as defined in the proof of* (31.1), *and let K be the maximal perfect subfield of $R/\mathfrak{m}$. Then there is a coeffi-*

cient ring I of R which contains B and every coefficient ring of R contains the multiplicative representatives of all elements of K.

Proof: (1) is obvious by the proof of (31.1). The existence of I containing the given B was really proved in the proof of (31.1). We are to prove the last half of (2). Using the notation employed just before (31.9), the b_n can be chosen from a given coefficient ring I' of R, whence the multiplicative representative a of $a' \in K$ is in I'.

(31.10): COROLLARY: *Let $(R, \mathfrak{m})$ be a complete local ring which may not be Noetherian such that $\mathfrak{m} \neq 0$. (1) If $R/\mathfrak{m}$ is of characteristic zero, then R has only one coefficient field when and only when $R/\mathfrak{m}$ is algebraic over the prime field. (2) If $R/\mathfrak{m}$ is of characteristic $p \neq 0$, then R has only one coefficient ring when and only when $R/\mathfrak{m}$ is perfect.*

Lastly, we prove a structure theorem of ramified regular local rings.

We note, first, that the classical theorem of Eisenstein on the irreducibility of polynomials can be stated as follows:

(31.11) *Let $\mathfrak{p}$ be a prime ideal in a ring R and let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ $(a_i \in R)$ be a monic polynomial in an indeterminate x over R. Assume that all the a_i are in $\mathfrak{p}$ and that $a_n \notin \mathfrak{p}^2$, then $f(x)$ is irreducible over R. Hence, if furthermore R is a normal ring, then $f(x)$ is irreducible over the field of quotients of R.*

Proof: If $f(x)$ is reducible, say $f(x) = g(x)h(x)$ with monic polynomials $g(x)$ and $h(x)$, then, since $f(x) \equiv x^n$ modulo $\mathfrak{p}$, we have $g(x) \equiv x^r$, $h(x) \equiv x^{n-r}$ modulo $\mathfrak{p}$ and $a_n \in \mathfrak{p}^2$ which is a contradiction, which proves the first assertion, from which the last assertion follows.

When $(R, \mathfrak{m})$ is a local ring, a polynomial $f(x)$ as above with $\mathfrak{p} = \mathfrak{m}$ is called an *Eisenstein polynomial* over R and $R[x]/f(x)R[x]$ is called an *Eisenstein extension* of R. Now we can state:

(31.12) THEOREM: *Every complete regular local ring $(R, \mathfrak{m})$ is an Eisenstein extension of a complete unramified regular local ring $(R_0, \mathfrak{m}_0)$, which is necessarily the power series ring in a finite number of analytically independent elements over a coefficient ring of R_0. Every Eisenstein extension of a regular local ring is again a regular local ring.*

Proof: As for the first assertion, we have only to prove the case where R does not contain any field. Let I be a coefficient ring of R and let p be the characteristic of $R/\mathfrak{m}$. Let $x_1, \ldots, x_n$ be a regular system of parameters of R. If R is unramified, i.e., if $p \notin \mathfrak{m}^2$, then we may assume that $x_1 = p$, whence $R = I[[x_2, \ldots, x_n]]$, which proves the last statement of the first assertion. Returning to the general

case, we may assume that $p, x_2, \ldots, x_n$ is a system of parameters of R. Set $R_0 = k[[x_2, \ldots, x_n]]$. Then R is a finite R_0 module by (30.6), whence $R = R_0[x_1]$, again by (30.6), whence altitude $R_0 = n$ and R_0 is regular. Let $f(X) = X^r + c_1X^{r-1} + \cdots + c_r$ be the irreducible monic polynomial over R_0 which has x_1 as a root. Since $x_1 \in \mathfrak{m}$, we have $c_r \in \mathfrak{m}_0$. Since R_0 is Henselian by (30.3) and since $f(X)$ is irreducible, we see that all the c_i are in $\mathfrak{m}_0$. On the other hand, since $p \in \mathfrak{m}$, $p = \sum d_ix_i$ with $d_i \in R = R_0[x_1]$, whence, writing d_i as polynomials in x_1 with coefficients in R_0, we see that there is a polynomial $g(X) = \sum a_iX^i$ over R_0 such that $g(x_1) = 0$ and such that $a_0 = p + q$ with $q \in \sum_2^n x_iR_0$. Since $g(x_1) = 0$, $g(X)$ must be a multiple of $f(X)$, whence $a_0 \notin \mathfrak{m}_0^2$ implies that $c_r \notin \mathfrak{m}_0^2$ and $f(X)$ is an Eisenstein polynomial over R_0, which completes the proof of the first assertion. Assume now that $(R, \mathfrak{m})$ is a regular local ring and that $f(X)$ is an Eisenstein polynomial. Let c_0 be the constant term of $f(X)$ and let $x_1, \ldots, x_n$ be a regular system of parameters of R such that $c_0 = x_1$. Let u be the residue class of X in $R[X]/f(X)R[X]$. Then it is obvious that this last ring has only one maximal ideal which is generated by u, $x_2, \ldots, x_n$, by virtue of (10.7), whence $R[X]/f(X)R[X]$ is a regular local ring, which proves the last assertion. Thus the proof is complete.

EXERCISES: *1*. Give a direct proof of (31.7) using the fact that the form ring of R with respect to the maximal ideal is a Noetherian ring.

2. Let $(R, \mathfrak{m})$ and $(R', \mathfrak{m}')$ be complete local rings which may not be Noetherian, such that R' is integral over R $(R \leq R')$. Prove that if $R'/\mathfrak{m}'$ is separable over $R/\mathfrak{m}$, then, for any coefficient ring I of R, there is a coefficient ring I' of R' which contains I. Prove furthermore that such an I' is uniquely determined by I.

3. Let $(R, \mathfrak{m})$ be a complete local ring which may not be Noetherian. Assume that R contains a field of characteristic $p \neq 0$. Assume that $(R', \mathfrak{m}')$ is a local ring which may not be Noetherian such that $R'^p \subseteq R \subseteq R'$. Prove that there are coefficient fields I and I' of R and R', respectively, such that $I \subseteq I'$.

32. *Finiteness of derived normal rings*

We first prove the following:

(32.1) THEOREM: *If R is a complete local integral domain, then an arbitrary almost finite integral extension of R is a finite module.*

As for the proof, since R is a finite integral extension of a complete regular local ring by (31.6), we have only to prove the following:

Let R be a complete regular local ring and let K be the field of quotients

of R. Let L be a finite algebraic extension of K and let R' be the integral closure of R in L. Then R' is a finite R module.

Proof: Let p be the characteristic of K. If $p \neq 0$, then L is separable over K, and R' is finite, by (10.16). Therefore we assume that $p \neq 0$, whence R is the power series ring in analytically independent elements $x_1, \ldots, x_r$ over a field I. There is a finite purely inseparable extension L' of K such that $L(L')$ is separable over L'. If we know that the integral closure R'' of R in L' is finite over R, then we see that the integral closure of R in $L(L')$ is finite because $L(L')$ is separable over L', and therefore R' is finite over R, by (3.1). Thus we may assume that $L = L'$. Let $q = [L:K]$ (q is a power of p) and set $I^* = I^{1/q}$, $y_i = x_i^{1/q}$, $R^* = I^*[[y_1, \ldots, y_r]]$. If $a \in R'$, then $a^q \in R$, whence $R' \subseteq R^*$, which implies that every element a of R' is uniquely expressed as a power series in the y_i with coefficients in I^*, and in that sense we define the leading form of an element of R'. We want to show first that when $a_1, \ldots, a_s$ are elements of R' such that the leading forms $f_1, \ldots, f_s$ of these elements are linearly independent over R, then $a_1, \ldots, a_s$ are linearly independent over R. Indeed, if $\sum a_i b_i$ ($b_i \in R$) is a non-trivial linear combination, then the leading form of $\sum a_i b_i$ is a non-trivial linear combination of the f_i which cannot be zero because of their linear independency. Thus $a_1, \ldots, a_s$ are linearly independent. Since L is finite over K, we see that there are elements $a_1, \ldots, a_s$ of R' with leading forms $f_1, \ldots, f_s$ such that if a is an element of R', then the leading form f of a is linearly dependent on $f_1, \ldots, f_s$. Let $c_1, \ldots, c_t$ be the set of coefficients of $f_1, \ldots, f_s$. Then the coefficients of f are in $I(c_1, \ldots, c_t)$. Therefore, if $d_0 = 1$, $d_1, \ldots, d_u$ is a linear base of $I(c_1, \ldots, c_t)$ over I and if $m_0 = 1$, $m_1, \ldots, m_v$ is the set of monomials in the y_i of degree less than rq, then f is in the module $\sum R m_i d_j$, whence the module M generated by leading forms of elements of R' is a finite R-module; let $g_1, \ldots, g_w$ be a base of M such that each g_j is the leading form of an element b_j of R' and let $R'' = R[b_1, \ldots, b_w]$. R'' is a finite R-module, whence it is complete. Therefore, R'' is a subspace of both R^* and R' by (30.2). Let d be an element of R'. We want to show by induction on n that there is a sequence $\{d_n\}$ of elements of R'' such that $d - d_n$ has leading degree not less than n. We may start with $d_0 = 0$. If $d_0, \ldots, d_n$ are already defined, let f be the leading form of $d - d_n$. We can write $f = \sum h_j g_j$ with $h_j \in R$, and we may assume that h_j are homogeneous forms, whence $d^* = \sum h_j b_j$ has the same leading form f, and there-

fore $d_{n+1} - d_n \in d^*$ is the required element. Thus, the existence of the sequence is proved. Since R'' is a subspace of R^* the sequence is a Cauchy sequence in R''. Since R'' is complete, the sequence has a limit d'' in R''. $d - d''$ because R'' is a subspace of R', which implies that $R' \subseteq R''$, and R' is a finite R-module.

We say that a semi-local ring R is *analytically unramified* if the completion R^* of R has no nilpotent element except zero; an ideal $\mathfrak{a}$ of R is said to be *analytically unramified* if $R/\mathfrak{a}$ is analytically unramified (or, equivalently, if $\mathfrak{a}R^*$ is semi-prime). Under this terminology, we can state the following corollary to (32.1):

(32.2) THEOREM: *If a semi-local integral domain R is analytically unramified, then the derived normal ring R' of R is a finite R-module.*

Proof: Assuming the contrary, let $R = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_n \subset \cdots$ be an infinite ascending chain of subrings of R' such that each R_n is a finite R-module. Let R^* be the completion of R. Then the completion R_n^* of R_n is generated by R^* and R_n (and is identified with $R_n \otimes R^*$) by (17.8), which implies that R_n^* is a finite module over R^* and is contained in the integral closure Q^* of R^* in its total quotient ring. Let K be the field of quotients of R. Then $R_n^* \cap K = R_n$ by (18.4), which implies that Q^* is not finite over R^*. On the other hand, let $\mathfrak{n}_i^*$ be all of the prime divisors of zero of R^*. Then Q^* is the direct sum of derived normal rings of $R^*/\mathfrak{n}_i^*$, whence Q^* must be finite over R^* by (32.1). Thus R' must be finite over R.

33. Derived normal rings of Noetherian integral domains

(33.1) *Let R be a Noetherian integral domain with field of quotients K and let R' be a ring such that $R \subseteq R' \subseteq K$. If R is integrally closed in R' and if, for any given prime ideal $\mathfrak{p}$ of R, there is a prime ideal $\mathfrak{p}'$ of R' such that $\mathfrak{p}' \cap R = \mathfrak{p}$, then it holds that $R = R'$.*

Proof: Assume the contrary and let b' be an element of R' which is not in R. Let $\mathfrak{a}$ be the set of elements a of R such that $ab' \in R$. Let $\mathfrak{p}$ be a prime divisor of $\mathfrak{a}$ and set $\mathfrak{c} = \mathfrak{a}:\mathfrak{p}$. Then $\mathfrak{a} \neq \mathfrak{c}$, whence there is an element c of $\mathfrak{c}$ such that $cb \notin R$. Let $\mathfrak{p}'$ be a prime ideal of R' such that $\mathfrak{p}' \cap R = \mathfrak{p}$. $(cb')\mathfrak{p} \subseteq R$ and furthermore $(cb')\mathfrak{p} \subseteq \mathfrak{p}'$, whence $(cb')\mathfrak{p} \subseteq \mathfrak{p}' \cap R = \mathfrak{p}$, which implies that cb' is integral over R, by (10.4). Since R is integrally closed in R', we have $cb' \in R$, which is a contradiction, and we complete the proof.

(33.2) THEOREM: *Let R be a Noetherian integral domain with field of quotients K, let L be a finite algebraic extension of K and let R' be a ring such that $R \subseteq R' \subseteq L$. If* altitude $R = 1$, *then for any ideal $\mathfrak{a}'$ of R' such that $\mathfrak{a}' \neq 0$, $R'/\mathfrak{a}'$ is a module of finite length over $R/(\mathfrak{a}' \cap R)$. In particular, R' is a Noetherian ring of altitude at most one.* (THEOREM OF KRULL-AKIZUKI)

Proof: Taking a finite integral extension of R we may assume that $L = K$. Set $\mathfrak{a} = \mathfrak{a}' \cap R$ and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be all of the prime divisors of $\mathfrak{a}$. Since $\mathfrak{a}' \neq 0$, we have $\mathfrak{a} \neq 0$, and therefore the $\mathfrak{p}_i$ are maximal. Let S be the intersection of complements of the $\mathfrak{p}_i$ in R. Then every element of S is a unit module $\mathfrak{a}$, whence $R'/\mathfrak{a}' = R'_S/\mathfrak{a}'R'_S$ and $R/\mathfrak{a} = R_S/\mathfrak{a}R_S$. Therefore we may assume that R is a semi-local ring, that $\mathfrak{a}$ is contained in the Jacobson radical $\mathfrak{m}$ of R and that R is dominated by R'. Let R'' be the integral closure of R in R'. We first prove the assertion for R'' instead of R'. Let x be an element of $\mathfrak{a}$ which is different from zero and let $y_1, \ldots, y_t$ be arbitrary elements of R''. Then R and $R[y_1, \ldots, y_t]$ are Macaulay rings, and therefore $\text{length}_R\, R/xR = \mu(xR)$, $\text{length}_R\, R[y]/xR[y] = \mu_R(xR[y])$. By (23.4), we have $\mu(xR) = \mu_R(xR[y])$, whence we have

$$\text{length } R/xR = \text{length}_R\, R[y]/xR[y].$$

Since the y_i are arbitrary, we see that $\text{length}_R\, R''/xR'' \leq \text{length } R/xR$, hence the assertion is proved for R'' instead of R'. Therefore, we may replace R with R''. Thus, we assume that $R = R''$. Then the assumptions in (33.1) are satisfied by R and R', whence $R = R'$, and the assertion is proved in the general case.

We note that the derived normal ring R' of a local integral domain of altitude 1 is not necessarily a finite module. See Example 3 in the Appendix; cf. Exercise 1 below.

An integral domain R is called a *Krull ring* if the following two conditions are satisfied:

(1) If $\mathfrak{p}$ is a prime ideal of height 1 in R, then $R_\mathfrak{p}$ is a Noetherian valuation ring.

(2) An arbitrary principal ideal aR $(a \neq 0)$ of R is the intersection of a finite number of primary ideals of height 1.

(33.3) *The condition* (2) *above is equivalent to the following two conditions*:

(2.a) *Every principal ideal of R has only a finite number of prime divisors $\mathfrak{p}$ such that* height $\mathfrak{p} = 1$.

(2.b) *Letting* $\mathfrak{p}$ *run over all prime ideals of* height 1 *in* R, *we have* $R = \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$.

Proof: Assume that (2) holds. (2.a) holds by (7.5). Set $D = \bigcap R_{\mathfrak{p}}$ and let c/d ($c, d \in R$) be an arbitrary element of D. Then $cR_{\mathfrak{p}} \subseteq dR_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ of height 1, whence $c \in \bigcap(dR_{\mathfrak{p}} \cap R)$, and this last intersection coincides with dR by condition (2) by virtue of (6.6), whence $c/d \in R$, and we see that $R = D$, which proves the validity of (2.b). Conversely, assume that (2.a) and (2.b) hold and let a be an element of R which is not zero. Set $\mathfrak{a} = \bigcap(aR_{\mathfrak{p}'} \cap R)$ where $\mathfrak{p}'$ runs over all prime divisors of aR such that height $\mathfrak{p}' = 1$. We have only to prove that $\mathfrak{a} = aR$, hence that $\mathfrak{a} \subseteq aR$. Let b be an arbitrary element of $\mathfrak{a}$. If $\mathfrak{p}$ is a prime ideal of height 1 and if $\mathfrak{p} \neq \mathfrak{p}'$ for any $\mathfrak{p}'$, then $a \notin \mathfrak{p}$, whence $aR_{\mathfrak{p}} = R_{\mathfrak{p}}$. Therefore, we see that $b \in aR_{\mathfrak{p}}$ for any $\mathfrak{p}$ (height $\mathfrak{p} = 1$), whence $b/a \in \bigcap R_{\mathfrak{p}} = R$, and $b \in aR$. Thus, the proof is complete.

We note that:

(33.4) *A Krull ring is a normal ring. A Noetherian normal ring is a Krull ring.*

Proof: The first assertion follows from condition (1) and (2.b), while the last assertion follows from (12.9).

(33.5) *Let* R *be an integral domain with field of quotients* K *and assume that a set* F *of Noetherian valuation rings* V *of* K *satisfies the following two conditions*:

(1) R *is the intersection of all* $V \in F$.

(2) *If* a ($\in R$) *is not zero, then there are only a finite number of* V *in* F *such that* a *is non-unit in* V.

Let S *be a multiplicatively closed subset of* R *such that* $0 \notin S$ *and let* F' *be the subset of* F *consisting of those* V *in which every element of* S *is a unit. Then we have the equality* $R_S = \bigcap_{V \in F'} V$.

Proof: Let D be the last intersection. Since $R_S \subseteq D$ obviously, we have only to prove that $D \subseteq R_S$. Let c/d ($c, d \in R$) be an arbitrary element of D. Let $V_1, \ldots, V_r$ be the set of $V \in F$ in which d is a non-unit; we renumber them so that $V_i \in F'$ if and only if $i \leq s$. For each $i > s$, there is an element s_i of S which is non-unit in V_i. If m is sufficiently large, we have $sc/d \in V_j$ for every j with $s = (s_{s+1} \cdots \cdots s_r)^m$. Then $sc/d \in V$ for any $V \in F$, whence $sc/d \in R$. Therefore $c/d \in R_S$.

(33.6) THEOREM: *Let* R *be an integral domain. Then there is an* F

as in (33.5) if and only if R is a Krull ring. In that case, $R_\mathfrak{p}$ is a member of F for every prime ideal $\mathfrak{p}$ of height 1 in R.

Proof: If R is a Krull ring, then the set of $R_\mathfrak{p}$, $\mathfrak{p}$ being prime ideals of height 1, satisfies the conditions for F. Conversely, assume that there is an F as in (33.5). (33.5) implies that there is a subset F' of F such that $R_\mathfrak{p} = \bigcap_{V \in F'} V$ for an arbitrarily given prime ideal $\mathfrak{p}$ of height 1. Let a be an element of $\mathfrak{p}$ different from zero. Since there is only a finite number of $V \in F$ in which a is a non-unit, we see that F' is a finite set, which implies that $R_\mathfrak{p}$ must be one $V \in F'$ by (11.11). Thus, if $\mathfrak{p}$ is a prime ideal of height 1 in R, then $R_\mathfrak{p}$ is in F and is a Noetherian valuation ring. Therefore it is sufficient to show that if $a \in R$, $a \neq 0$, then aR is the intersection of a finite number of primary ideals of height 1. Let $V_1, \ldots, V_r$ be the set of $V \in F$ in which a is non-unit and let $\mathfrak{m}_i$ be the maximal ideal of V_i. Set $\mathfrak{p}_i = \mathfrak{m}_i \cap R$, $\mathfrak{q}_i = aV_i \cap R$. Since $\mathfrak{m}_i^t \subseteq aV_i$ for some t, we have $\mathfrak{p}_i^t \subseteq \mathfrak{q}_i$, and since aV_i is primary, we see that $\mathfrak{q}_i$ is a primary ideal belonging to $\mathfrak{p}_i$. $b \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ implies that $b \in aV_i$ and by our choice of V_i we have $b \in aV$ for all $V \in F$, and $b/a \in \bigcap_{V \in F} V = R$, hence $b \in aR$. Therefore we see that $aR = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. We can derive an irredundant representation of aR from $\bigcap \mathfrak{q}_i$; let it be $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Assume, for instance, that height $\mathfrak{p}_1 \geq 2$. Let F' be the subset of F such that $R_{\mathfrak{p}_1} = \bigcap_{V \in F'} V$. If F' is a finite set, then $R_{\mathfrak{p}_1} \in F'$, by (11.11), which is impossible, whence F' is not a finite set. Therefore, there are infinitely many members V' of F' in which a is unit. Let $\mathfrak{m}'$ be the maximal ideal of an arbitrary V' as above, and set $\mathfrak{p}' = \mathfrak{m}' \cap R$. Then, since units of $R_{\mathfrak{p}_1}$ are units of V', we see that $\mathfrak{p}' \subset \mathfrak{p}_1$. $aR \neq \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s$ by our assumption. Since $\mathfrak{q}_1 : \mathfrak{p}_1^t = R$ for a t, we have $aR : \mathfrak{p}_1 \neq aR$. Let b be an element of $aR : \mathfrak{p}_1$ such that $b \notin aR$, and let h be an element of $\mathfrak{p}'$ ($h \neq 0$). Then $(b/a)h \in (b/a)\mathfrak{p}_1 \subseteq R$. Since $aV' = V'$, $(b/a)h \in \mathfrak{m}'$, whence we have $(b/a)h \in \mathfrak{p}'$. Thus $(b/a)\mathfrak{p}' \subseteq \mathfrak{p}'$, whence $(b/a)^n \mathfrak{p}' \subseteq \mathfrak{p}'$ for any natural number n, and therefore $(b/a)^n h \in R$, and $(b/a)^n h \in V$ for any $V \supset F$. Since V is a Noetherian valuation ring, and since the above is true for any large n, we see that $b/a \in V$. Since V is arbitrary, we conclude that $b/a \in \bigcap V = R$, and $b \in aR$, which contradicts the choice of b. Thus height $\mathfrak{q}_i = 1$ for $i \leq s$, and the assertion is proved completely.

(33.7) *If V is a Noetherian valuation ring of a field L and if K is a subfield of L, then $V \cap K$ is also a Noetherian valuation ring.*

Proof: Let a be an element of K. Then either $a \in V$ or $a^{-1} \in V$,

whence $a \in V \cap K$ or $a^{-1} \in V \cap K$, which shows that $V \cap K$ is a valuation ring. For elements a, b of V, $aV \subseteq bV$ if and only if a/b is in the maximal ideal $\mathfrak{m}$ of V, whence $a/b \in \mathfrak{m} \cap (V \cap K)$. Thus $aV \subset bV$ is equivalent to saying that $a(V \cap K) \subset b(V \cap K)$. Therefore, the maximum condition in V implies that in $V \cap K$, which proves the assertion.

(33.8) *Let R be an integral domain and let F be a family of prime ideals of R such that, for any element a of R, and for any prime divisor $\mathfrak{p}$ of aR, there is a $\mathfrak{q} \in F$ such that $\mathfrak{p} \subseteq \mathfrak{q}$. Then $R = \bigcap_{\mathfrak{q} \in F} R_{\mathfrak{q}}$.*

Proof: The inclusion $R \subseteq \bigcap R_{\mathfrak{q}}$ is obvious. Let a/b $(a, b \in R)$ be an arbitrary element of $\bigcap R_{\mathfrak{q}}$ and set $\mathfrak{c} = bR:aR$. $a/b \in R_{\mathfrak{q}}$ implies that $bR_{\mathfrak{q}}:aR_{\mathfrak{q}} = R_{\mathfrak{q}}$, hence that $\mathfrak{c}R_{\mathfrak{q}} = R_{\mathfrak{q}}$. Assume for a moment that $\mathfrak{c} \neq R$ and let $\mathfrak{p}$ be a prime divisor of $\mathfrak{c}$. Let p be an arbitrary element of $\mathfrak{p}$. Then, there is an element $y \notin \mathfrak{c}$ such that $py \in \mathfrak{c}$. Then $pya \in bR$. But, since $y \notin \mathfrak{c}$, we have $ya \notin bR$, and we see that p is a zero divisor modulo bR. Therefore, there is a prime divisor $\mathfrak{p}'$ of bR such that $\mathfrak{p} \subseteq \mathfrak{p}'$, hence there is a $\mathfrak{q} \in F$ such that $\mathfrak{p} \subseteq \mathfrak{q}$, whence $\mathfrak{c}R_{\mathfrak{q}} \subseteq \mathfrak{p}R_{\mathfrak{q}} \neq R_{\mathfrak{q}}$, which is a contradiction. Therefore $\mathfrak{c} = R$, namely, $a/b \in R$. Thus, the assertion is proved.

(33.9) COROLLARY: *If R is an integral domain, then $R = \bigcap R_{\mathfrak{m}}$ if $\mathfrak{m}$ runs over all maximal ideals of R.*

(33.10) THEOREM: *Let R be a Noetherian integral domain and let R' be the derived normal ring of R. Then*: (1) *R' is a Krull ring and* (2) *if $\mathfrak{p}$ is a prime ideal of R, then there are only a finite number of prime ideals $\mathfrak{p}'$ of R' such that $\mathfrak{p} = \mathfrak{p}' \cap R$, and, for any such $\mathfrak{p}'$, $R'/\mathfrak{p}'$ is an almost finite integral extension of $R/\mathfrak{p}$.*

Proof: We consider, first, the case where R is a local ring and $\mathfrak{p}$ is the maximal ideal of R. Let R^* be the completion of R and let $\mathfrak{n}^*$ be the radical of R^*. Set $S = R^*/\mathfrak{n}^*$. Since $\mathfrak{n}^* \cap R = 0$, R is regarded as a subring of S. Since any non-zero element a of R is not a zero divisor of R^* by (18.1), a is not in any minimal prime divisor of zero of R^*, whence a is not a zero divisor in S. Thus, the field of quotients K of R is a subring of the total quotient ring L of S. Let S' be the integral closure of S in L. We want to show first that $R' = S' \cap K$. The inclusion $R' \subseteq S' \cap K$ is obvious. Assume that a/b $(a, b \in R)$ is in $S' \cap K$. Then, since a/b is integral over S, there are elements $c_1', \ldots, c_n'$ of S such that $(a/b)^n + c_1'(a/b)^{n-1} + \cdots + c_n' = 0$. Let $c_i^* \in R^*$ be such that $c_i' = c_i^*$ modulo $\mathfrak{n}^*$. Then we have $a^n +$

$c_1^* a^m b + \cdots + c_n^* b^m \in \mathfrak{n}^*$. Since $\mathfrak{n}^*$ is nilpotent, some power of this last sum becomes zero, whence there are elements $d_1^*, \ldots, d_m^*$ of R^* such that $a^m + d_1^* a^m b + \cdots + d_m^* b^m = 0$. Whence $a^m \in (\sum_1^m a^m b^i R^*) \cap R$, and this last ideal is $\sum_1^m a^m b^i R$ by (17.9), which imply that there are elements $d_1, \ldots, d_m$ of R such that $a^m + d_1 a^m b + \cdots + d_m b^m = 0$, and a/b is integral over R, hence $a/b \in R'$ and the equality $R' = S' \cap K$ is proved. Let $\mathfrak{p}_1^*, \ldots, \mathfrak{p}_r^*$ be the prime divisors of $\mathfrak{n}^*$. Then L is the direct sum of the fields of quotients K_i of $R^*/\mathfrak{p}_i^*$ and S' is the direct sum of the derived normal rings S_i' of $R^*/\mathfrak{p}_i^*$. Since $R^*/\mathfrak{p}_i^*$ is a complete local ring, S_i' is a finite $(R^*/\mathfrak{p}_i^*)$-module, by (32.1). Let e_i be the identity of K_i. For an arbitrary prime ideal $\mathfrak{q}_i^*$ of height 1 in S_i', $(S_i')_{\mathfrak{q}_i^*}$ is a Noetherian valuation ring, because S_i' is a Noetherian normal ring. Set $\mathfrak{v}(\mathfrak{q}_i^*) = K_1 + \cdots + K_{i-1} + (S_i')_{\mathfrak{q}_i^*} + K_{i+1} + \cdots + K_r$. Then we see that the intersection of all possible $\mathfrak{v}(\mathfrak{q}_i^*)$ becomes S'. Therefore, we have $R' = \bigcap(K \cap \mathfrak{v}(\mathfrak{q}_i^*))$. It is obvious that $a \in K$ is in $K \cap \mathfrak{v}(\mathfrak{q}_i^*)$ if and only if $ae_i \in S'_{\mathfrak{q}_i^*}$, hence $K \cap \mathfrak{v}(\mathfrak{q}_i^*)$ is isomorphic to $Ke_i \cap (S_i')_{\mathfrak{q}_i^*}$, which implies that $K \cap \mathfrak{v}(\mathfrak{q}_i^*)$ is a Noetherian valuation ring, by (33.7). Thus R' is the intersection of Noetherian valuation rings $K \cap \mathfrak{v}(\mathfrak{q}_i^*)$ of K. If $a \in R'$ $(a \neq 0)$ is a non-unit in $\mathfrak{v}(\mathfrak{q}_i^*)$, then it follows that $a \in S_1' + \cdots + S_{i-1}' + \mathfrak{q}_i^* + S_{i+1}' + \cdots + S_r'$, and therefore there are only a finite number of such $\mathfrak{v}(\mathfrak{q}_i^*)$. Thus R' is a Krull ring in this case. Let $y_1, \ldots, y_t$ be arbitrary elements of R' and consider $R[y] = R[y_1, \ldots, y_t]$. $R[y]$ is a semi-local ring, whose completion is generated by R^* and the y_i. Therefore S' is the integral closure in L of $R^*[y]$ modulo its radical. Since this is true for any y, and since the completion of a semi-local ring having u maximal ideals is the direct sum of u local rings, we see that the number of maximal ideals of R' is at most r, and furthermore, the maximal ideals of S' lie over those of R'. Whence the assertion is proved for the case of a local ring R and its maximal ideal $\mathfrak{p}$. Now we consider the general case. Let S be the complement of $\mathfrak{p}$ in R. Then we see that R_S' is the derived normal ring of $R_S = R_{\mathfrak{p}}$. Therefore, by what was proved above, R_S' is a Krull ring and furthermore R_S' has only a finite number of maximal ideals $\mathfrak{p}'$ and $R_S'/\mathfrak{p}'$ is finite over $R_S/\mathfrak{p}R_S$, which implies the last assertion in our theorem. Furthermore, since $\mathfrak{p}$ is arbitrary, for any given prime ideal $\mathfrak{q}'$ of height 1 in R', applying the above for $\mathfrak{p} = \mathfrak{q}' \cap R$, we see that $R'_{\mathfrak{q}'}$ is a Krull ring, which shows that $R'_{\mathfrak{q}'}$ is a Noetherian valuation ring. Furthermore, we have $R' = \bigcap R'_{\mathfrak{p}'}$, where

$\mathfrak{p}'$ runs over all maximal ideals of R', by (33.9), whence $R' = \bigcap R'_{\mathfrak{q}'}$ where $\mathfrak{q}'$ runs over all prime ideals of height 1 in R', by the fact that the $R'_{\mathfrak{p}'}$ are Krull rings. Therefore, by (33.3), it remains only to prove that any principal ideal aR' of R' has only a finite number of minimal prime divisors. Since $R[a]$ is Noetherian and since R' is the derived normal ring of $R[a]$, we may assume that $a \in R$. aR has only a finite number of prime divisors, hence by the finiteness of lying-over prime ideals proved above, the finiteness of minimal prime divisors of aR' follows from the following lemma.

(33.11) *With the same R, a, and R' as above, if $\mathfrak{p}'$ is a minimal prime divisor of aR', then $\mathfrak{p} = \mathfrak{p}' \cap R$ is a prime divisor of aR.*

Proof: Let S be the complement of $\mathfrak{p}$ in R. Then $\mathfrak{p}'R'_S$ is a minimal prime divisor of aR'_S, and $\mathfrak{p}R_S = \mathfrak{p}'R'_S \cap R_S$. As is easily seen by the primary decomposition of aR, $\mathfrak{p}$ is a prime divisor of aR if and only if $\mathfrak{p}R_{\mathfrak{p}}$ is a prime divisor of $aR_{\mathfrak{p}}$. Therefore, by the fact that R'_S is the derived normal ring of R_S, we may assume that R is a local ring with maximal ideal $\mathfrak{p}$. Therefore R' is a Krull ring, in this case, whence height $\mathfrak{p}' = 1$. Since $\mathfrak{p} = \mathfrak{p}' \cap R$ is maximal, we see that $\mathfrak{p}'$ is also a maximal ideal by (10.7). Let x be an element of $\mathfrak{p}'$ which is not in any other maximal ideal of R'; x exists because R' has only a finite number of maximal ideals by our assumption. Set $R'' = R[x]$ and $\mathfrak{p}'' = \mathfrak{p}' \cap R''$. Then $\mathfrak{p}'$ is a unique prime ideal of R' which lies over $\mathfrak{p}''$. Therefore height $\mathfrak{p}''$ = height $\mathfrak{p}' = 1$ and $\mathfrak{p}''$ is maximal by (10.8). Consider the completion R''^* of R''. R''^* is the direct sum of complete local rings R_i where R_1 is the completion of $R''_{\mathfrak{p}''}$. Let e be the identity of R_1. Let R^* be the completion of R. Then $R''^* = R^*[x]$. There is an element $b \neq 0$ of R such that $bR'' \subseteq R$, whence $bR''^* \subseteq R^*[x]$. Since height $\mathfrak{p}'' = 1$, there is an n such that $(\mathfrak{p}R_1)^n \subseteq bR_1$. Therefore $\mathfrak{p}^n e \subseteq bR_1 \subseteq R^*$, whence $\mathfrak{p}^{tn}e \subseteq b^tR_1 \subseteq b^{t-1}R^*$. Assume for a moment that $\mathfrak{p}$ is not a prime divisor of bR. Then $\mathfrak{p}$ is not a prime divisor of b^tR for any t, by (12.6), hence $\mathfrak{p}$ contains an element p which is not a zero divisor modulo b^tR (in R), whence modulo b^tR^* in R^*. Therefore, the fact that $\mathfrak{p}^{tn}(\mathfrak{p}^n e) = \mathfrak{p}^{(t+1)n}e \subseteq b^tR^*$ implies that $\mathfrak{p}^n e \subseteq b^tR^*$ for any t, which is impossible because $\bigcap_t b^tR^* = 0$. Thus $\mathfrak{p}$ is a prime divisor of bR, hence of aR by (12.6). Thus the lemma is proved, and the proof of (33.10) is complete.

(33.12) THEOREM: *The derived normal ring R' of a Noetherian integral domain R of altitude 2 is again Noetherian.*

Proof: We have only to prove that if $\mathfrak{p}'$ is a prime ideal of R', then

$\mathfrak{p}'$ has a finite basis, by virtue of (3.4) (theorem of Cohen). We first prove the case where $\mathfrak{p}'$ is not maximal, assuming that every maximal ideal has a finite base. We may assume that $\mathfrak{p}' \neq 0$. Set $\mathfrak{p} = \mathfrak{p}' \cap R$. Then $\mathfrak{p}$ is not maximal by (10.7), whence height $\mathfrak{p} = 1$. Let a be an element of $\mathfrak{p}'$ which is not in any other prime ideal of R' which lies over $\mathfrak{p}$. Since $R[a]$ is Noetherian, we may replace R with $R[a]$. Thus we may assume that $\mathfrak{p}'$ is the unique prime ideal lying over $\mathfrak{p}$. Since $R'_{\mathfrak{p}'}$ is a Noetherian valuation ring, there is an element b of $\mathfrak{p}'$ such that $bR'_{\mathfrak{p}'} = \mathfrak{p}'R'_{\mathfrak{p}'}$. Considering $R[b]$, we may assume that $b \in R$, whence that $\mathfrak{p}'R'_{\mathfrak{p}'} = \mathfrak{p}R'_{\mathfrak{p}'}$. Set $\mathfrak{q}' = \mathfrak{p}R' : \mathfrak{p}'$. $\mathfrak{q}'$ contains $bR' : \mathfrak{p}'$. Since R' is a Krull ring, $bR' = \mathfrak{p}' \cap \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_r$ with primary ideals $\mathfrak{q}'_i$ ($\not\subseteq \mathfrak{p}'$) of height 1. Since $\mathfrak{p}'$ is the unique prime ideal lying over $\mathfrak{p}$, $\mathfrak{q}'_i \cap R$ is not contained in $\mathfrak{p}$, whence $\mathfrak{q}' \cap R$, which contains $(\mathfrak{q}'_1 \cap R) \cdots (\mathfrak{q}'_r \cap R)$, is not contained in $\mathfrak{p}$. Since $\mathfrak{q}' \cap R$ contains $\mathfrak{p}$, we see that $\mathfrak{q}' \cap R \supset \mathfrak{p}$ and depth $(\mathfrak{q}' \cap R) = 0$. Let $\mathfrak{q}'^*$ be the radical of $\mathfrak{q}'$. Since depth $(\mathfrak{q}' \cap R) = 0$, we see that $\mathfrak{q}'^*$ is the product of a finite number of maximal ideals, say $\mathfrak{m}'_1, \ldots, \mathfrak{m}'_r$. Since each $\mathfrak{m}'_i$ has a finite basis, we see that $\mathfrak{q}'^{*n}$ has a finite basis and that $R/\mathfrak{q}'^{*n}$ is Noetherian by the theorem of Cohen, and furthermore that $\mathfrak{q}'$ contains some $\mathfrak{q}'^{*n}$. It follows that $\mathfrak{q}'$ has a finite basis. $\mathfrak{q}'/\mathfrak{p}'\mathfrak{q}'$ is an $R'/\mathfrak{p}'$-module. Since $\mathfrak{q}'$ has a finite basis, $\mathfrak{q}'/\mathfrak{p}'\mathfrak{q}'$ is a finite module, whence its submodule $(\mathfrak{p}' \cap \mathfrak{q}')/\mathfrak{p}'\mathfrak{q}'$ is a finite module because $R'/\mathfrak{p}'$ is Noetherian by the theorem of Cohen. Since $\mathfrak{p}'\mathfrak{q}' \subseteq \mathfrak{p}R' \subseteq \mathfrak{p}' \cap \mathfrak{q}'$, we can consider $(\mathfrak{p}' \cap \mathfrak{q}')/\mathfrak{p}R'$, and it is a finite $R'/\mathfrak{p}'$-module. Since $\mathfrak{p}$ has a finite basis, we see that $\mathfrak{p}' \cap \mathfrak{q}'$ has a finite basis. Since $R'/\mathfrak{p}'$ and $R'/\mathfrak{q}'$ are Noetherian, we see that $R'/(\mathfrak{p}' \cap \mathfrak{q}')$ is Noetherian by (3.16), and we see that $\mathfrak{p}'/(\mathfrak{p}' \cap \mathfrak{q}')$ has a finite basis, and therefore $\mathfrak{p}'$ has a finite basis because $\mathfrak{p}' \cap \mathfrak{q}'$ has a finite basis. Thus, it remains only to prove that every maximal ideal of R' has a finite basis. Let $\mathfrak{m}'$ be an arbitrary maximal ideal of R'. By the same reason as stated above for $\mathfrak{p}'$, we may assume that $\mathfrak{m}'$ is a unique prime ideal lying over $\mathfrak{m} = \mathfrak{m}' \cap R$. Then $R'/\mathfrak{m}R' = R'_{\mathfrak{m}'}/\mathfrak{m}R'_{\mathfrak{m}'}$. Therefore we may assume that R and R' are local rings. If height $\mathfrak{m} = 1$, then the assertion is true by the theorem of Krull-Akizuki (33.2), and we assume that height $\mathfrak{m} = 2$. Let a, b be a system of parameters of R and let x be a transcendental element over R. If we know that $\mathfrak{m}'R'(x)$ has a finite basis, say $f_1, \ldots, \ldots, f_s$ ($\in R'[x]$), then we see that $\mathfrak{m}'$ is generated by the coefficients of f_i, and therefore $\mathfrak{m}'$ has a finite basis. Therefore it is sufficient to show that $\mathfrak{m}'R'(x)$ has a finite basis. Since aR and bR have no common

minimal prime divisors, we see that aR' and bR' have no common prime divisors by the facts that R' is a Krull ring and that $\mathfrak{m}'$ is the unique maximal ideal of R'. We want to show that $ax + b$ generates a prime ideal in $R'[x]$. Indeed, let $\mathfrak{p}^*$ be the prime ideal such that $R'[x]/\mathfrak{p}^* = R'[b/a]$ (x modulo $\mathfrak{p}^* = -b/a$). Then $\mathfrak{p}^*$ is generated by elements $cx + d$ with $c(b/a) = d$ by (11.13). Since aR' and bR' have no common prime divisors, we see that $c \in aR'$, whence $\mathfrak{p}^*$ is generated by $ax + b$. Therefore, we see that $ax + b$ generates a prime ideal in $R'(x)$. Consider $R^* = R(x)/((ax + b)R'(x) \cap R(x))$. This ring is Noetherian and of altitude 1. Therefore $R'(x)/(ax + b)R'(x)$ is Noetherian by the theorem of Krull-Akizuki, which implies that $\mathfrak{m}'R'(x)/(ax + b)R'(x)$, hence $\mathfrak{m}'R'(x)$, hence $\mathfrak{m}'$, too, have finite bases, which completes the proof.

We note that there is a local integral domain R of altitude 2 such that it has non-Noetherian integral extensions contained in its derived normal ring and that there is a local ring of altitude 3 whose derived normal ring is not Noetherian; see Examples 4 and 5 in the Appendix.

EXERCISES: *1.* Let R be a semi-local integral domain of altitude 1, and let R^* be the completion of R. Prove that R is analytically unramified if and only if the derived normal ring R' of R is a finite R-module. Prove also that the number of the prime divisors of zero in R^* coincides with that of maximal ideals in R'.

(Note that the above assertions are not true in general if we do not assume that altitude $R = 1$; see Examples 6 and 7 in the Appendix.)

2. Let R be a Noetherian integral domain of altitude 1 and with field of quotients K. Prove that if L is a finite algebraic extension of K and if R' is a ring such that $R \subseteq R' \subseteq L$, then there is an integral extension R'' of R such that R' is a ring of quotients of R''.

34. *Chains of prime ideals*

Let R be a ring and let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals of R such that $\mathfrak{p} \subset \mathfrak{q}$. A chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$ in R is called a *maximal chain of prime ideals* between $\mathfrak{p}$ and $\mathfrak{q}$ if $\mathfrak{p}_0 = \mathfrak{p}$, $\mathfrak{p}_r = \mathfrak{q}$ and if there is no prime ideal $\mathfrak{p}'$ of R such that $\mathfrak{p}_{i-1} \subset \mathfrak{p}' \subset \mathfrak{p}_i$ for any $i = 1, \ldots, r$. A maximal chain of prime ideals between a minimal prime divisor of zero and a maximal ideal is called a *maximal chain of prime ideals* in R.

We say that R satisfies *the chain condition for prime ideals* if, for any prime ideals $\mathfrak{p} \subset \mathfrak{q}$, and for any integral extension R' of $R_\mathfrak{q}/\mathfrak{p}R_\mathfrak{q}$, every maximal chain of prime ideals in R' has length equal to altitude R'. Note that this is equivalent to saying that if R^* is integral over

R and if $\mathfrak{p}'$, $\mathfrak{q}'$ are prime ideals of R^* such that $\mathfrak{p}' \subset \mathfrak{q}'$ and such that $\mathfrak{p} = \mathfrak{p}' \cap R$, $\mathfrak{q} = \mathfrak{q}' \cap R$, the length of any maximal chain of prime ideals between $\mathfrak{p}'$ and $\mathfrak{q}'$ is equal to height $\mathfrak{q}/\mathfrak{p}$.

It is obvious by our definition that:

(34.1) *If a ring R satisfies the chain condition for prime ideals then the condition is satisfied by any $R'_S/\mathfrak{a}'R'_S$, where R' is an over-ring of R such that R' is integral over R, $\mathfrak{a}'$ is an ideal of R', and S is a multiplicatively closed subset of R'.*

In order to discuss the condition, we introduce the following terminology for a ring R.

We say that R satisfies *the first chain condition for prime ideals* if every maximal chain of prime ideals in R has length equal to altitude R. We say that R satisfies *the second chain condition for prime ideals* if, for every minimal prime divisor $\mathfrak{p}$ of zero in R, and for any integral extension R' of $R/\mathfrak{p}$, the length of any maximal chain of prime ideals in R' is equal to altitude R. Note that the validity of the second chain condition for prime ideals in a ring R whose altitude is finite is equivalent to (a) every maximal ideal $\mathfrak{m}$ of R has height equal to altitude R and (b) R satisfies the chain condition for prime ideals.

We note that, though the validity of the second chain condition for prime ideals implies the validity of the first one, the converse is not true. See Example 2 in the Appendix.

We note furthermore that a ring R whose altitude is finite satisfies the chain condition for prime ideals if and only if for every minimal prime divisor $\mathfrak{p}$ of zero in R and for every maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{p}$, the ring $R_{\mathfrak{m}}/\mathfrak{p}R_{\mathfrak{m}}$ satisfies the second chain condition for prime ideals. Therefore, it is of great importance to discuss the second chain condition for prime ideals in local integral domains.

(34.2) *Assume that R is a subring of a ring R' and that R' is integral over R. If R' satisfies the chain condition, or the first or the second chain condition, for prime ideals, then R does, too.*

The proof is immediate from (10.9).

(34.3) *A Noetherian integral domain R satisfies the second chain condition for prime ideals if and only if the first chain condition is satisfied by every finite integral extension R'' of R.*

Proof: The *only if* part is obvious by definition. Assume the validity of the first chain condition in any R'' as above and let R' be an arbitrary integral extension of R. Let $0 = \mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \cdots \subset \mathfrak{p}'_r$ be a maximal chain of prime ideals in R'. Set $\mathfrak{p}_i = \mathfrak{p}'_i \cap R$. Then there are only

a finite number of prime ideals in R' which lie over $\mathfrak{p}_i$, by (33.10), whence there is a finite extension R'' of R ($R'' \subseteq R'$) such that every $\mathfrak{p}_i'$ is the unique prime ideal of R' lying over $\mathfrak{p}_i''$ $\quad \mathfrak{p}_i' \cap R''$. Since $\mathfrak{p}_0'' \subset \mathfrak{p}_1'' \subset \cdots \subset \mathfrak{p}_r''$ is a maximal chain of prime ideals in R'' by the going-up theorem, we see that r = altitude R'' = altitude R, which proves the assertion.

(34.4) THEOREM: *If R is a complete semi-local ring, then the following three conditions are equivalent to each other:*

(1) *R satisfies the second chain condition for prime ideals.*

(2) *R satisfies the first chain condition for prime ideals.*

(3) *Every minimal prime divisor of zero in R has depth equal to* altitude R.

Proof: (1) implies (2) and (2) implies (3) obviously. Therefore, it is sufficient to show that (3) implies (1), and for that purpose, it is sufficient to show that the second chain condition is satisfied by every complete local integral domain R. Since any finite integral extension of R is again a complete local integral domain, by (30.5), it suffices to show that the first chain condition is satisfied by every complete local integral domain by virtue of (34.3). Let R be an arbitrary complete local integral domain. Set r = altitude R and let $0 = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_s$ be a maximal chain of prime ideals in R. Let I be a coefficient ring of R. We prove that $r = s$ by induction on r. If $s = 0$, then the assertion is obvious, and we assume that $s > 0$. We consider at first the case where I is a field. Let x_1 be an arbitrary non-zero element of $\mathfrak{p}_1$. Then there exists a system of parameters $x_1, \ldots, \ldots, x_r$ of R, and R is a finite module over the complete regular local ring $I[[x]] = I[[x_1, \ldots, x_r]]$ by (31.5). Since a regular local ring is a normal ring by (25.14), height $(\mathfrak{p}_1 \cap I[[x]]) = 1$ by (10.14), hence $\mathfrak{p}_1 \cap I[[x]]$ is generated by x_1. Thus $R/\mathfrak{p}_1$ is a finite module over $I[[x]]/x_1 I[[x]]$, which is of altitude $r - 1$. Since $0 = \mathfrak{p}_1/\mathfrak{p}_1 \subset \mathfrak{p}_2/\mathfrak{p}_1 \subset \cdots \cdots \subset \mathfrak{p}_s/\mathfrak{p}_1$ is a maximal chain of prime ideals in $R/\mathfrak{p}_1$, we see that $s - 1 = r - 1$ by induction, which proves the assertion in this case. Assume that I is not a field and let p be a prime element of I. If $p \in \mathfrak{p}_1$, we see that $R/\mathfrak{p}_1$ is a finite integral extension of $I[[x_1, \ldots, \ldots, x_{r-1}]]/pI[[x_1, \ldots, x_{r-1}]]$ with x_i such that $p, x_1, \ldots, x_{r-1}$ is a system of parameters of R, and we prove this case similarly. If $p \notin \mathfrak{p}$, let $x_1, \ldots, x_{r-1}$ be such that $x_1 \in \mathfrak{p}$ and such that $p, x_1, \ldots, x_{r-1}$ is a system of parameters of R. Then we prove the case similarly. Thus we prove the assertion.

We say that a semi-local ring R is *quasi-unmixed* if every minimal

prime divisor of zero in the completion of R has depth equal to altitude R.

(34.5) *If R is a quasi unmixed semi local ring and if $\mathfrak{p}$ is a prime ideal of R, then $R/\mathfrak{p}$ is quasi unmixed and* height $\mathfrak{p}$ + depth $\mathfrak{p}$ altitude R.

Proof: Let R^* be the completion of R and let $\mathfrak{p}^*$ be an arbitrary minimal prime divisor of $\mathfrak{p}R^*$. Since the theorem of transition holds for R and R^*, we see that height $\mathfrak{p}$ = height $\mathfrak{p}^*$ by (22.9). Since R^* satisfies the first chain condition by (34.4), we see that depth $\mathfrak{p}^*$ altitude R − height $\mathfrak{p}^*$ = altitude R − height $\mathfrak{p}$. Since this is true for any minimal prime divisors $\mathfrak{p}^*$ of $\mathfrak{p}R^*$ and since $R^*/\mathfrak{p}R^*$ is the completion of $R/\mathfrak{p}$, by (17.9), we see that depth $\mathfrak{p}^*$ = altitude $R^*/\mathfrak{p}R^*$ = altitude $R/\mathfrak{p}$ = depth $\mathfrak{p}$ and that the assertion is true.

(34.6) THEOREM: *Every quasi-unmixed semi-local ring R satisfies the second chain condition for prime ideals.*

Proof: We see easily the validity of the first chain condition in R, by (34.5) and by induction on altitude R. Let $\mathfrak{p}$ be an arbitrary minimal prime divisor of zero in R. Then, since height $\mathfrak{p} = 0$, it holds that depth $\mathfrak{p}$ = altitude R. Therefore, by the remark given above and by (34.3), we have only to prove that every finite integral extension R' of $R/\mathfrak{p}$ is quasi-unmixed, which is easy because $R/\mathfrak{p}$ is quasi unmixed by (34.5).

(34.7) COROLLARY: *Assume that R is an unmixed semi-local integral domain and that R' is an integral extension of R. A chain of prime ideals $\mathfrak{p}_0' \subset \mathfrak{p}_1' \subset \cdots \subset \mathfrak{p}_r'$ in R' is maximal if and only if $(\mathfrak{p}_0' \cap R) \subset (\mathfrak{p}_1' \cap R) \subset \cdots \subset (\mathfrak{p}_r' \cap R)$ is a maximal chain of prime ideals in R. Furthermore, if $\mathfrak{a}'$ is an ideal of R', then* height $\mathfrak{a}'$ = height $(\mathfrak{a}' \cap R)$.

Proof: The first is an easy consequence of the validity of the second chain condition for prime ideals. Consequently, the last assertion is true if $\mathfrak{a}'$ is a prime ideal, whence the proof of (10.14) can be applied, which proves the last assertion.

(34.8) COROLLARY: *If R is a homomorphic image of a locally Macaulay ring, then R satisfies the chain condition for prime ideals. If furthermore R is an integral domain and if R' is a finite integral extension of R, then for an ideal $\mathfrak{a}'$ of R', it holds that* height $\mathfrak{a}'$ = height $(\mathfrak{a}' \cap R)$.

We add here the following result on unmixedness of local rings:

(34.9) THEOREM: *A local integral domain is unmixed if it is a homomorphic image of a Macaulay local ring.*

Proof: Assume that $\mathfrak{p}$ is a prime ideal of a Macaulay local ring R. Let r be the height of $\mathfrak{p}$ and let $x_1, \ldots, x_r$ be elements of $\mathfrak{p}$ such that $\mathfrak{a} = \sum x_i R$ is of height r (by (9.5)). Let R^* be the completion of R. Then R^* is a Macaulay ring, hence the unmixedness theorem holds in R^* by (25.6), which implies that every prime divisor of $\mathfrak{a}R^*$ is a minimal prime divisor, and $R^*/\mathfrak{a}R^*$ is unmixed (cf. Exercise in §25). Since $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$, every prime divisor of $\mathfrak{p}R^*$ is a prime divisor of $\mathfrak{a}R^*$, by (18.11), and therefore it follows that $R^*/\mathfrak{p}R^*$ is unmixed. Thus the assertion is proved.

(34.10) COROLLARY: *Assume that R is a Macaulay semi-local ring. For an ideal $\mathfrak{a}$ of R, $R/\mathfrak{a}$ is an unmixed semi-local ring if and only if every prime divisor of $\mathfrak{a}$ is of height which is equal to* height $\mathfrak{a}$.

CHAPTER VI

Geometric Local Rings

35. *Localities*

We say that a ring R' is of *finitely generated type* over a ring R if R' is a ring of quotients of a finitely generated ring R^* over R; R' is said to be of *finite type* over R if furthermore R^* can be chosen to be integral over R.

A ring R is called an *affine ring* over a ring I if R is an integral domain and if R is finitely generated over I, whence I must be an integral domain in this case. A quasi-local integral domain which is of finitely generated type over a ring I is called a *locality* over I. Such an I as above is called a *ground ring* of the affine ring of the locality. Note that local rings which are used in usual algebraic geometry are localities over fields, which we call *algebraic-geometrical local rings*. In ring-theoretic formulations of algebraic geometry, it is sometimes convenient not to restrict oneself to localities but to consider local rings which are of finitely generated type over fields or some kinds of rings. But, most of the important results on them are conveniently formulated in the case of integral domains or are derived easily from that case, and this is the reason we defined a special term "locality." Of course, we do not have any good results without any restriction on the ring I. Since the case where I is a field is rather too special from the ring-theoretic point of view, we shall prove important results concerning algebraic-geometrical local rings for more general cases in this chapter.

We say that an integral domain I satisfies the *finiteness condition for integral extensions* if every almost finite integral extension of I is a finite extension.

We note that:

(35.1) *If an integral domain I satisfies the finiteness condition for integral extensions, then so does every ring of quotients of I.*

The proof is straightforward and we omit it.

A field L is called a *function field* over a ground ring I if L is the

field of quotients of an affine ring over I. If L is the field of quotients of a ring R which is an affine ring or a locality over I, then we say that L is the *function field of* R and that R is an *affine ring* or a *locality of* L.

We begin with the following finiteness theorem for polynomial rings:

(35.2) THEOREM. *Let $x_1, \ldots, x_n$ be algebraically independent elements over a Noetherian integral domain I. If I satisfies the finiteness condition for integral extensions, then so does $I[x] = I[x_1, \ldots, x_n]$.*

Proof. Let L be an arbitrary finite extension of the field of quotients K of $I[x]$. We have only to prove that an arbitrary integral extension R of $I[x]$ contained in L is a finite $I[x]$-module. By our assumption for I, we may assume that I is normal. If L is separable over K, then the assertion is obvious by (10.16). When L is inseparable over K, take elements $a_1, \ldots, a_r$ of I and a power q of the characteristic p of I such that $L' = L(a_1^{1/q}, \ldots, a_r^{1/q}, x_1^{1/q}, \ldots, x_n^{1/q})$ is separable over $K' = K(a_1^{1/q}, \ldots, a_r^{1/q}, x_1^{1/q}, \ldots, x_n^{1/q})$. Let I' be the derived normal ring of $I[a_1^{1/q}, \ldots, a_r^{1/q}]$. Then I' is finite over I by our assumption, and $I'[x_1^{1/q}, \ldots, x_n^{1/q}]$ is finite over $I[x]$. Since L' is separable over K', the integral closure of $I'[x_1^{1/q}, \ldots, x_n^{1/q}]$ in L' is finite over $I'[x_1^{1/q}, \ldots, \ldots, x_n^{1/q}]$, whence it is finite over $I[x]$. Therefore R is finite over $I[x]$ by (3.1).

(35.3) THEOREM. *Let A be an affine ring over a Noetherian integral domain I. Assume that I satisfies the finiteness condition for integral extensions and that the derived normal ring of $A_\mathfrak{p}$ is a finite $A_\mathfrak{p}$-module for every prime ideal $\mathfrak{p}$ of A. Then the derived normal ring A' of A is a finite A-module.*

Proof. There are elements $z_1, \ldots, z_r$ of A which are algebraically independent over I and an element a ($\neq 0$) of I such that $A[1/a]$ is integral over $I[1/a, z] = I[1/a, z_1, \ldots, z_r]$ by (14.4). Let L be the field of quotients of A. Then the integral closure of $I[1/a, z]$ in L is $A'[1/a]$ and is a finite $I[1/a, z]$-module by (35.2). Thus we see that $A'[1/a]$ is a finite $A[1/a]$-module, whence there are a finite number of elements $b_1, \ldots, b_s$ of A' such that $A'[1/a] = A[1/a, b_1, \ldots, b_s]$. Set $A_1 = A[b_1, \ldots, b_s]$. If a is a unit in A, then the assertion is obvious and we assume that a is a non-unit in A. Let the prime divisors of aA_1 be $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Then there are a finite number of elements $c_1, \ldots, c_u$ of A' such that $(A_1)_{\mathfrak{p}_i}[c_1, \ldots, c_u]$ is normal for every $\mathfrak{p}_i$. We set $A_2 = A[b_1, \ldots, b_s, c_1, \ldots, c_u]$. A_2 is a finite A-module. We prove here the following:

Let B be a Noetherian ring such that $A_2 \subset B \subset A'$. Then (1) if $\mathfrak{p}$ is a prime ideal of height 1 in B, then $B_{\mathfrak{p}}$ is a normal ring and (2) if the imbedded prime divisors of aB are $\mathfrak{q}_1, \ldots, \mathfrak{q}_w$ and if $d_1, \ldots, \ldots, d_m$ are elements of A' such that $B_{\mathfrak{q}_i}[d_1, \ldots, d_m]$ is normal for every $\mathfrak{q}_i$, then for an arbitrary imbedded prime divisor $\mathfrak{q}'$ of $aB[d_1, \ldots, d_m]$, $\mathfrak{q}' \cap B$ contains some $\mathfrak{q}_i$ properly ($\mathfrak{q}_i \subset \mathfrak{q}' \cap B$).

Indeed, if $a \notin \mathfrak{p}$, then $B_{\mathfrak{p}}$ contains $1/a$, and $B_{\mathfrak{p}}$ is a ring of quotients of $A'[1/a]$, which implies that $B_{\mathfrak{p}}$ is normal in this case; if $a \in \mathfrak{p}$, set $\mathfrak{p}' = \mathfrak{p} \cap A_1$, $\mathfrak{p}'' = \mathfrak{p} \cap A_2$. Since height $\mathfrak{p} = 1$, we see that $\mathfrak{p}'$ is a prime divisor of aA_1 by (33.11) (by virtue of the going-up theorem applied to B and A' with $0 \subset \mathfrak{p}$). Therefore $(A_2)_{\mathfrak{p}''}$ is normal, and $(A_2)_{\mathfrak{p}''}$ contains A', whence $B_{\mathfrak{p}}$ is a ring of quotients of A' and is a normal ring, and (1) is proved. As for (2), set $\mathfrak{q} = \mathfrak{q}' \cap B$. Since $\mathfrak{q}'$ is an imbedded prime divisor of $aB[d_1, \ldots, d_w]$, $B[d_1, \ldots, d_w]_{\mathfrak{q}'}$ is not a normal ring, by (12.9). By the same reason as for $B_{\mathfrak{p}}$ above, we see that $B_{\mathfrak{q}}$ is not a normal ring, whence, by virtue of (1), we see that $aB_{\mathfrak{q}}$ has an imbedded prime divisor $\mathfrak{q}''B_{\mathfrak{q}}$, which must be some $\mathfrak{q}_iB_{\mathfrak{q}}$. Since $B_{\mathfrak{q}_i}[d_1, \ldots, d_s]$ is a normal ring, $\mathfrak{q}$ cannot be the $\mathfrak{q}_i$, whence $\mathfrak{q}_i \subset \mathfrak{q}$, and (2) is proved.

Now we proceed with the proof of (35.3). Starting with $B_0 = A_2$, we construct a sequence B_i of rings as follows: When B_i is defined, let $d_1, \ldots, d_w$ be as in (2) above, applied for $B = B_i$, and set $B_{i+1} = B_i[d_1, \ldots, d_w]$. Then, by the finiteness of the ascending chain of prime ideals in A_2, we see that there is a B_n such that aB_n has no imbedded prime divisor. Then the assertion is proved, because B_n is normal, whence $B_n = A'$, by the following lemma:

(35.4) *Let R be a Noetherian integral domain and let a ($\neq 0$) be an element of R. Assume that $R[1/a]$ is a normal ring and that $R_{\mathfrak{p}}$ is a normal ring for every prime divisor $\mathfrak{p}$ of aR. Then R is a normal ring.*

Proof. Let $\mathfrak{q}$ be a prime ideal of height 1 in R. If $a \notin \mathfrak{q}$, then $R_{\mathfrak{q}}$ is a ring of quotients of $R[1/a]$ and is a normal ring. If $a \in \mathfrak{q}$, then $\mathfrak{q}$ is a minimal prime divisor of aR and $R_{\mathfrak{q}}$ is a normal ring. Let b ($\neq 0$) be an element of R and assume that bR has an imbedded prime divisor $\mathfrak{q}$. Since $R[1/a]$ is a normal ring, $bR[1/a]$ has no imbedded prime divisor, whence $\mathfrak{q}R[1/a] = R[1/a]$, that is, $a \in \mathfrak{q}$, which implies that $\mathfrak{q}$ is an embedded prime divisor of aR by (12.6), which is a contradiction, and (35.4) is proved by virtue of (12.9).

If I is a subring of an integral domain R, the transcendence degree of R over I is denoted by trans. $\deg_I R$.

We say that the *altitude formula* holds for an integral domain I if,

for any locality $(R, \mathfrak{m})$ over I, altitude R | trans. $\deg_{I/(\mathfrak{m}\cap I)} R/\mathfrak{m}$ altitude $I_{(\mathfrak{m}\cap I)}$ | trans. $\deg_I R$.

(35.5) THEOREM. *If an integral domain I is a homomorphic image of a locally Macaulay ring M, then the altitude formula holds for I. Furthermore, any locality R over I is a homomorphic image of a Macaulay ring, and consequently, the chain condition for prime ideals and the altitude formula hold in R.*

Proof. There are algebraically independent elements $x_1, \ldots, x_n$ over M and prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$ of $M[x] = M[x_1, \ldots, x_n]$ such that $R = M[x]_{\mathfrak{p}}/\mathfrak{q}M[x]_{\mathfrak{p}}$. Since $M[x]$ is a locally Macaulay ring by (25.10), $M[x]_{\mathfrak{p}}$ is a Macaulay ring, and R is a homomorphic image of a Macaulay ring, whence the last assertion follows from (34.8) and the first assertion. In order to prove the first assertion, we have only to prove the formula stated above for I and R, because R is arbitrary. We prove it by induction on n as follows: If $n = 1$, then the assertion is straightforward by the validity of the chain condition for prime ideals in any affine ring over I and, in particular, in $M[x]$. Assume that $n > 1$, and set $B = I[x_1]/(\mathfrak{q} \cap I[x_1])$, $\mathfrak{p}' = \mathfrak{m} \cap B$. Then altitude $B_{\mathfrak{p}'}$ + trans. $\deg_{I/(\mathfrak{p}'\cap I)} B/\mathfrak{p}'$ = altitude $I_{(\mathfrak{p}'\cap I)}$ + trans. $\deg_I B$ by the case $n = 1$, and altitude R + trans. $\deg_{B/\mathfrak{p}'} R/\mathfrak{m}$ = altitude $B_{\mathfrak{p}'}$ + trans. $\deg_B R$. Since $\mathfrak{m} \cap I = \mathfrak{p}' \cap I$, we prove the formula. Thus (35.5) is proved completely.

As an application of (35.5) to general Noetherian integral domains, we can prove the following theorem:

(35.6) THEOREM. *Let A be an affine ring over a Noetherian integral domain I and set r = trans. $\deg_I A$. If $\mathfrak{p}$ is a prime ideal of I and if $\mathfrak{p}'$ is a minimal prime divisor of $\mathfrak{p}A$ such that $\mathfrak{p} = \mathfrak{p}' \cap I$, then* trans. $\deg_{I/\mathfrak{p}} A/\mathfrak{p}' \geq r$.

Proof. Let S be the complement of $\mathfrak{p}$ in I. Then considering I_S and A_S, we may assume that $(I, \mathfrak{p})$ is a local ring. We prove the assertion by double induction on height $\mathfrak{p}$ and the number of generators of A over I. If height $\mathfrak{p} \leq 1$, then by our assumption, I is a Macaulay ring, whence by the altitude formula we prove the assertion in this case. Therefore, we assume that height $\mathfrak{p} \geq 2$. If height $\mathfrak{p}' \neq 1$, then let $\mathfrak{q}'$ be a prime ideal of A such that $\mathfrak{q}' \subset \mathfrak{p}'$, $\mathfrak{q}' \cap I \neq 0$ and such that height $\mathfrak{q}' = 1$. Since $\mathfrak{p}'$ is a minimal prime divisor of $\mathfrak{p}A$, we see that $\mathfrak{q}' \cap I \neq \mathfrak{p}$. Since height $\mathfrak{q}' = 1$, $\mathfrak{q}'$ is a minimal prime divisor of $(\mathfrak{q} \cap I)A$, whence by our induction on height $\mathfrak{p}$, applied to $\mathfrak{q}' \cap I$,

we see that trans. $\deg_{R/(q'\cap I)} R/q' = r$. Therefore, by our induction applied to $\mathfrak{p}/(\mathfrak{q}' \cap I)$, we see that the assertion is true in this case. Therefore, we assume that height $\mathfrak{p}' \geq 1$. Let $x_1, \ldots, x_n$ be a set of generators of A over I. If $A/\mathfrak{p}'$ is not algebraic over $I/\mathfrak{p}$, say if x_1 modulo $\mathfrak{p}'$ is not algebraic over $I/\mathfrak{p}$, then we consider $A'' = I[x_1]$ and $\mathfrak{p}'' = \mathfrak{p}' \cap A''$. Since x_1 modulo $\mathfrak{p}''$ is transcendental over $I/\mathfrak{p}$, we see that $\mathfrak{p}'' = \mathfrak{p}A''$ and that height $\mathfrak{p}'' \leq$ height $\mathfrak{p}$ by the altitude theorem of Krull and by the fact that a system of parameters of $I_{\mathfrak{p}}$ generates an ideal which is primary to $\mathfrak{p}''A''_{\mathfrak{p}''}$ in $A''_{\mathfrak{p}''}$, whence by our induction on n applied to A over A'' with the prime ideal $\mathfrak{p}''$, we see that trans. $\deg_{A''/\mathfrak{p}''} A/\mathfrak{p}' \geq$ trans. $\deg_{A''} A$. Since trans. $\deg_{I/\mathfrak{p}} A''/\mathfrak{p}'' = 1$ and since trans. $\deg_I A'' \leq 1$, we prove the assertion in this case. Therefore, we assume that $A/\mathfrak{p}'$ is algebraic over $I/\mathfrak{p}$. It suffices to prove now that A is algebraic over I. Let A^* be the derived normal ring of A and let $\mathfrak{p}^*$ be a prime ideal of A^* which lies over $\mathfrak{p}'$. Then height $\mathfrak{p}^* = 1$ by the going-up theorem. Since A^* is a Krull ring by (33.10), $A^*_{\mathfrak{p}^*}$ is a Noetherian valuation ring. Let K be the field of quotients of I and set $B = A^*_{\mathfrak{p}^*} \cap K$. B is a Noetherian valuation ring by (33.7). Set $C = B[A]$; this last ring is an affine ring over B. Set furthermore $\mathfrak{p}^{**} = \mathfrak{p}^*A^*_{\mathfrak{p}^*} \cap B$ and $\mathfrak{p}'' = \mathfrak{p}^*A^*_{\mathfrak{p}^*} \cap C$, and let C^* be the derived normal ring of C. Then obviously $A^* \subseteq C^* \subseteq A^*_{\mathfrak{p}^*}$, whence $A^*_{\mathfrak{p}^*}$ is a ring of quotients of C^*, that is, $A^*_{\mathfrak{p}^*} = C^*_{\mathfrak{r}}$ with $\mathfrak{r} = \mathfrak{p}^*A^*_{\mathfrak{p}^*} \cap C^*$. It follows that $\mathfrak{r}$ is a minimal prime divisor of $\mathfrak{p}^{**}C^*$ and height $\mathfrak{r} = 1$. Since B contains I, $B/\mathfrak{p}^{**}$ contains $I/\mathfrak{p}$, whence $A^*_{\mathfrak{p}^*}/\mathfrak{p}^*A^*_{\mathfrak{p}^*}$ is algebraic over $B/\mathfrak{p}^{**}$. Therefore $C^*/\mathfrak{r}$ is algebraic over $B/\mathfrak{p}^{**}$, whence C^* is algebraic over B by (35.5) and by the fact that B is a Macaulay ring, which proves that A is algebraic over I. Thus the proof is complete.

36. *Pseudo-geometric rings*

We say that a ring R is a *pseudo-geometric ring* if R is Noetherian and if, for every prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ satisfies the finiteness condition for integral extensions.

We note first that:

(36.1) *If R is a pseudo-geometric ring, then every homomorphic image of R, every ring of quotients of R, and every ring which is a finite module over R are pseudo-geometric rings.*

The proof is straightforward.

(36.2) *Let R be a semi-local integral domain and assume that $\mathfrak{p}$ is a*

prime ideal of height 1 in R such that $R_{\mathfrak{p}}$ is a valuation ring. If $\mathfrak{p}$ is analytically unramified and if $\mathfrak{p}^*$ is a minimal prime divisor of $\mathfrak{p}R^*$, R^* being the completion of R, then $R^*_{\mathfrak{p}^*}$ is a valuation ring.

Proof. Let w be an element of $\mathfrak{p}$ which is not in $\mathfrak{p}^2R_{\mathfrak{p}}$. Then $\mathfrak{p}R_{\mathfrak{p}} = wR_{\mathfrak{p}}$, whence $\mathfrak{p}^*R^*_{\mathfrak{p}^*} = wR^*_{\mathfrak{p}^*}$. Since w is not a zero divisor in R^* by (18.1), we see that $R^*_{\mathfrak{p}^*}$ is a valuation ring by (12.1).

(36.3) *Let R be a semi-local integral domain and let x ($\neq 0$) be an element of the Jacobson radical of R. Assume that xR has no imbedded prime divisor and that, for every prime divisor $\mathfrak{p}$ of xR, $\mathfrak{p}$ is analytically unramified and $R_{\mathfrak{p}}$ is a valuation ring. Then R is analytically unramified.*

Proof. Let R^* be the completion of R and let the prime divisors of xR be $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. By our assumption, and by (36.2), if the prime divisors of $\mathfrak{p}_iR^*$ are $\mathfrak{p}^*_{ij}$ ($j = 1, \ldots, n(i)$), then each $\mathfrak{p}^*_{ij}$ contains a prime divisor $\mathfrak{P}^*_{ij}$ of zero which is the kernel of the natural homomorphism from R^* into the valuation ring $R^*_{\mathfrak{p}^*_{ij}}$. Let $\mathfrak{n}$ be the intersection of all the $\mathfrak{P}^*_{ij}$. Since the $\mathfrak{p}_i$ are all the prime divisors of xR, we see that the $\mathfrak{p}^*_{ij}$ are all the prime divisors of xR^* by (18.11). Since $\mathfrak{P}^*_{ij}$ is contained in any primary ideal belonging to $\mathfrak{p}^*_{ij}$, we see that $\mathfrak{n}$ is contained in xR^*. Since x is in the Jacobson radical of R^* and since $\mathfrak{n}:xR^* = \mathfrak{n}$, we see that $\mathfrak{n} = 0$ by (4.3), which proves that the zero ideal of R^* is semi-prime, i.e., R is analytically unramified.

(36.4) THEOREM. *A pseudo-geometric semi-local integral domain R is analytically unramified.*

Proof. We prove the assertion by induction on r = altitude R. Let R' be the derived normal ring of R. Then R' is a finite R-module by our assumption, whence R is a subspace of R' by (16.8). Therefore, it is sufficient to show that R' is analytically unramified. Since R' is pseudo-geometric, we may assume that R is normal. If $r = 0$, then the assertion is obvious, and we assume that $r \geq 1$. Let x ($\neq 0$) be an element of the Jacobson radical of R. Then, by (36.3) applied to this x, we see that R is analytically unramified, which proves the assertion.

(36.5) THEOREM. *If R is a pseudo-geometric ring, then every ring which is of finitely generated type over R is a pseudo-geometric ring.*

Proof. By the definition, and by (36.1), we have only to prove that if R is a pseudo-geometric integral domain, then every affine ring A over R is a pseudo-geometric ring. Using induction on the

number of generators of A, we have only to prove the case where $A = R[x]$ with an element x of A. It suffices to show that if $\mathfrak{q}$ is a prime ideal of A, then $A/\mathfrak{q}$ satisfies the finiteness condition for integral extensions. Since $R/(\mathfrak{q} \cap R)$ is pseudo geometric, we have only to prove that A as above satisfies the finiteness condition for integral extensions. If x is transcendental over R, then the assertion follows from (35.2), and we assume that x is algebraic over R. Then, considering a suitable finite integral extension of R, which is pseudo geometric by (36.1), we may assume that x is in the field of quotients K of R. Let L be an arbitrary finite algebraic extension of K. In order to prove the finiteness of the integral closure A' of A in L, since the integral closure of R in L is a finite R-module, we may assume that $L = K$ and that R is a normal ring. Thus it is sufficient to prove the finiteness of the derived normal ring of A (assuming that R is normal, and that $x \in K$). By virtue of (35.3), it suffices to show that if $\mathfrak{p}$ is a prime ideal of A, then the derived normal ring of $A_{\mathfrak{p}}$ is a finite module over $A_{\mathfrak{p}}$. Obviously, we have only to prove it in the case where $\mathfrak{p}$ is maximal. Since $R_{(\mathfrak{p} \cap R)}$ is a pseudo-geometric local ring, we may assume furthermore that R is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p} \cap R$. Since $\mathfrak{p}$ is maximal, x modulo $\mathfrak{p}$ is integral over $R/\mathfrak{m}$. If $x \in R$, then there is nothing to prove. Assume that $x \notin R$. Let $f(X)$ be an irreducible monic polynomial over R which is irreducible modulo $\mathfrak{m}$ and such that $f(x) \in \mathfrak{p}$. Considering a suitable, finite integral extension of R, we may assume furthermore that $f(x)$ is of degree 1, hence that $x \in \mathfrak{p}$. Let F be the set of pairs (a, b) of elements of R such that $ax = b$. Then the set of $aX - b$ generates a prime ideal $\mathfrak{q}$ of the polynomial ring $R[X]$ such that $R[X]/\mathfrak{q}$ is naturally isomorphic to $R[x]$ by (11.13). Then the set $\mathfrak{b}$ of the b has no imbedded prime divisor by (11.13), and by its proof, and A/xA is isomorphic to $R/\mathfrak{b}$, which implies that xA, hence $xA_{\mathfrak{p}}$, both have no imbedded prime divisors. If $\mathfrak{p}'$ is a prime divisor of $xA_{\mathfrak{p}}$, then $\mathfrak{p}' \cap R$ is a prime divisor of $\mathfrak{b}$, hence we see that $R_{(\mathfrak{p}' \cap R)}$ is a valuation ring and x is in the valuation ring. Thus we see that $A_{\mathfrak{p}}$ is analytically unramified by virtue of (36.3), whence the derived normal ring of $A_{\mathfrak{p}}$ is a finite $A_{\mathfrak{p}}$-module by (32.2), which completes the proof of (36.5).

(36.6) COROLLARY. *If A is an affine ring over a pseudo-geometric integral domain, then the derived normal ring of A is a finite A-module.*

(36.7) *A semi-local ring R is analytically unramified if and only if $R_{\mathfrak{m}}$ is analytically unramified for every maximal ideal $\mathfrak{m}$ of R.*

The proof is immediate by (17.7).

(36.8) THEOREM. *Let $x_1, \ldots, x_n$ be algebraically independent elements over a semi-local ring R. Assume that R is analytically unramified. If a semi-local ring R' is a ring of quotients of the polynomial ring $R[x] = R[x_1, \ldots, x_n]$, then R' is analytically unramified. In particular, if $\mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}}$ is analytically unramified.*

Proof. By virtue of (36.7), we may assume that R' is a local ring. Let $\mathfrak{q}$ be the prime ideal of $R[x]$ such that $R[x]_{\mathfrak{q}} = R'$ and set $\mathfrak{p} = \mathfrak{q} \cap R$. Let R^* be the completion of R and let $\mathfrak{p}^*$ be a minimal prime divisor of $\mathfrak{p}R^*$. Then the theorem of transition holds for $R_{\mathfrak{p}}$ and $R^*_{\mathfrak{p}^*}$ and $R_{\mathfrak{p}}$ is a subspace of $R^*_{\mathfrak{p}^*}$. Since R^* is a pseudo-geometric ring by (32.1), we see that $R^*_{\mathfrak{p}^*}$ is a pseudo-geometric ring by (36.1), which implies that the completion of $R^*_{\mathfrak{p}^*}$ has no nilpotent elements except zero, whence the same is true for its subspace $R_{\mathfrak{p}}$. Thus $R_{\mathfrak{p}}$ is analytically unramified and we may assume that R is a local ring with maximal ideal $\mathfrak{p}$. Since $R^*[x]/\mathfrak{p}^nR^*[x]$ is isomorphic to $R[x]/\mathfrak{p}^nR[x]$, $\mathfrak{q}R^*[x]$ is a prime ideal of $R^*[x]$ (because $R^*[x]/\mathfrak{q}R^*[x] = (R^*[x]/\mathfrak{p}R^*[x])/(\mathfrak{q}R^*[x]/\mathfrak{p}R^*[x])$), and furthermore the theorem of transition holds for the local rings R' and $R^*[x]_{\mathfrak{q}R^*[x]}$ by virtue of (18.8) and (19.1), whence R' is a subspace of $R^*[x]_{\mathfrak{q}R^*[x]}$. Therefore we may assume that $R = R^*$, whence R' is pseudo-geometric by (32.1) and (36.5), and the assertion is proved by (36.4).

We add, here, a result on the normality of pseudo-geometric semi-local integral domains. We first prove it in a more general case:

(36.9) THEOREM. *Let R be a Noetherian integral domain and assume that a ($\neq 0$) is an element of the Jacobson radical of R. Assume furthermore that*: (1) *aR has only one minimal prime divisor $\mathfrak{p}$*, (2) *$aR_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$, and* (3) *$R/\mathfrak{p}$ is a normal ring. Let R' be the derived normal ring of R. If R' is a finite R-module and if every (minimal) prime divisor $\mathfrak{p}'$ of aR' lies over $\mathfrak{p}$, then R itself is normal and $\mathfrak{p} = aR$.*

Proof. $R'/\mathfrak{p}'$ is integral over $R/\mathfrak{p}$. Since $R_{\mathfrak{p}}$ is a valuation ring by our assumption (2) and by (12.1), we see that R' is contained in $R_{\mathfrak{p}}$. Therefore $R'/\mathfrak{p}' \subseteq R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, which implies that $R'/\mathfrak{p}'$ and $R/\mathfrak{p}$ have a common field of quotients. Therefore that $R/\mathfrak{p}$ is normal implies that $R'/\mathfrak{p}' = R/\mathfrak{p}$. On the other hand, $R' \subseteq R_{\mathfrak{p}}$ implies that $\mathfrak{p}' = R' \cap \mathfrak{p}R_{\mathfrak{p}}$, whence $\mathfrak{p}'$ is unique, and that $R'_{\mathfrak{p}'} = R_{\mathfrak{p}}$, whence $aR'_{\mathfrak{p}'} =$

$\mathfrak{p}'R'_{\mathfrak{p}'}$. It follows that $aR' \quad \mathfrak{p}'$. Therefore $R'/aR' \quad R/\mathfrak{p}$, which implies that $R' \quad aR' + R$. Since R' is a finite R-module and since a is in the Jacobson radical of R, we see that $R = R'$ by the lemma of Krull-Azumaya, whence $aR' = \mathfrak{p}'$ implies that $aR = \mathfrak{p}$. Thus the proof is complete.

Now we apply the above result to the case of pseudo-geometric integral domains.

(36.10) THEOREM. *Assume that a pseudo-geometric integral domain R is a homomorphic image of a locally Macaulay ring, and that $a_1, \ldots, \ldots, a_r$ are elements of R such that* height $(\sum a_iR) = r$ *and such that they are in the Jacobson radical of R. If $\sum a_iR$ has only one minimal prime divisor $\mathfrak{p}$, if the a_i form a regular system of parameters of $R_\mathfrak{p}$ and if $R/\mathfrak{p}$ is a normal ring, then R is normal and $\mathfrak{p} = \sum a_iR$, and furthermore every $R/\sum_1^j a_iR$ is a normal ring.* (LEMMA OF HIRONAKA)

Proof. We prove the assertion by induction on r. If $r = 1$, then (36.9) and (34.9) imply the validity of the assertion, and we assume that $r > 1$. Let $\mathfrak{q}$ be a minimal prime divisor of a_rR. If $\mathfrak{r}$ is a minimal prime divisor of $\mathfrak{q} + \sum a_iR$, then height $\mathfrak{r}/\mathfrak{q} \leq r - 1$, whence, by the validity of the chain condition for prime ideals, height $\mathfrak{r} \leq r$, and $\mathfrak{p} = \mathfrak{r}$. Therefore $\mathfrak{q} \subseteq \mathfrak{p}$. Since the a_i form a regular system of parameters of $R_\mathfrak{p}$ we see that $\mathfrak{q}$ is unique and that $a_rR_\mathfrak{q} = \mathfrak{q}R_\mathfrak{q}$. Consider $R'' = R/\mathfrak{q}$. Then, applying the induction to R'' with elements a_i modulo $\mathfrak{q}$, we see that $\mathfrak{p}/\mathfrak{q} = (\mathfrak{q} + \sum a_iR)/\mathfrak{q}$ and that $R/(\mathfrak{q} + \sum_1^j a_iR)$ is normal for each $j = 0, 1, \ldots, r - 1$. In particular, $R/\mathfrak{q}$ is normal. This, the uniqueness of $\mathfrak{q}$ and the equality $a_rR_\mathfrak{q} = \mathfrak{q}R_\mathfrak{q}$ imply that R is normal and that $\mathfrak{q} = a_rR$ by the case where $r = 1$. Therefore the proof is complete.

EXERCISE. Prove that a pseudo-geometric semi-local integral domain R is unmixed if and only if R satisfies the second chain condition for prime ideals. Generalize (36.10) to the case where R is a pseudo-geometric unmixed local integral domain.

37. *Analytical normality*

We say that a semi-local integral domain R is *analytically irreducible* if the completion of R is an integral domain. R is called *analytically normal* if the completion of R is a normal ring; in this case, R itself must be a normal ring by (18.4).

We say that a prime ideal $\mathfrak{p}$ of a semi-local ring R is *analytically irreducible* if $R/\mathfrak{p}$ is analytically irreducible.

(37.1) *Let R be a ring and assume that t, $u \in R$ are such that (1) t is not a zero-divisor in R and (2) $tR:uR = tR$. If v is an element of the total quotient ring of R such that tv and uv are in R, then v is in R.*

Proof. Since $tuv \in tR$, we have $uv \in tR:uR = tR$, whence there is an element v' of R such that $tv = tv'$. Since t is not a zero divisor, we have $v = v' \in R$.

(37.2) *Let R be a normal semi-local ring and let R^* be its completion. Assume that t is an element of R which is neither zero nor unit in R such that every prime divisor of tR is analytically unramified. If v is an element of the total quotient ring of R^* such that v is integral over R^* and such that $tv \in R^*$, then v is in R^*.*

Proof. Let the prime divisor of tR be $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. They are of height 1 by (12.9). Let S be the intersection of the complements of $\mathfrak{p}_i$ in R. Then R_S is a semi-local Dedekind domain with maximal ideals $\mathfrak{p}_i R_S$, whence $\mathfrak{p}_i R_S$ is a principal ideal for every i by (28.9). Let x_i be an element of $\mathfrak{p}_i$ such that $\mathfrak{p}_i R_S = x_i R_S$ for each i, and let e_i be natural numbers such that $tR_S = x_1^{e_1} \cdots x_r^{e_r} R_S$. Since $tR^*:sR^* = tR^*$ for any s of S by (18.1), it is sufficient by virtue of (37.1) to show that there is an s of S such that $tvs \in x_1^{e_1} \cdots x_r^{e_r} R^*$ (observing that $x_1^{e_1} \cdots x_r^{e_r} \subset tR$). Let $\mathfrak{p}^*_{ij}$ $(j = 1, \ldots, n(i))$ be all the prime divisors of $\mathfrak{p}_i R^*$ and let w_{ij} be the valuation of the field of quotients of $R^*_{\mathfrak{p}^*_{ij}}$ with $R^*_{\mathfrak{p}^*_{ij}}$ as valuation ring and such that $w_{ij}(x_i) = 1$. Let ϕ_{ij} be the natural homomorphism from R^* into $R^*_{\mathfrak{p}^*_{ij}}$. Let $f_1, \ldots, f_r$ be non-negative integers satisfying the following condition: tvs is in $x_1^{f_1} \cdots x_r^{f_r} R^*$ for some s of S but for any s of S and for any i, tvs is not in $x_1^{f_1} \cdots x_r^{f_r} \cdot x_i R^*$. Then it is sufficient to show that $f_i \geq e_i$. Assume the contrary, for instance that $f_1 < e_1$. We take an element s of S such that tvs is in $x_1^{f_1} \cdots x_r^{f_r} R^*$ and let z be an element of R^* such that $tvs = x_1^{f_1} \cdots x_i^{f_i - 1} z$. We may regard ϕ_{ij} as a homomorphism from the total quotient ring R^{**} of R^* into the field of quotients of $R^*_{\mathfrak{p}^*_{ij}}$. Then, since v is integral over R^*, $\phi_{ij}(v)$ is in $R^*_{\mathfrak{p}^*_{ij}}$, whence $w_{ij}(\phi_{ij}(v)) \geq 0$. Since $w_{1j}(\phi_{1j}(t)) = e_1 > f_1 = w_{1j}(\phi_{1j}(x_1^{f_1} \cdots x_r^{f_r}))$, we have $w_{1j}(\phi_{1j}(z)) \geq 1$. This shows that $\phi_{1j}(z)$ is in $\phi_{1j}(\mathfrak{p}^*_{1j})$. Since the kernel of ϕ_{1j} is contained in $\mathfrak{p}^*_{1j}$, it follows that z is in $\mathfrak{p}^*_{1j}$. Since $x_1 R^*_S = \bigcap_j \mathfrak{p}^*_{1j} R^*_S$, z is in $x_1 R^*_S$ and therefore there is an element s' of S such that $zs' \in x_1 R^*$. Thus, with $s'' = ss'$ which is in S, $tvs'' \in x_1 \cdot x_1^{f_1} \cdots x_r^{f_r} R^*$, which is a contradiction and we have $e_i \leq f_i$ for every i. Thus the proof is complete.

(37.3) *Assume that a normal local ring R is analytically normal. Let*

L be a finite separable extension of the field of quotients K of R and let I be the integral closure of R in L. Assume that every prime ideal $\mathfrak{p}$ of height 1 in I is analytically unramified. Then the completion I^* of I is integrally closed, that is, for every maximal ideal $\mathfrak{M}$ of I, $I_{\mathfrak{M}}$ is analytically normal.

Proof. Let a be an element of I such that $L = K(a)$ and let d be the discriminant of the irreducible monic polynomial over R which has a as a root. Let R^* be the completion of R and let I^{**} be the integral closure of I^* in its total quotient ring. Since I is a finite R-module by (10.16), the integral closure of $R^*[a]$ in its total quotient ring coincides with I^{**} by (17.8). Therefore we see that $dI^{**} \subseteq R^*[a]$ by (10.15), which implies that $I^{**} = I^*$ by (37.2), and therefore I^* is integrally closed. If b is a nilpotent element of I^* and if x is not a zero divisor, then b/x is integral over I^* and is in I^{**}, and $b \in xI^{**} = xI^*$, which implies that $b \in \mathfrak{m}^n I^*$ with Jacobson radical $\mathfrak{m}$ of R and with an arbitrary natural number n. Therefore we have $b = 0$ by (4.2), which proves that I^* has no nilpotent elements except zero, i.e., the zero ideal of I^* is the intersection of a finite number of prime ideals, say $\mathfrak{p}_1^*, \ldots, \mathfrak{p}_r^*$. The idempotents of the total quotient ring of I^* are integral over I^*, and therefore they are in I^*, and we see that I^* is the direct sum of $I^*/\mathfrak{p}_i^*$. Since I^* is integrally closed, each $I^*/\mathfrak{p}_i^*$ must be normal, and the proof is complete.

(37.4) THEOREM. *Assume that a normal local ring $(R, \mathfrak{m})$ is analytically irreducible. Let K be the field of quotients of R. Assume that a local ring $(R', \mathfrak{m}')$ satisfies the following three conditions*: (1) $R \leq R' \subseteq K$, (2) *$R'/\mathfrak{m}R'$ is a finite $R/\mathfrak{m}$-module, and* (3) altitude R' = altitude R. *Then R' coincides with R.*

Proof. Let R^* and R'^* be the completions of R and R', respectively. Since $\mathfrak{m}' \cap R = \mathfrak{m}$, we see that $\mathfrak{m}^i \subseteq \mathfrak{m}'^i \cap R$ for every i. Therefore there exists a natural homomorphism ϕ from R^* into R'^* and $\phi(R^*)$ becomes the closure of R in R'^*. By assumption (2), we see that R'^* is a finite $\phi(R^*)$-module by (30.6), whence altitude R'^* = altitude $\phi(R^*)$ by (10.10). Since altitude R'^* = altitude R' = altitude R = altitude R^* by (17.12), we have altitude R^* = altitude $\phi(R^*)$. Since R^* is an integral domain, it follows that ϕ is an isomorphism. Thus we see that R is a subspace of R' and R'^* is integral over R^*. Let a/b $(a, b \in R)$ be an arbitrary element of R'. Since a/b is integral over R^*, there are elements $c_1^*, \ldots, c_n^*$ of R^* such that $(a/b)^n + c_1^*(a/b)^{n-1} + \cdots + c_n^* = 0$ and therefore $a^n + ba^{n-1}c_1^* + \cdots +$

$b''c_n^* = 0$, which shows that a'' is in the ideal of R^+ generated by $ba''^{-1}, \ldots, b''$. Since $(\sum_1^n b'a''^{-1}R^+) \cap R = \sum_1^n b'a''^{-1}R$ by (17.9), we see that there are elements $c_1, \ldots, c_n$ of R such that $a'' + ba''^{-1}c_1 + \cdots + b''c_n = 0$, whence $(a/b)'' + c_1(a/b)''^{-1} + \cdots + c_n = 0$ and a/b is integral over R. Since R is normal, a/b is in R, which proves the assertion.

Now we prove a theorem on localities over fields or Dedekind domains which satisfies the finiteness condition for integral extensions. Note that a Dedekind domain I is pseudo-geometric ring if and only if it satisfies the finiteness condition for integral extensions. A part of the following theorem (analytical unramifiedness and the finiteness of the derived normal rings) follows from (36.4) and (36.5). But we shall give a direct proof of this part in our special case:

(37.5) THEOREM. *If I is either a field or a pseudo-geometric Dedekind domain and if R is a locality over I, then the derived normal ring R' of R is a finite module, and R is analytically unramified. If furthermore R is normal, then R is analytically normal.*

Proof. Let r be the altitude of R. We prove the assertion by induction on r. If $r = 0$, then the assertion is obvious, and we assume that $r > 0$. Our induction assumption means by virtue of (36.6) that if S is a semi-local ring of altitude $\leq r - 1$ such that, for any maximal ideal $\mathfrak{m}$ of S, $S_{\mathfrak{m}}$ is a locality over I, then S is analytically unramified. Let $\mathfrak{m}$ be the maximal ideal of R and set $\mathfrak{p} = I \cap \mathfrak{m}$. Then $I_{\mathfrak{p}}$ is either a field or a Noetherian valuation ring and is pseudo-geometric. Therefore, we may assume that $I = I_{\mathfrak{p}}$. Let $x_1, \ldots, x_n$ be elements of R such that their residue classes modulo $\mathfrak{m}$ form a transcendence base of $R/\mathfrak{m}$ over $I/\mathfrak{p}$. Since I is a field or a valuation ring, we see that the x_i are algebraically independent over I. Set $B = I(x_1, \ldots, x_n)$. Then B is either a field or a Noetherian valuation ring and satisfies the finiteness condition for integral extensions by (35.2), whence we may assume that $I = B$, i.e., that $R/\mathfrak{m}$ is algebraic over $I/\mathfrak{p}$. Let $y_1, \ldots, y_r$ be a system of parameters of R, where if I is not a field, we choose y_1 to be a prime element of I. There is a chain of prime ideals $0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_r = \mathfrak{m}$ in R such that $y_i \in \mathfrak{q}_j$ if and only if $i \leq j$, and therefore, in the ring $I[y] = I[y_1, \ldots, y_r]$, we have a chain of prime ideals $0 \subset \mathfrak{q}_1 \cap I[y] \subset \cdots \subset \mathfrak{q}_r \cap I[y]$, whence height $\mathfrak{q}_r \cap I[y] \geq r$, which implies that $y_1, \ldots, y_r$ (or, $y_2, \ldots, y_r$ if I is not a field) are algebraically independent over I and, by virtue of the validity of the altitude formula for $I[y]$, that

R is algebraic over $I[y]$. Let L be the function field of R and let J be the integral closure of $I[y]$ in L. Furthermore, set $R'' = R[J]$. Since J is a finite $I[y]$-module, we see that R'' is a finite R-module.

(a) When L is separable over $I[y]$, let $\mathfrak{m}''$ be an arbitrary maximal ideal of R'' and set $\mathfrak{n} = \mathfrak{m}'' \cap J$. By (37.3) and by our induction assumption, we see that the completion of $J_{\mathfrak{n}}$ is a normal ring. Since the y_i form a system of parameters of $R''_{\mathfrak{m}''}$ and of $J_{\mathfrak{n}}$, we see that $R''_{\mathfrak{m}''} = J_{\mathfrak{n}}$ by (37.4). Therefore R'' is analytically unramified, whence its subspace R (by (16.8)) is analytically unramified. On the other hand, since $R''_{\mathfrak{m}''}$ is normal for arbitrary $\mathfrak{m}''$, we see that R'' is normal by (33.9), whence $R'' = R'$, and the first assertion is proved in this case. If R is normal, then $R = R''$, and $R = J_{\mathfrak{n}}$, which is analytically normal.

(b) Next we consider the case where L is not separable over $I[y]$. Take elements $a_1, \ldots, a_s$ of I and a power q of the characteristic p of I such that $L' = L(a_1^{1/q}, \ldots, a_s^{1/q}, y_1^{1/q}, \ldots, y_r^{1/q})$ is separable over $I[a_1^{1/q}, \ldots, a_s^{1/q}, y_1^{1/q}, \ldots, y_r^{1/q}]$. Let I' be the derived normal ring of $I[a_1^{1/q}, \ldots, a_s^{1/q}]$ and let J' be the integral closure of $I[y]$ in L'. Since L' is separable over $I'[y_1^{1/q}, \ldots, y_r^{1/q}]$, for every maximal ideal $\mathfrak{r}$ of $P = R[J']$, the completion of $P_{\mathfrak{r}}$ is a normal ring and $P_{\mathfrak{r}} = J'_{(\mathfrak{r}\cap J')}$ by our observation in (a) above. Hence P is normal. P is a finite R-module because J' is a finite $I[y]$-module by (35.2), whence R' is a finite R-module. P is analytically unramified as in (a) above, whence its subspace R is analytically unramified. Thus the first assertion is proved. Assume now that R is normal. Let $b_1, \ldots, b_t$ be elements of J which form a linearly independent basis for L over the field of quotients of $I[y]$; let $c_1, \ldots, c_u$ be element of J' which form a linearly independent basis for L' over L. Since J' is a finite $I[y]$-module, there is an element d ($\neq 0$) of $I[y]$ such that $dJ' \subseteq \sum I[y]b_ic_j$. Let P^*, R^* and S^* be the completions of P, R and $I[y]_{(\mathfrak{m}\cap I[y])}$, respectively, and let T be the integral closure of R^* in its total quotient ring. By the choice of d, we have $dP^* \subseteq \sum S^*b_ic_j$. Since P^* is integrally closed, we see that T is contained in P^*, whence $dT \subseteq \sum S^*b_ic_j$. Since the c_j are linearly independent over $S^*[b_1, \ldots, b_t]$ by (18.1), we see that $dT \subseteq S^*[b_1, \ldots, b_t]$, and $dT \subseteq R^*$. Therefore $T = R^*$ by (37.2), and therefore we see that R^* is a normal ring because R^* is a local ring (cf. the last step of the proof of (37.3)). Thus the proof is complete.

(37.6) COROLLARY. *If R is a locality over a field or over a pseudo-geometric Dedekind domain, then the number of prime divisors of zero*

in the completion R^* of R is equal to the number of maximal ideals in the derived normal ring R' of R.

Proof. The completion of R' is $R^*[R']$, which has the same total quotient ring with R^*, whence the number of prime divisors of zero in R^* coincides with that in $R^*[R']$. Since $R^*[R']$ is the direct sum of normal local rings, we prove the assertion.

The following is another corollary to (37.5), and is really contained in the proof of (37.5).

(37.7) *If R is a normal locality over a ring I which is either a field or a pseudo-geometric Dedekind domain, then there are a finite number of algebraically independent elements $x_1, \ldots, x_m, y_1, \ldots, y_n$ over I such that R is of finite type over $I(x_1, \ldots, x_m)[y_1, \ldots, y_n]_{\mathfrak{p}}$ with prime ideal $\mathfrak{p}$ generated by a prime ideal of I and the y_i.*

We want to add here an application of (37.3) to pseudo-geometric rings.

(37.8) THEOREM. *If a normal pseudo-geometric local ring R is of finite type over an analytically normal ring S, then R is analytically irreducible. If furthermore R is separable over S, then R is analytically normal.*

Proof. The separable case follows immediately from (37.3) and (36.4). Let R' be, in the general case, the separable algebraic closure of S in R. Then R' is analytically normal, whence it is analytically irreducible. Since R is purely inseparable over R', it follows that the completion R^* of R has only one minimal prime divisor of zero. Since R is analytically unramified by (36.4), it follows that R is analytically irreducible.

(37.9) COROLLARY. *Assume that a pseudo-geometric semi-local integral domain R is of finite type over an analytically normal ring, and let R' be the derived normal ring of R. Let r be the number of maximal ideals of R'. Then the zero ideal of the completion of R is the intersection of r prime ideals.*

We note that

(37.10) *Let I be a complete local integral domain and let $x_1, \ldots, x_n$ be algebraically independent elements over I. If a local integral domain R is of finite type over $I[x_1, \ldots, x_n]$, then R satisfies the conditions in* (37.9).

Proof. I is a finite integral extension of a complete regular local ring by (31.6), whence we may assume that I is regular. Since every

local ring which is a ring of quotients of $k[x_1, \ldots, x_n]$ is then regular by (14.8) and (28.3), we prove the assertion by (36.5).

EXERCISE. Let R be a normal pseudo geometric local ring and let R' be a finite integral extension of R. Assume that, for every maximal ideal $\mathfrak{m}'$ of R', the local ring $R'_{\mathfrak{m}'}$ is analytically normal. Prove that R is analytically normal.

38. Some types of ring extensions

Let $(R, \mathfrak{m})$ be a local integral domain and let $(V, \mathfrak{v})$ be a valuation ring such that $R \leq V$. Let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a} \neq R$ and let $a_1, \ldots, a_r$ be a basis for $\mathfrak{a}$. Then there is an a_i, say a_1 such that $\mathfrak{a}V = a_1V$. Set $b_i = a_i/a_1$, $B = R[b_1, \ldots, b_r]$ and $\mathfrak{p} = \mathfrak{v} \cap B$. Then as will be shown below, the ring $B_{\mathfrak{p}}$ is uniquely determined by R, $\mathfrak{a}$, and V, and this $B_{\mathfrak{p}}$ is called the *dilatation* of R by the ideal $\mathfrak{a}$ with respect to V. When $\mathfrak{a} = \mathfrak{m}$, we call $B_{\mathfrak{p}}$ the *quadratic dilatation* of R with respect to V.

The proof of the uniqueness: Let $a'_1, \ldots, a'_{r'}$ be another basis for $\mathfrak{a}$. We assume first that $a_i = a'_i$ for $i = 1, \ldots, r$. Let a'_j be such that $a'_jV = \mathfrak{a}V$ and set $b'_i = a'_i/a'_1$, $B' = R[b'_1, \ldots, b'_{r'}]$, $\mathfrak{p}' = \mathfrak{v} \cap B'$, $c_i = a'_i/a'_j$, $C = R[c_1, \ldots, c_{r'}]$, $\mathfrak{q} = \mathfrak{v} \cap C$. Since $a'_1V = a'_jV$, we see that c_1 is not in $\mathfrak{q}$, whence c_1 is a unit in $C_{\mathfrak{q}}$, which implies that $C_{\mathfrak{q}}$ contains B', and $B'_{\mathfrak{p}'} \leq C_{\mathfrak{q}}$. Similarly, since b'_j is not in $\mathfrak{p}'$, we see that $C_{\mathfrak{q}} \leq B'_{\mathfrak{q}'}$. Thus $C_{\mathfrak{q}} = B'_{\mathfrak{p}'}$. On the other hand, since the $a'_{i'}$ are linear combinations of the a_i with coefficients in R, we see that $B' \subseteq B$, and $B = B'$, whence $B_{\mathfrak{p}} = B'_{\mathfrak{p}'}$. Thus we have proved the uniqueness in this case. The general case can be proved easily, considering the basis $a_1, \ldots, a_r, a'_1, \ldots, a'_{r'}$.

The main interest of dilatations lies in geometric applications, which should be stated with regard to varieties or something similar. Therefore, we shall deal only with very special results concerning quadratic dilatations which are of ring-theoretic interest.

Let $(R, \mathfrak{m})$ be a regular local ring and let $\mathfrak{p}$ be a prime ideal of R such that $\mathfrak{p} \neq \mathfrak{m}$ and let V be a valuation ring which dominates R and has a prime ideal $\mathfrak{q}$ such that $V_{\mathfrak{q}}$ dominates $R_{\mathfrak{p}}$; the existence of V follows from (11.9). Starting with $R_0 = R$, let R_{i+1} be, if R_i is already defined, the quadratic dilatation of R_i with respect to V. Then we have the following:

(38.1) THEOREM. *Each R_i is a regular local ring, $\mathfrak{q} \cap R_i$ is not maximal and $R_{\mathfrak{p}} = (R_i)_{(\mathfrak{q} \cap R_i)}$. If furthermore* depth $\mathfrak{p} = 1$ *and if the de-*

rived normal ring of $R/\mathfrak{p}$ is a finite $R/\mathfrak{p}$ module, then there is one i such that $\mathfrak{q} \cap R_i$ is generated by a subset of a regular system of parameters of R_i, or equivalently, $R_i/(\mathfrak{q} \cap R_i)$ is a Noetherian valuation ring.

Proof. We prove the first assertion by induction on i. The assertion is obvious for $i = 0$, and we assume that $i > 0$. Let $x_1, \ldots, x_r$ be a regular system of parameters of R_{i-1}, where we may assume that $x_j \in x_1 V$ for every j. Then R_i is a ring of quotients of $R_{i-1}[x_2/x_1, \ldots, \ldots, x_r/x_1]$. Since $\mathfrak{q} \cap R_{i-1}$ is not the maximal ideal, $x_1 \notin \mathfrak{q} \cap R_{i-1}$, which proves that $(R_{i-1})_{(\mathfrak{q} \cap R_{i-1})} = R_{\mathfrak{p}}$ contains x_1 as a unit. Therefore $(R_i)_{(\mathfrak{q} \cap R_i)}$ is a ring of quotients of $R_{i-1}[1/x_1]$, and coincides with $R_{\mathfrak{p}}$. x_1 is a non-unit in R_i, which implies that $\mathfrak{q} \cap R_i$ is not maximal. Applying this to the case where height $\mathfrak{p} = r - 1$, we see that altitude R_i = altitude R_{i-1} $(= r)$ in the special case. This fact implies in the general case that $x_2/x_1, \ldots, x_r/x_1$ modulo $x_1 R_{i-1}[x_2/x_1, \ldots, \ldots, x_r/x_1]$ are algebraically independent over $R_{i-1}/(\sum x_j R_{i-1})$, whence $R_i/x_1 R_i$ is a regular local ring by (14.8), and therefore we see that R_i is a regular local ring. Now we shall prove the last assertion. Let R' be the derived normal ring of $R/\mathfrak{p}$ and let a be an arbitrary element of R'. Let L' be the field of quotients of $R/\mathfrak{p}$ and set $V' = (V/\mathfrak{q}) \cap L'$. Since depth $\mathfrak{p} = 1$, R' is a Dedekind domain by the theorem of Krull-Akizuki, whence V' is a ring of quotients of R'. Let v' be a valuation of L' whose valuation ring is V'. We want to show that there is an i such that $R_i/(\mathfrak{q} \cap R_i)$ contains a. Let a be b_{i-1}/c_{i-1} with $b_{i-1}, c_{i-1} \in R_{i-1}$. If s and t are the degree of b_{i-1} and c_{i-1} with respect to the maximal ideal $\sum x_j R_{i-1}/(\mathfrak{q} \cap R_{i-1})$, then b_{i-1} and c_{i-1} are divisible by x_1^u modulo $(\mathfrak{q} \cap R_i)$ in $R_i/(\mathfrak{q} \cap R_i)$ with $u = \min(s, t)$. Therefore, if $a \notin R_{i-1}$, then $a = b_i/c_i$ with $b_i, c_i \in R_i$ such that $v'(c_i) < v'(c_{i-1})$. Since V' is a Noetherian valuation ring, there is an n such that $v(c_n) = 0$, i.e., $a \in R_n$. Since R' is finite over $R/\mathfrak{p}$, it follows now that there is an n such that $R_n/(\mathfrak{q} \cap R_n)$ contains R'. Since V' is a ring of quotients of R', it follows that $R_n/(\mathfrak{q} \cap R_n) = V'$, and the last assertion is proved by virtue of (25.18).

(38.2) COROLLARY. *Every quadratic dilatation of a regular local ring is again a regular local ring.*

Proof. If $x_1, \ldots, x_r$ is a regular system of parameters of a regular local ring R, then $x_2/x_1, \ldots, x_r/x_1$ are algebraically independent over $R/(\sum x_i R)$ by the proof of (38.1), and the assertion is proved similarly.

As an application of (38.1), we prove the following:

(38.3) THEOREM. *Let f ($\neq 0$) be an element of a regular local ring $(R, \mathfrak{m})$ and let $\mathfrak{p}$ be a prime ideal of R. Then the degree d of f with respect to $\mathfrak{m}$ is not less than the degree d' of f with respect to $\mathfrak{p}R_{\mathfrak{p}}$ (in $R_{\mathfrak{p}}$).*

Proof. If we know the validity of the assertion in the case where depth $\mathfrak{p}$ $\neq$ 1, then, considering a maximal chain of prime ideals between $\mathfrak{p}$ and $\mathfrak{m}$, say, $\mathfrak{p}$ $\supset \mathfrak{p}_0 \supset \cdots \supset \mathfrak{p}_i$ $\supset \mathfrak{m}$, and applying the validity to each $R_{\mathfrak{p}_i}$ with prime ideal $\mathfrak{p}_i R_{\mathfrak{p}_i}$, we prove the assertion by virtue of (28.3). Thus we may assume that depth $\mathfrak{p} = 1$. Assume that R' is a regular local ring dominating R such that (1) $\mathfrak{m}R'$ is the maximal ideal, (2) there is a prime ideal $\mathfrak{p}'$ in R' such that $\mathfrak{p} = \mathfrak{p}' \cap R$, and (3) $\mathfrak{m}^n R' \cap R = \mathfrak{m}^n$. Then d is the degree of f with respect to $\mathfrak{m}R'$. Since $\mathfrak{p} \subseteq \mathfrak{p}'$, the degree of f with respect to $\mathfrak{p}'R'_{\mathfrak{p}'}$ is not less than d'. Therefore R and $\mathfrak{p}$ may be replaced by R' and $\mathfrak{p}'$. Hence, in particular, we may assume that R is complete. Let I be a coefficient ring. We treat from now on the case where I is not a field, because the case where I is a field can be treated similarly but in a simpler way. Let p be the characteristic of the residue class field. Then there is a Noetherian valuation ring I^* such that I^*/pI^* is the algebraic closure of I/pI; the existence is proved easily by virtue of Zorn's lemma. Let $x_1, \ldots, x_r$ be a regular system of parameters of R. Then there is a homomorphism ϕ from the formal power series ring in indeterminates $X_1, \ldots, X_r$ over I such that $\phi(X_i) = x_i$. The kernel of ϕ is generated by a Eisenstein polynomial say F by (31.12). Consider $R^* = I^*[[X_1, \ldots, X_r]]/FI^*[[X_1, \ldots, X_r]]$. Since F is an Eisenstein polynomial, we see that R^* is regular. By the construction, we see that R^* satisfies the conditions for R' above and has a prime ideal $\mathfrak{p}'$ as stated there. Thus we may assume that $R/\mathfrak{m}$ is algebraically closed. Let $(V, \mathfrak{n})$ be a valuation ring which dominates R and which has a prime ideal $\mathfrak{q}$ such that $R_{\mathfrak{p}} \leq V_{\mathfrak{q}}$ and such that $V/\mathfrak{n}$ is algebraic over $R/\mathfrak{m}$, hence, $V/\mathfrak{n} = R/\mathfrak{m}$. The proof of the existence of such a V is similar to the proof of (11.9), considering a maximal chain of prime ideals of R which goes through $\mathfrak{p}$. Then there is a regular system of parameters $x_1, \ldots, x_r$ such that $x_i V \subset x_1 V$ for every $i = 2, \ldots, r$. Then, obviously, $x_1, x_2/x_1, \ldots, x_r/x_1$ is a regular system of parameters of the quadratic dilatation R_1 of R with respect to V. Since f is of degree d with respect to $\mathfrak{m}$, f is a homogeneous form in the x_i of degree d with coefficients in R, and not all the coefficients are in $\mathfrak{m}$. Therefore $f_1 = f/x_1^d$ is in R_1 and the degree of f_1 with respect to the maximal ideal of R_1 is not greater than d. Since $x_1 \notin \mathfrak{p}$, the

degree of f_1 with respect to $\mathfrak{p}R_1$, $(\mathfrak{q} \cap R_1)(R_1)_{(\mathfrak{q} \cap R_1)}$, is equal to d'. Therefore R may be replaced by R_1 (and f is replaced by f_1). Since the original R was complete, we have, after a finite number of the above replacements, the case where $\mathfrak{p}$ is generated by a subset of a regular system of parameters of R by (38.1), and the assertion is easily proved in this case. Thus the proof is complete.

Secondly, we consider a special type of inseparable extensions of local integral domains.

(38.4) *Let $(R, \mathfrak{m})$ be a local integral domain and let a be an element of an integral extension of R. Assume that a is not in the field of quotients of R, that the characteristic p of R is different from zero and that $a^p \in R$. Then $R[a]$ is a local ring. Let $\mathfrak{m}'$ be the maximal ideal of $R[a]$. Then either* $\text{length}_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \text{length}_{R[a]/\mathfrak{m}'} \mathfrak{m}'/\mathfrak{m}'^2$, *or* $(\text{length}_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2) + 1 = \text{length}_{R[a]/\mathfrak{m}'} \mathfrak{m}'/\mathfrak{m}'^2$. *The first equality holds if and only if either the irreducible polynomial $X^p - a^p$ over R is irreducible modulo $\mathfrak{m}$ or there exists an element $b \in R$ such that $(a - b)^p \in \mathfrak{m}$, $\notin \mathfrak{m}^2$.*

Proof. Since a is purely inseparable over R, $R[a]$ is a local ring. Let $x_1, \ldots, x_r$ be a minimal basis for $\mathfrak{m}$. If $X^p - a^p$ is irreducible modulo $\mathfrak{m}$, then it is easy to see that $\mathfrak{m}'$ is generated by $\mathfrak{m}$. Furthermore, the x_i form a minimal basis for $\mathfrak{m}'$. For, otherwise, there is a linear combination $y = \sum a_i x_i$ of the x_i such that $\sum a_i R[a] = R[a]$, and such that $y \in \mathfrak{m}'^2 = \mathfrak{m}^2 R[a]$, which is impossible because $1, a, \ldots, a^{p-1}$ are linearly independent over R, and this case is settled. Assume now that $X^p - a^p$ is reducible modulo $\mathfrak{m}$. Then there is an element $b \in R$ such that $a^p - b^p \in \mathfrak{m}$. Therefore, considering $a - b$ instead of a, we may assume that $b = 0$, that is, $a \in \mathfrak{m}'$. Then $\mathfrak{m}' = \mathfrak{m}R[a] + aR[a] = \mathfrak{m} + aR[a]$. Assume that an element $y \in \mathfrak{m}$, which is not in $\mathfrak{m}^2$, is in $\mathfrak{m}'^2$. Then, since $\mathfrak{m}' = \mathfrak{m} + aR[a]$, there is a relation of the form $y = \sum c_{ij} x_i x_j + (\sum d_i x_i)a + (\sum_0^{p-1} e_i a^i)a^2$ ($c_{ij}, d_i, e_j \in R$). Since $1, a, \ldots, a^{p-1}$ are linearly independent over R, we have $y = \sum c_{ij} x_i x_j + e_{p-2} a^p$. This shows that the residue class of y modulo $\mathfrak{m}^2$ is of the form unit $\times$ (a^p modulo $\mathfrak{m}^2$). Therefore $\text{length}_{R[a]/\mathfrak{m}'} \mathfrak{m}'/\mathfrak{m}'^2$ is either r or $r + 1$ according as $a^p \notin \mathfrak{m}^2$ or $a^p \in \mathfrak{m}^2$. Thus the proof is complete.

(38.5) COROLLARY. *With the notation as in* (38.4), *if $R[a]$ is regular, then R is regular, too.*

Lastly, we consider unramified extensions. A quasi-local ring R' dominating another quasi-local ring R is said to be *unramified* over R if the maximal ideal of R' is generated by that of R and if the resi-

due class field of K' is inseparable over that of K: otherwise, K' is called *ramified* over K. A prime ideal $\mathfrak{p}'$ of K' is said to be *unramified* or *ramified* over K, or over $\mathfrak{p}' \cap K$, if $K'_{\mathfrak{p}'}$ is unramified or ramified, respectively, over $K_{(\mathfrak{p}' \cap K)}$.

Using the above terminology, we have the following theorem:

(38.6) THEOREM. *Assume that a quasi-local ring* $(R', \mathfrak{m}')$ *dominates a quasi-local ring* $(R, \mathfrak{m})$ *and that* R' *is of finite type over* R. *Then*

(1) *If* R' *is a ring of quotients of* $R[u]$ *with an element* u *of* R' *and if there is a polynomial* $f(x)$ *over* R *such that* $f(u) = 0$ *and such that, denoting by* $f'(x)$ *the derivative of* $f(x)$, $f'(u)$ *is not in* $\mathfrak{m}'$, *then* R' *is unramified over* R.

(2) *Conversely, assume that* R' *is unramified over* R, *and let* R'' *be a finitely generated subring of* R' *which is integral over* R *and such that* R' *is a ring of quotients of* R''. *Let* $\mathfrak{m}'' = \mathfrak{m}''_1, \ldots, \mathfrak{m}''_s$ *be the maximal ideals of* R'', *where* $\mathfrak{m}''$ *is chosen to be* $R' = R''_{\mathfrak{m}''}$. *Let* u *be an element of* R'' *such that* u *modulo* $\mathfrak{m}''$ *generates* $R'/\mathfrak{m}'$ *over* $R/\mathfrak{m}$ *and such that, denoting by* $f_i(x)$ *a monic polynomial over* R *such that* $f_i(x)$ *modulo* $\mathfrak{m}$ *is the irreducible monic polynomial for* u *modulo* $\mathfrak{m}''_i$ *over* $R/\mathfrak{m}$, $f_1(u)$ *is not in* $\mathfrak{m}''_j$ *for every* $j \neq 1$. *Then* R' *is a ring of quotients of* $R[u]$ *and* u *is a root of a monic polynomial* $f(x)$ *such that* $f - f_1 f_2^{n_2} \cdots f_r^{n_r} \in \mathfrak{m}R[x]$ *for some natural numbers* n_j ; *hence, in particular, if* $f'(x)$ *is the derivative of* f *above, then* $f'(u)$ *is not in* $\mathfrak{m}'$.

Proof. If $R[u]$ is isomorphic to $R[x]/fR[x]$, then (1) is obvious, and the general case of (1) follows from the following obvious remark:

(38.7) *If a quasi-local ring* R' *is unramified over a quasi-local ring* R *and if* $\mathfrak{a}'$ *is an ideal of* R', *then* $R'/\mathfrak{a}'$ *is unramified over* $R/(\mathfrak{a}' \cap R)$.

We shall prove (2). Set $Q = R[u]$, $\mathfrak{n} = \mathfrak{m}'' \cap Q$ and $Q' = Q_{\mathfrak{n}}$. Since $f_1(u)$ is in $\mathfrak{m}''$ but not in any other $\mathfrak{m}''_j$, $\mathfrak{m}''$ is the unique prime ideal of R'' which lies over $\mathfrak{n}$. Therefore $R' = R''_{\mathfrak{m}''}$ is integral over Q'. Since R' is of finite type, it follows that R' is a finite module over Q'. Since R' is unramified over R and since $R \leq Q' \leq R'$, R' is unramified over Q', whence $\mathfrak{m}' = \mathfrak{n}R'$. Furthermore, by our choice of u, $R'/\mathfrak{m}' = Q'/\mathfrak{n}Q'$. Therefore $R' = Q' + \mathfrak{n}R'$, which implies that $R' = Q'$ by the lemma of Krull-Azumaya, whence the first assertion in (2) is proved. Since $Q' = R'$, there are natural numbers n_j such that, with $g(x) = f_1 f_2^{n_2} \cdots f_r^{n_r}$, $g(u) \in \mathfrak{m}R[u]$. Therefore u is a root of a polynomial $f^*(x)$ such that $f^* - g \in \mathfrak{m}R[x]$. In order to show that we can choose such an f^* to be monic, it is sufficient to show that u is a root of a monic polynomial f^{**} of degree at most the degree of g. Set

d = deg g, and consider $M = R + Ru + \cdots + Ru^{d-1}$. Then, since g is monic, $g(u) \in \mathfrak{m}R[u]$ implies that $R[u] = M + \mathfrak{m}R[u]$. Therefore by the lemma of Krull-Azumaya we see that $R[u] = M$, and u is a root of a monic polynomial of degree d, which completes the proof.

The following three assertions are corollaries to (38.6).

(38.8) *Assume that a ring R' is of finite type over a ring R. If a prime ideal $\mathfrak{p}'$ of R' is unramified over R, then every prime ideal $\mathfrak{q}'$ of R' such that $\mathfrak{q}' \subseteq \mathfrak{p}'$ is unramified over R.*

The proof is straightforward.

(38.9) *Let $f(x)$ be a monic polynomial over R such that the discriminant d of $f(x)$ is a unit in R. If u is a root of $f(x)$, then every prime ideal of $R[u]$ is unramified over R. In particular, if furthermore $R_{\mathfrak{p}}$ is a regular local ring for a prime ideal $\mathfrak{p}$, then for every prime ideal $\mathfrak{p}'$ of R' which lies over $\mathfrak{p}$, $R'_{\mathfrak{p}'}$ is a regular local ring.*

The proof is straightforward by virtue of (10.17).

(38.10) THEOREM. *Assume that an integral domain R' is of finite type over a normal ring R. If every maximal ideal $\mathfrak{m}'$ of R' is unramified over R, then R' is a normal ring.*

Proof. With the notation as in (38.6), $R'_{\mathfrak{m}'}$ is a ring of quotients of $R[u]$ such that $f(u) = 0$, $f'(u) \notin \mathfrak{m}'$, whence $R'_{\mathfrak{m}'}$ is a ring of quotients of $R[u, 1/f'(u)]$, which is a normal ring by (10.18). Therefore $R'_{\mathfrak{m}'}$ is a normal ring. Since R' is the intersection of all the $R'_{\mathfrak{m}'}$ by (33.9), we see that R' is a normal ring.

EXERCISE. Let $\mathfrak{p}$ be a prime ideal of a regular local ring R such that $R/\mathfrak{p}$ is regular and let V be a valuation ring which dominates R. Let R' be the dilatation of R by the ideal $\mathfrak{p}$ with respect to V. Prove that R' is a regular local ring.

39. Separably generated extensions

We say that an integral domain R is *separably generated* over its subring I if either R is of characteristic 0 or, denoting by L and K the fields of quotients of R and I respectively, and by p the characteristic by R, the tensor product $L \otimes_K K^{1/p}$ is an integral domain.

In order to prove a characterization and some properties of separably generated extensions, we introduce the notion of derivations of a ring (we need in this section only those of field, but we need the general case later).

A *derivation* D of a ring R is an additive endomorphism of the total quotient ring L of R which satisfies the following condition: (1)

$D(xy) = xDy + yDx$ for $x, y \in L$ and (2) there is an element d of R which is not a zero divisor such that $dD(R) \subseteq R$. If d can be chosen to be 1, then D is called an *integral derivation* of R.

Let D be a derivation of R and let I be a subring of R. If $dI = 0$, then we say that D is a *derivation over* I; *if* $dR = 0$, then D is called the *zero derivation* and is denoted by 0.

We note that:

(39.1) *If D is a derivation of a ring R with total quotient ring L, then $D1 = 0$, $D(x/y) = (yDx - xDy)/y^2$ ($x, y \in L$, y not being a zero divisor).*

Proof. Since $1 = 1^2$, we have $D1 = 2D1$ and $D1 = 0$. Since $x = y(x/y)$, we have $Dx = yD(x/y) + (x/y)Dy$, and $D(x/y) = (yDx - xDy)/y^2$.

The set of derivations of a ring R over its subring I forms an R-module, which is denoted by $\mathfrak{Der}(R/I)$. *Linear dependence* of derivations always means dependence in this module, hence over R.

(39.2) *If I is a subring of a ring R and if R is of finitely generated type over I, then, denoting by L the total quotient ring of R, we have $\mathfrak{Der}(R/I) = \mathfrak{Der}(L/I)$.*

Proof. It is obvious that $\mathfrak{Der}(R/I) \subseteq \mathfrak{Der}(L/I)$ by the definition of derivations. Let D be an arbitrary derivation of L over I and let $c_1, \ldots, c_n$ be elements of R such that R is a ring of quotients of $I[c_1, \ldots, c_n]$. Since $Dc_i \in L$, there is an element d of $I[c_1, \ldots, c_n]$ which is not a zero divisor such that $dDc_i \in I[c_1, \ldots, c_n]$. Since every element a of $I[c_1, \ldots, c_n]$ is a polynomial in the c_i with coefficients in I, we see that $dDa \in I[c_1, \ldots, c_n]$. Let S be a multiplicatively closed set such that $R = I[c_1, \ldots, c_n]_S$. If $b \in R$, then $b = a/s$ with $a \in I[c_1, \ldots, c_n]$, $s \in S$. Then $dDb = d(sDa - aDs)/s^2$ by (39.1). Since dDa and dDs are in $I[c_1, \ldots, c_n]$, we see that $dDb \in R$, whence D is a derivation of R. Thus $\mathfrak{Der}(L/I) = \mathfrak{Der}(R/I)$.

Let R be a ring and let $X_1, \ldots, X_n$ be indeterminates. Then there are derivations D_i ($i = 1, \ldots, n$) of $R[[X_1, \ldots, X_n]]$ such that $D_i(\sum a_{j_1 \cdots j_n} X_1^{j_1} \cdots X_n^{j_n}) = \sum j_i a_{j_1 \cdots j_n} X_1^{j_1} \cdots X_n^{j_n}/X_i$. These D_i are called the *partial derivations* and are denoted by $\partial/\partial X_i$; if f is in the total quotient ring Q of $R[[X_1, \ldots, X_n]]$, then $D_i f$ may be denoted by $\partial f/\partial X_i$. When $f_1, \ldots, f_m$ are elements of Q, then the matrix $(\partial f_i/\partial X_j)$ is called the *Jacobian matrix* of $f_1, \ldots, f_m$ and is denoted by $J(f_1, \ldots, f_m; X_1, \ldots, X_n)$ or by $J(f_1, \ldots, f_m)$. If D is a derivation of R, then there is a uniquely determined derivation D'

of $R[[X_1, \ldots, X_n]]$ such that $D'(\sum a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}) = \sum (Da_{i_1 \cdots i_n}) X_1^{i_1} \cdots X_n^{i_n}$. When f is an element of Q, $D'f$ is denoted by f''.

We note that the partial derivations and the above D' for integral D are integral derivations of the polynomial ring $R[X_1, \ldots, X_n]$. If ϕ is a homomorphism defined on $R[[X_1, \ldots, X_n]]$ and if x_i are such that $x_i = \phi(X_i)$, then, for an $f \in R[[X_1, \ldots, X_n]]$, $\phi(\partial f/\partial X_i)$ may be denoted by $\partial f/\partial x_i$.

From now on in this section we deal only with finitely generated rings and its application to separably generated extensions.

(39.3) *With the same R, X as above, let D be an integral derivation of R and let $\mathfrak{a}$ be an ideal of $R[X] = R[X_1, \ldots, X_n]$ such that $\mathfrak{a} \cap R = 0$. Let x_i be the homomorphic image of X_i modulo $\mathfrak{a}$. Then there exists a derivation D' of $R[x_1, \ldots, x_n]$ such that $Dr = D'r$ for any $r \in R$ and such that $D'x_i = u_i$ with given elements $u_1, \ldots, u_n$ of the total quotient ring L of $R[x_1, \ldots, x_n]$ if and only if the u_i satisfy the relations $f_i^D(x_1, \ldots, x_n) + \sum_j (\partial f_i/\partial x_j) u_j = 0$ with an aribtrary base $\{f_i\}$ of $\mathfrak{a}$. In this case, D' is uniquely determined.*

Proof. Assume that D' exists. Then the uniqueness is obvious. Since $f_i(x_1, \ldots, x_n) = 0$, we see that $0 = D'(f_i(x_1, \ldots, x_n)) = f_i^D(x_1, \ldots, x_n) + \sum_j (\partial f_i/\partial x_j) u_j$. Conversely, assume that $f_i^D(x_1, \ldots, x_n) + \sum_j (\partial f_i/\partial x_j) u_j = 0$. If $f \in \mathfrak{a}$, then $f = \sum f_i g_i$ with $g_i \in R[X]$, whence $f_i^D = \sum f_i^D g_i + \sum f_i g_i^D$, $\partial f/\partial X_j = \sum (\partial f_i/\partial X_j) g_i + \sum f_i (\partial g_i/\partial X_j)$, and therefore $f^D(x_1, \ldots, x_n) + \sum (\partial f/\partial x_j) u_j = 0$. We define a map D^* from $R[X]$ into L as follows: $D^* g = g^D(x_1, \ldots, x_n) + \sum_j (\partial g/\partial x_j) u_j$. What we have proved above is that D^* induces a map D'' from $R[X]/\mathfrak{a}$ into L. Defining $D'(a/b) = (bD''a - aD''b)/b^2$ for $a, b \in R[X]/\mathfrak{a}$ such that b is not a zero divisor, we see easily that this map D' is uniquely determined (independent of the expression of a/b) and that D' is really a derivation of $R[x_1, \ldots, x_n]$. Thus we prove the assertion.

(39.4) COROLLARY. *Assume that a field L is generated by elements $x_1, \ldots, x_n$ over a field K and let $f_1, \ldots, f_s$ be a basis for the kernel of the homomorphism ϕ over K from $K[X_1, \ldots, X_n]$ onto $K[x_1, \ldots, x_n]$ such that $\phi(X_i) = x_i$. If r is the rank of the Jacobian matrix $J(f_1, \ldots, f_s)$, then every maximal linearly independent set of derivations of L over K consists of $n - r$ elements. On the other hand, if L is separably algebraic over K, then every derivation of K can be extended uniquely to a derivation of L.*

A set of elements $x_1, \ldots, x_t$ of a field L is called a *separating transcendence base* of L over its subfield K if the x_i are algebraically independent over K and if L is separably algebraic over $K(x_1, \ldots, \ldots, x_t)$.

A set of elements $x_1, \ldots, x_t$ of an integral domain R is called a *separating transcendence base* of R over its subring I if it is a separating transcendence base of the field of quotients of R over the field of quotients of I.

(39.5) THEOREM. *Let L be a function field over a field K, and let p be the characteristic of K.* (1) *If $t = \text{trans. deg}_K L$, then $\text{length}_L \mathfrak{Der}(L/K) \geq t$ and the equality holds if and only if L has a separating transcendence base over K.* (2) *Assume that $p \neq 0$ and that a is an element of L such that $a^p \in K$, $a \notin K$. Then there is a derivation D of $K(a)$ over K such that $Da = 1$ and $\mathfrak{Der}(K(a)/K) = K(a) \cdot D$.*

Proof. We prove (2) first. The existence of D is obvious by (39.3). Since $J(X^p - a^p) = 0$, we see that length $\mathfrak{Der}(K(a)/K) = 1$ by (39.4), which proves (2). Next we prove a particular case of (1) as follows:

(39.6) *With K and L as above, L is separably algebraic over K if and only if $\mathfrak{Der}(L/K) = 0$.*

Proof. If L is separable over K, then the zero derivation is uniquely extended to a derivation of L by (39.4), which shows that $\mathfrak{Der}(L/K) = 0$. Conversely, assume that $\mathfrak{Der}(L/K) = 0$. Let $x_1, \ldots, x_n$ be elements of L which generate L. We prove that L is separable over K by induction on n. Set $K' = K(x_1)$. Since $\mathfrak{Der}(L/K') \subseteq \mathfrak{Der}(L/K)$, we see that $\mathfrak{Der}(L/K') = 0$, whence L is separable over K' by induction. Therefore (39.4) and $\mathfrak{Der}(L/K) = 0$ imply that $\mathfrak{Der}(K'/K) = 0$. (Thus we have reduced the problem to the case where $n = 1$.) If x_1 is transcendental over K, then there is a derivation $\partial/\partial x_1$ which is not zero, whence x_1 is algebraic over K. If x_1 is not separable over K, then K is of characteristic $p \neq 0$ and $K(x_1^p) \neq K'$, whence $\mathfrak{Der}(K'/K) \supseteq \mathfrak{Der}(K'/K(x_1^p))$, which is not zero by (2) in (39.5), proved above, and there is a contradiction. Thus x_1 is separable, whence L is separable over K. Thus (39.6) is proved.

Now we proceed with the proof of (39.5). Assume first that L has a separating transcendence base $z_1, \ldots, z_t$ over K. Since L is separable over $K(z) = K(z_1, \ldots, z_t)$, the partial derivations $\partial/\partial z_i$ are uniquely extended to derivations D_i of L by (39.4). Assume that $\sum c_i D_i = 0$ $(c_i \in L)$. Then $0 = (\sum c_i D_i) z_j = c_j D_j z_j = c_j$, which

proves that the D_i are linearly independent. Let D be an arbitrary derivation of L over K and set $u_i = Dz_i$. Then $(D - \sum u_i D_i)z_j = 0$ for every j, which implies that $D = \sum u_i D_i$ induces the zero derivation on $K(z)$, whence $D = \sum u_i D_i = 0$ because L is separable over $K(z)$, which proves that $\mathfrak{Der}(L/K)$ is generated by the D_i, whence length $\mathfrak{Der}(L/K) = t$. Now we consider the general case. We use the notation in (39.4). Reordering the f_i and x_j if necessary, we may assume that the determinant $|\partial f_i/\partial x_j|$ for $1 \leq i \leq r, 1 \leq j \leq r$ is not zero. If we consider a similar Jacobian matrix for L over $K(x_{r+1}, \ldots, \ldots, x_n)$ with generating elements $x_1, \ldots, x_r$, then the rank of the new Jacobian matrix is r, which implies that $\mathfrak{Der}(L/K(x_{r+1}, \ldots, \ldots, x_n)) = 0$. Therefore, we see by (39.6) that L is separably algebraic over $K(x_{r+1}, \ldots, x_n)$, whence $t \leq n - r = \text{length } \mathfrak{Der}(L/K)$. If $t = n - r$, then it is obvious that $x_{r+1}, \ldots, x_n$ is a separating transcendence base of L over K. Thus (39.5) is proved completely.

(39.7) *If L is a function field over a field K, if L' is a field containing K, and if L' is purely inseparable over K, then $L \otimes_K L'$ is a local ring of altitude zero.*

Proof. Since L is a ring of finitely generated type over K, $L \otimes L'$ is of finitely generated type over L', which implies that $L \otimes L'$ is Noetherian. Let p be the characteristic of K. If $p = 0$, then the assertion is obvious because $L' = K$ in this case. Therefore we assume that $p \neq 0$. Let $f = \sum a_i \otimes b_i$ ($a_i \in L$, $b_i \in L'$) be a non-unit of $L \otimes L'$. Let q be a power of p such that $b_i^q \in K$ for every i. Then $f^q = \sum a_i^q \otimes b_i^q = \sum a_i^q b_i^q \in L$. Since f is a non-unit, f^q is a non-unit, whence $f^q = 0$. Thus every non-unit of $L \otimes L'$ is nilpotent, from which the assertion follows.

(39.8) *A field L is separably generated over its subfield K if and only if every finitely generated subextension of L over K is a separably generated extension of K.*

Proof. The *if* part is obvious by the definition, while the *only if* part is easy because $\otimes_K L$ is exact (for K is a field).

By virtue of the above lemma, we consider finitely generated extensions:

(39.9) THEOREM. *Assume that L is a function field over its subfield K. Then the following three conditions are equivalent to each other*:

(1) *L is separably generated over K.*

(2) *L has a separating transcendence base over K.*

(3) *If a field L' contains K and if every element of L' which is*

separably algebraic over K is in K, then it holds that $L \otimes_K L'$ is an integral domain.

Proof. We show at first that (1) implies (2). This is obvious if K is of characteristic 0, whence we assume that K is of characteristic $p \neq 0$. Let $x_1, \ldots, x_n$ be elements of L which generate L, and we prove the assertion by induction on n. Let $\mathfrak{p}$ be the kernel of the homomorphism ϕ over K from the polynomial ring $K[X_1, \ldots, X_n]$ onto $K[x_1, \ldots, x_n]$ such that $\phi(X_i) = x_i$, and let $f \neq 0$ be a polynomial in $\mathfrak{p}$ which is of the smallest degree among those in $\mathfrak{p}$ (if $\mathfrak{p} = 0$, then the assertion is obvious and we assume that $\mathfrak{p} \neq 0$). Since $L \otimes K^{1/p}$ is a field, hence is the field of quotients of $K[x_1, \ldots, x_n] \otimes K^{1/p} \cong K^{1/p}[X_1, \ldots, X_n]/\mathfrak{p}K^{1/p}[X_1, \ldots, X_n]$, it follows that $\mathfrak{p}K^{1/p}[X_1, \ldots, X_n]$ is a prime ideal, and f is irreducible over $K^{1/p}$. It follows that there is one i such that $\partial f/\partial X_i \neq 0$. We may assume that $\partial f/\partial X_n \neq 0$. Then we see that x_n is separable over $K(x_1, \ldots, x_{n-1})$. Since $K(x_1, \ldots, x_{n-1})$ is separably generated by (39.8), it has a separating transcendence base, which becomes a separating transcendence base of L over K by the separability of x_n. Thus we have proved that (1) implies (2). Next we prove that (2) implies (3). Assume that (2) is true but (3) is not true. We want to show a contradiction. Let ϕ be a homomorphism over L' of $L \otimes L'$ into a field such that trans. $\deg_{L'} \phi(L \otimes L') =$ trans. $\deg_K L$. Let $x_1, \ldots, x_t$ be a separating transcendence base of L over K and let $y_i = \phi(x_i)$. Then $y_1, \ldots, y_t$ are algebraically independent over L'. Among non-zero elements $\sum a_i \otimes b_i$ ($a_i \in L$, $b_i \in L'$) of $\phi^{-1}(0)$ (which is not zero by our assumption), let $f = \sum a_i^* \otimes b_i^*$ be one which has the smallest number of terms. We may assume that $b_i^* = 1$. Let K^* be the field generated by the b_i^*. Then, by our assumption, K^* is not separably algebraic over K, whence there is a non-zero derivation D of K^* over K by (39.6). Since the y_i are algebraically independent over K^*, D can be extended to a derivation of $K^*(y_1, \ldots, y_t)$ so that $Dy_i = 0$ for every i by virtue of (39.3). Since every element of $\phi(L)$ is separably algebraic over $K(y_1, \ldots, y_t)$, hence over $K^*(y_1, \ldots, y_t)$, it follows that the extended D can be extended uniquely to a derivation of $K^*(\phi(L))$ by (39.4). Since $D(K(y_1, \ldots, y_t)) = 0$ and since $\phi(L)$ is separably algebraic over $K(y_1, \ldots, y_t)$, $D(\phi(L)) = 0$ by (39.4). Thus the extended derivation D is a derivation over $\phi(L)$. Since $\sum \phi(a^*)b^* = 0$, we have $0 = D(\sum \phi(a_i^*)b_i^*) = \sum \phi(a_i^*)(Db_i^*)$, which implies that $\sum a_i^* \otimes$

(Db_i^*) is in $\phi^{-1}(0)$. Since $Db_i^* \quad D1 \quad 0$ and since some Db_i^* is different from 0 (because $D \neq 0$ on K^*), we have a contradiction to the minimality of the number of terms in f. Thus we prove that (2) implies (3). It is obvious that (3) implies (1), therefore the proof is complete.

(39.10) THEOREM. *If L is a function field over a field K. Then there is a finite, purely inseparable extension K' of K such that $L(K')$ is separably generated over K'.*

Proof. Let K^* be the smallest perfect field containing K. Then K^* is purely inseparable over K, whence $L \otimes K^*$ is a local ring of altitude zero by (39.7). Let $n_j = \sum_i f_{ij} \otimes g_{ij}$ $(j = 1, \ldots, n)$ be a basis for the radical of $L \otimes K^*$ and let K' be the field generated by all the g_{ij}. Then we see that $L(K') \otimes_{K'} K^*$ coincides with the residue class field of $L \otimes K^*$, which means that $L(K') \otimes_{K'} K^*$ is a field, which contains $L(K') \otimes_{K'} K'^{1/p}$ because K' is a field, and $L(K')$ is separably generated over K'.

(39.11) THEOREM. *Let A be an affine ring over an integral domain I. If A is separably generated over I, then there is a separating transcendence base $z_1, \ldots, z_t$ of A over I and an element a $(\neq 0)$ of I such that $A[1/a]$ is integral over $I[1/a, z_1, \ldots, z_t]$.* (NORMALIZATION THEOREM FOR SEPARABLY GENERATED AFFINE RINGS).

Proof. Let p be the characteristic of I. If $p = 0$, then the assertion is nothing but a special case of the normalization theorem for finitely generated rings. Therefore we assume that $p \neq 0$. Let $x_1, \ldots, x_t$ be a separating transcendence base of A over I and let $x_{t+1}, \ldots, x_n$ be such that A is generated by $x_1, \ldots, x_n$ over I. Let $X_1, \ldots, X_n$ be indeterminates and let ϕ be the homomorphism over I from $I[X] = I[X_1, \ldots, X_n]$ onto A such that $\phi(X_i) = x_i$. Let $\mathfrak{a}$ be the kernel of ϕ and apply the normalization theorem for polynomial rings and the proof of (14.3). We see that there are elements $Y_1, \ldots, Y_n$ of $I[X]$ and an element a of I such that: (1) $I[X][1/a]$ is integral over $I[1/a][Y_1, \ldots, Y_n]$, (2) $\mathfrak{a}I[X][1/a] \cap I[1/a, Y_1, \ldots, Y_n]$ is generated by $Y_{t+1}, \ldots, Y_n$, and (3) $Y_i = X_i + F_i$ for $i = 1, \ldots, t$ with $F_i \in \pi[X_{i+1}^p, \ldots, X_n^p]$ where π is the prime integral domain. Set $z_i = \phi(Y_i)$ for $i = 1, \ldots, t$. Then (1) implies that $A[1/a]$ is integral over $I[1/a, z_1, \ldots, z_t]$, and (2) shows that the z_i are algebraically independent, as we have done in the proof of (14.4). What we have to prove here is that A is separably algebraic over $I[z_1, \ldots, z_t]$.

Since $x_i \equiv z_i \pmod{\mathfrak{M}}$ by our construction, we see that $Dx_i \equiv Dz_i \pmod{\mathfrak{M}}$ for every i and for every derivation D of A, which implies that $\mathrm{Der}(A/I|x_1, \ldots, x_d) \subseteq \mathrm{Der}(A/I|z_1, \ldots, z_d)$. Since $x_1, \ldots, x_d$ is a separating transcendence base, $\mathrm{Der}(A/I|x_1, \ldots, x_d) = 0$, and $z_1, \ldots, z_d$ form a separating transcendence base by (39.6). Thus the proof is complete.

Exercises. *1.* Let $(R, \mathfrak{m})$ be a normal locality over a ring I which is either a field or a Dedekind domain and assume that R is separably generated over I. Prove that there is a separating transcendence basis $z_1, \ldots, z_d$ of R over I such that $\mathfrak{n} = \mathfrak{m} \cap I[z_1, \ldots, z_d]$ is generated by $\mathfrak{m} \cap I$ and a subset of the z_i and such that R is of finite type over $I[z_1, \ldots, z_d]_{\mathfrak{n}}$.

2. Let K and L be fields of characteristic $p \neq 0$ such that $K \subseteq L$. Prove that L is separably generated over K if and only if a p-base of K is a subset of a suitable p-base of L.

3. Let $(R, \mathfrak{m})$ be a complete local ring which may not be Noetherian and let p be the characteristic of $R/\mathfrak{m}$. Assume that a local ring I is dominated by R, that pI is the maximal ideal of I, and that $R/\mathfrak{m}$ is separably generated over I/pI. Prove that there is a coefficient ring of R which contains I. (Hint: Making use of Exercise 2, above, adapt the proof of the structure theorem of complete local rings.)

40. Multiplicity of a local ring

When $(R, \mathfrak{m})$ is a local ring, the multiplicity $\mu(\mathfrak{m})$ is called the *multiplicity* of R and is denoted by $m(R)$.

(40.1) Theorem. *Let $\mathfrak{p}$ be a prime ideal of a local ring R. If* height $\mathfrak{p}$ + depth $\mathfrak{p}$ = altitude R *and if $\mathfrak{p}$ is analytically unramified, then the multiplicity of $R_{\mathfrak{p}}$ is not greater than that of R.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R. If $R/\mathfrak{m}$ contains only a finite number of elements, then, taking a transcendental element x over R, we consider $R(x)$ and $R_{\mathfrak{p}}(x)$. By the facts that $R_{\mathfrak{p}}(x) = R(x)_{\mathfrak{p}R(x)}$, $\mathfrak{p}R(x)$ is analytically unramified by (36.8), $m(R) = m(R(x))$ and $m(R_{\mathfrak{p}}(x)) = m(R_{\mathfrak{p}})$, we may assume that $R/\mathfrak{m}$ contains infinitely many elements. Let R^* be the completion of R and let $\mathfrak{p}^*$ be a minimal prime divisor of $\mathfrak{p}R^*$. Then the theorem of transition holds for $R_{\mathfrak{p}}$ and $R^*_{\mathfrak{p}^*}$, whence $m(R_{\mathfrak{p}}) = m(R^*_{\mathfrak{p}^*})$ by the analytical unramifiedness of $\mathfrak{p}$. Therefore we may assume that $R = R^*$ (because $m(R) = m(R^*)$). Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be all the prime divisors $\mathfrak{P}$ of zero such that depth $\mathfrak{P}$ = altitude R, where we assume that $\mathfrak{P}_i \subseteq \mathfrak{p}$ if and only if $i \leq s$. Then (23.5) implies that $m(R) = \mu(\mathfrak{m}) = \sum_1^r \mu(\mathfrak{m}/\mathfrak{P}_i) \cdot \text{length } R_{\mathfrak{P}_i}$ and that $m(R_{\mathfrak{p}}) = \sum_1^s \mu(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{P}_iR_{\mathfrak{p}}) \cdot \text{length}$

$R_{\mathfrak{p}_i}$. Therefore, if we know the validity of our assertion in the case where R is an integral domain, then we prove the general case. Thus we may assume, furthermore, that R is an integral domain. Let I be a coefficient ring of R and let $x_1, \ldots, x_t$ be a system of parameters of R such that $m(R) = \mu(\sum x_i R)$; the existence of I follows from (31.1), and that of the x_i follows from (24.1). Set $S = I[[x_1, \ldots, \ldots, x_t]]$, $\mathfrak{n} = \sum x_i S$ and $\mathfrak{q} = \mathfrak{p} \cap S$. We denote by $[R:S]$ the degree of extension of the field of quotients of R over that of S. Then $m(R) \cdot \mu(\mathfrak{n}R) = \mu_S(\mathfrak{n}; R) = [R:S] \cdot \mu(\mathfrak{n})$. Similarly, if we denote by T the complement of $\mathfrak{q}$ in S, then $m(R_{\mathfrak{p}}) \leq \mu(\mathfrak{q}R_{\mathfrak{p}}) \leq \mu(\mathfrak{q}R_T) = \mu_{S_{\mathfrak{q}}}(\mathfrak{q}S_{\mathfrak{q}}; R_T) = [R:S] \cdot \mu(\mathfrak{q}S_{\mathfrak{q}})$. Hence it suffices to show that $\mu(\mathfrak{n}) \geq \mu(\mathfrak{q}S_{\mathfrak{q}})$. Therefore, it suffices to prove the assertion in the case where $R = S$. If R is regular, then $R_{\mathfrak{q}}$ is regular by (28.3), whence $\mu(\mathfrak{q}R_{\mathfrak{q}}) = 1$ and the assertion is true. Therefore we assume that I is not a field. Let $X_1, \ldots, X_t$ be indeterminates and consider $\mathfrak{R} = I[[X_1, \ldots, X_t]]$. Let ϕ be the homomorphism over I from $\mathfrak{R}$ onto R such that $\phi(X_i) = x_i$. The kernel $\mathfrak{k}$ of ϕ is a prime ideal of height 1, whence $\mathfrak{k}$ is principal by (28.7); let $f \in \mathfrak{R}$ be such that $\mathfrak{k} = f\mathfrak{R}$. (40.2) below, implies that $m(R)$ is the degree of f with respect to $\phi^{-1}(\mathfrak{m})$ and that $m(R_{\mathfrak{p}})$ is the degree of f with respect to $\phi^{-1}(\mathfrak{p})\mathfrak{R}_{\phi^{-1}(\mathfrak{p})}$ and therefore $m(R) \geq m(R_{\mathfrak{p}})$ by (38.3), and the assertion is completely proved when (40.2) below, is proved.

(40.2) *Assume that* $(R,\mathfrak{m})$ *is a regular local ring. If* f $(\neq 0)$ *is an element of* $\mathfrak{m}$, *then* $m(R/fR)$ *is equal to the degree of* f *with respect to* $\mathfrak{m}$.

Proof. Let d be the degree of f with respect to $\mathfrak{m}$ and let $x_1, \ldots, \ldots, x_r$ be a regular system of parameters of R. Then there is a homogeneous form $h(X_1, \ldots, X_r)$ of degree d over R such that $h(x) = f$ and $h(X) \notin \mathfrak{m}R[X]$. We may assume, in the same way as in the proof of (40.1), that $R/\mathfrak{m}$ contains infinitely many elements. Then, considering a sufficiently general linear transformation of the x_i, we may assume that $h(X)$ has a term uX_1^d with unit u in R. Then $f, x_2, \ldots, \ldots, x_r$ is a system of parameters of R and length $R/(fR + \sum_2^r x_i R) = d$, whence the multiplicity of the ideal generated by the (x_i modulo fR) is equal to d because R/fR is a Macaulay ring, and $m(R/fR) \leq d$. Let $y_2, \ldots, y_r$ be such that $\mu(fR + \sum y_i R/fR) = m(R/fR)$, whence $m(R/fR) = \text{length } R/(fR + \sum y_i R) = \mu(fR + \sum y_i R)$ which is not less than d by (24.3) because $f \in \mathfrak{m}^d$. Thus we prove that $m(R/fR) = d$.

We shall prove a generalization of a well known result in algebraic

geometry which asserts that the set of singular points on an algebraic variety is a closed set in Zariski topology. In order to formulate an ideal theoretic generalization of the above result, we introduce two conditions on Noetherian rings:

(*) I being a Noetherian integral domain, we consider the condition that: there is an ideal $\mathfrak{a}$ which is different from zero and such that if a prime ideal $\mathfrak{p}$ of I does not contain $\mathfrak{a}$ then $I_{\mathfrak{p}}$ is a regular local ring.

(**) R being a Noetherian ring, we consider the condition that: there are ideals $\mathfrak{s}, \mathfrak{s}_1, \ldots, \mathfrak{s}_n, \ldots$ of R such that, for a prime ideal $\mathfrak{p}$ of R, (1) $R_{\mathfrak{p}}$ is not regular if and only if $\mathfrak{p}$ contains $\mathfrak{s}$ and (2) $R_{\mathfrak{p}}$ is of multiplicity greater than a given natural number n if and only if $\mathfrak{p}$ contains $\mathfrak{s}_n$.

Then our generalization is formulated as follows:

(40.3) THEOREM. *Assume that I is a pseudo-geometric ring such that if $\mathfrak{p}$ is a prime ideal of I and if I' is a finite purely inseparable integral extension of $I/\mathfrak{p}$, then I' satisfies the condition introduced in* (*) *above. Then every ring R which is of finitely generated type over I satisfies the condition introduced in* (**) *above.*

In order to prove the above assertion, we first prove the following lemma.

(40.4) *Let R be a Noetherian ring and let M be the set of prime ideals of R. For a subset N of M, there is an ideal $\mathfrak{a}$ of R such that $\mathfrak{p} \in N$ ($\mathfrak{p} \in M$) is equivalent to $\mathfrak{a} \subseteq \mathfrak{p}$ if and only if N satisfies the following two conditions:* (1) *if $\mathfrak{p} \in N$, then every prime ideal which contains $\mathfrak{p}$ is in N and* (2) *if a prime ideal $\mathfrak{p}$ is not in N, then there is an ideal $\mathfrak{b}$ such that $\mathfrak{b} \nsubseteq \mathfrak{p}$ and such that if $\mathfrak{p} \subseteq \mathfrak{q} \in N$ then $\mathfrak{q}$ contains $\mathfrak{b}$.*

Proof. Assume first the existence of $\mathfrak{a}$. Then the validity of (1) is obvious. As for (2), it is easy to see that $\mathfrak{a}$ satisfies the requirement for $\mathfrak{b}$. Thus we settle the *only if* part. Assume that N satisfies the conditions (1) and (2). Let $\mathfrak{c}$ be the intersection of all the prime ideals in N. It suffices to show that $\mathfrak{c}$ satisfies the requirement for $\mathfrak{a}$, and for that purpose, it is sufficient to show that if $\mathfrak{p} \in M$ is not in N, then $\mathfrak{p}$ does not contain $\mathfrak{c}$. Assume the contrary, and let $\mathfrak{q}$ be a minimal prime divisor of $\mathfrak{c}$ which is contained in $\mathfrak{p}$. Since $\mathfrak{p} \notin N$, and since $\mathfrak{q} \subseteq \mathfrak{p}$, it follows by (1) that $\mathfrak{q} \notin N$. Let the other minimal prime divisors of $\mathfrak{c}$ be $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ and let $\mathfrak{b}$ be an ideal, as in (2), applied to $\mathfrak{q}$. Then it is obvious that all $\mathfrak{r} \in N$ contain $(\mathfrak{b} + \mathfrak{q}) \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ and therefore $\mathfrak{c} \supseteq (\mathfrak{b} + \mathfrak{q}) \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ and $\mathfrak{q}R_{\mathfrak{q}} = \mathfrak{c}R_{\mathfrak{q}} =$

$(\mathfrak{b} \mid \mathfrak{q})R_{\mathfrak{q}} \neq R_{\mathfrak{q}}$, which is a contradiction and the *if* part is proved. Thus we complete the proof.

Next we prove the following auxiliary result:

(40.5) *Assume that R is a pseudo geometric ring such that for every prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ satisfies the condition introduced in* (*) *above. Then R satisfies the condition in* (**) *above.*

Proof. Let $N, N_1, \ldots, N_i, \ldots$ be the sets of prime ideals $\mathfrak{p}$ of R such that: (1) $R_{\mathfrak{p}}$ is not regular if and only if $\mathfrak{p}$ is in N and (2) $m(R_{\mathfrak{p}}) > i$ if and only if $\mathfrak{p}$ is in N_i. It follows from (28.3) and (40.1) that the sets N and N_i satisfy the condition (1) in (40.4), hence it suffices to show that they satisfy the condition (2) in (40.4). Assume that a prime ideal $\mathfrak{p}$ is not in N. Then $R_{\mathfrak{p}}$ is regular. Let $x_1, \ldots, x_r$ be elements of $\mathfrak{p}$ such that their natural images in $R_{\mathfrak{p}}$ form a regular system of parameters of $R_{\mathfrak{p}}$. Then there is an element a of R which is not in $\mathfrak{p}$ such that, with $S = \{a^n \mid n = 1, 2, \ldots\}$, $\sum x_i R_S = \mathfrak{p}R_S$. Let $\mathfrak{a}$ be the ideal of R such that $\mathfrak{p} \subset \mathfrak{a}$ and such that $\mathfrak{a}/\mathfrak{p}$ satsfies the condition for $\mathfrak{a}$ in (*) above applied to $R/\mathfrak{p}$. Set $\mathfrak{b} = a\mathfrak{a}$. If a prime ideal $\mathfrak{q}$ is such that $\mathfrak{q} \supseteq \mathfrak{p}$ and such that $\mathfrak{b} \nsubseteq \mathfrak{q}$, then $R_{\mathfrak{q}}$ is a ring of quotients of R_S and furthermore $R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}$ is regular, which implies that $R_{\mathfrak{q}}$ is regular, by our choice of a and by (9.11). Therefore we see the existence of $\mathfrak{s}$ by (40.4). Assume that a prime ideal $\mathfrak{p}$ is not in N_i. Then $m(R_{\mathfrak{p}}) \leq i$. Let $x_1, \ldots, x_r$ be a system of parameters of $R_{\mathfrak{p}}$ such that $m(R_{\mathfrak{p}}) = \mu(\sum x_i R_{\mathfrak{p}})$ and such that every x_i is in $\mathfrak{p}$. Then there is an element a of R which is not in $\mathfrak{p}$ such that, with $S = \{a^n \mid n = 1, 2, \ldots\}$, $\sum x_i R_S$ is a primary ideal belonging to $\mathfrak{p}R_S$. Set $\mathfrak{b} = a\mathfrak{a}$ with an ideal $\mathfrak{a}$ such that $\mathfrak{p} \subset \mathfrak{a}$ and such that $\mathfrak{a}/\mathfrak{p}$ satisfies the condition for $\mathfrak{a}$ in (*) applied to $R/\mathfrak{p}$. If a prime ideal $\mathfrak{q}$ contains $\mathfrak{p}$ and if $\mathfrak{b} \nsubseteq \mathfrak{q}$, then $R_{\mathfrak{q}}$ is a ring of quotients of R_S and furthermore $R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}$ is regular. Let $x_{r+1}, \ldots, x_s$ be elements of $\mathfrak{q}$ such that their residue classes modulo $\mathfrak{p}$ form a regular system of parameters of $R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}$. Then, it is obvious that the natural images $x_1', \ldots, x_s'$ of $x_1, \ldots, x_s$ in $R_{\mathfrak{q}}$ form a system of parameters of $R_{\mathfrak{q}}$. It follows from the associativity formula (24.7) that $\mu(\sum x_i' R_{\mathfrak{q}}) = \mu(\sum x_i' R_{\mathfrak{q}} \text{ modulo } \mathfrak{p}R_{\mathfrak{q}}) \cdot \mu(\sum_1^r x_i' R_{\mathfrak{p}}) = \mu(\sum_1^r x_i' R_{\mathfrak{p}})$, which is $m(R_{\mathfrak{p}})$ by our choice of the x_i. Therefore $m(R_{\mathfrak{q}}) = \mu(\mathfrak{q}R_{\mathfrak{q}}) \leq \mu(\sum x_i' R_{\mathfrak{q}}) = m(R_{\mathfrak{p}}) \leq i$. Therefore we see the existence of $\mathfrak{s}_i$ by virtue of (40.4), which completes the proof.

Now we want to prove (40.3). Since the validity of the condition stated in (**) for an R is carried over any ring of quotients of R, it suffices to prove the case where R is finitely generated over I. It is

sufficient by virtue of (40.5) to show that if $\mathfrak{p}$ is a prime ideal of R, then $R/\mathfrak{p}$ satisfies the condition stated in (*), hence, assuming that I is an integral domain and that R is an affine ring over I, we have only to show that R satisfies the condition stated in (*). There is a finite purely inseparable integral extension I' of I such that $I'[R]$ is separably generated over I' by (39.10). We prove the assertion by induction on the degree of the extension of the field of quotients K' of I' over the field of quotients K of I. If $[K':K] = 1$, then R is separably generated over I, whence there is a separating transcendence base $z_1, \ldots, z_t$ of R over I and an element a ($\neq 0$) of I such that $R[1/a]$ is integral over $I[1/a, z_1, \ldots, z_t]$. Let c be an element of R which generates the field of quotients L of R over $K(z_1, \ldots, z_t)$. Let $f(x)$ be the irreducible monic polynomial over $K(z_1, \ldots, z_t)$ which has c as a root. Considering elements of type cs ($s \in I[z_1, \ldots, z_t]$) instead of c if necessary, we may assume that $f(x)$ is a polynomial over $I[z_1, \ldots, z_t]$. Let d be the discriminant of $f(x)$. Let $\mathfrak{b}$ be such an ideal as $\mathfrak{a}$ described in (*) applied to I. Then we see that $ad\mathfrak{b}$ satisfies the requirement for $\mathfrak{a}$ in (*) by virtue of (38.9) and (14.8). Assume now that $[K':K] > 1$. Then the characteristic p of K is different from zero. Let c be an element of I' which is not in K and such that $c^p \in I$. If $c \in L$, then $c = y/x$ ($x,y \in R$) and we may replace R with $R[1/x]$; then we have $c \in R$. Then, applying our induction to R over $I[c]$, we prove this case. Thus we assume that $c \notin L$. By induction applied to $R[c]$ over $I[c]$, we see that there is an ideal $\mathfrak{a}$ of $R[c]$ as described in (*) applied to $R[c]$. Let $\mathfrak{a}'$ be the ideal $\mathfrak{a} \cap R$. Noting that $\mathfrak{a}'$ contains every pth power of elements of $\mathfrak{a}$, we see that $\mathfrak{a}'$ satisfies the requirement for $\mathfrak{a}$ in (*) applied to R by virtue of (38.5). Thus the proof of (40.3) is complete.

As is obvious, if $R_{\mathfrak{p}}$ is a regular local ring, then $m(R_{\mathfrak{p}}) = 1$, but not conversely. If we replace $\mathfrak{s}, \mathfrak{s}_1, \ldots, \mathfrak{s}_n, \ldots$ in (40.3) by their radicals, then we see the inclusion $\mathfrak{s} \subseteq \mathfrak{s}_1 \subseteq \cdots \subseteq \mathfrak{s}_n \subseteq \cdots$. Concerning the relationship between $\mathfrak{s}$ and $\mathfrak{s}_1$, we add the following result:

(40.6) THEOREM. *A local ring* $(R, \mathfrak{m})$ *is regular if and only if* R *satisfies the two conditions that* R *is unmixed and that* $m(R) = 1$.

Proof. The *only if* part is obvious, and we prove the converse. Assume that R is unmixed and that $m(R) = 1$. Let R^* be the completion of R. Then R^* is unmixed and $m(R^*) = m(R) = 1$. It follows from (23.5) that $1 = \mu(\mathfrak{m}R^*) = \sum_{\mathfrak{p}^*} \mu(\mathfrak{m}R^*/\mathfrak{p}^*) \cdot \text{length } R^*_{\mathfrak{p}^*}$,

where $\mathfrak{p}^*$ runs over all prime divisors of zero (such that depth $\mathfrak{p}^*$ altitude R^*). Therefore we see that R^* must be an integral domain. Since it suffices to show that R^* is regular (because of the equality $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}R^*/\mathfrak{m}^2R^*$), we may assume that R is complete. If $R/\mathfrak{m}$ contains only a finite number of elements, then take a transcendental element x over R and consider $R(x)$. Since R is a homomorphic image of a Macaulay ring by our assumption, the same is true for $R(x)$, whence $R(x)$ is unmixed by (34.9). Then, since length $\mathfrak{m}/\mathfrak{m}^2$ = length $\mathfrak{m}R(x)/\mathfrak{m}^2R(x)$ by (18.9) (cf. Exercise 2 in §18), we see that R is regular if and only if $R(x)$ is regular. Furthermore, since the theorem of transition holds for R and $R(x)$, we see that $m(R(x)) = 1$. Therefore R may be replaced by $R(x)$, whence, considering the completion of $R(x)$, we may assume that $R/\mathfrak{m}$ contains infinitely many elements. We now prove the assertion by induction on altitude R. If altitude $R = 0$, then R is a field and the regularity is obvious. If altitude $R = 1$, then there is a superficial element a of $\mathfrak{m}$ and $\mu(aR) = \mu(\mathfrak{m}) = 1$ by (24.1), while by (24.2) or by the fact that R is a Macaulay ring in this case, we see that $\mu(aR)$ = length R/aR, whence length $R/aR = 1$ and $\mathfrak{m} = aR$. Therefore R is a regular local ring. Assume that altitude $R = r > 1$. Let a be a superficial element of $\mathfrak{m}$. Then $1 = \mu(\mathfrak{m}) = \mu(\mathfrak{m}/aR)$ by (24.2), which implies that $m(R/aR) = 1$. Since every minimal prime divisor $\mathfrak{p}$ of aR is of height 1 by (9.2) and since the first chain condition is satisfied by every complete local integral domain by (34.4), we see that depth $\mathfrak{p} = r - 1$, whence, applying (23.5) to $\mathfrak{m}/aR$, we see that aR has only one minimal prime divisor $\mathfrak{p}$, that $aR_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ and that $m(R/\mathfrak{p}) = 1$. By induction, we see that $R/\mathfrak{p}$ is regular, whence $R/\mathfrak{p}$ is normal by (25.14). Therefore we see that $aR = \mathfrak{p}$ (and that R is normal) by the lemma of Hironaka (36.10). Therefore R/aR is regular, whence R is regular by (9.11), which completes the proof.

41. Purity of branch loci

The purity of branch loci at a simple point, which is known in algebraic geometry, can be formulated in a very general form as follows:

(41.1) THEOREM. *Let* $(R, \mathfrak{m})$ *be a regular local ring and let* $(P, \mathfrak{n})$ *be a normal local ring which dominates* R *and which is a ring of quotients of a finite separable integral extension of* R. *Assume that every*

prime ideal $\mathfrak{p}$ *of height* 1 *in* P *is unramified over* R. *Then* P *itself is unramified over* R.

In order to prove the theorem, we need some preliminaries. We begin with some results in Galois theory.

Let R be a normal ring and let R' be a separable Galois extension of R with Galois group G. Let $\mathfrak{p}'$ be a prime ideal in R'. Then the set H of σ in G such that $\mathfrak{p}'^{\sigma} = \mathfrak{p}'$ is a subgroup of G. This H is called the *splitting group* of $\mathfrak{p}'$. The set I of σ in G such that $a^{\sigma} - a \in \mathfrak{p}'$ for every $a \in R'$ is a subgroup of H. This I is called the *inertia group* of $\mathfrak{p}'$. The invariant subrings S and T of H and I are called the *splitting* and *inertia rings* of $\mathfrak{p}'$, respectively.

(41.2) THEOREM. *With the above notation, set* $\mathfrak{p} = \mathfrak{p}' \cap R$, $\mathfrak{q} = \mathfrak{p}' \cap S$, $\mathfrak{q}' = \mathfrak{p}' \cap T$. *Then*: (1) $\mathfrak{p}'$ *is the unique prime ideal of* R' *that lies over* $\mathfrak{q}$, (2) $S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, (3) $\mathfrak{q}$ *is unramified over* R, (4) $\mathfrak{q}'$ *is unramified over* R, *and* (5) I *is a normal subgroup of* H. *Furthermore*, (6) H/I *is the Galois group of* $R'_{\mathfrak{p}'}/\mathfrak{p}'R'_{\mathfrak{p}'}$ *and of* $T_{\mathfrak{q}'}/\mathfrak{q}'T_{\mathfrak{q}'}$ *over* $S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

Proof. Considering $R_{\mathfrak{p}}$, $S_{(R-\mathfrak{p})}$, etc., we may assume that $\mathfrak{p}$ is the unique maximal ideal of R. The splitting group of $\mathfrak{p}'$ over S is the Galois group H, which shows that $\mathfrak{p}'$ is the unique prime ideal of R' which lies over $\mathfrak{q}$. In order to prove (2), it suffices to show that if $a \in S$, then there is an element $b \in R$ such that $a - b \in \mathfrak{q}$, hence, considering an almost finite Galois extension containing a, we may assume that G is finite. Let $\mathfrak{a}$ be the intersection of maximal ideals of S other than $\mathfrak{q}$. Then, $\mathfrak{a} + \mathfrak{q} = S$ because of the finiteness of G, whence there is an element a' of $\mathfrak{a}$ such that $a - a' \in \mathfrak{q}$. If $a' \in \mathfrak{q}$, then $a \in \mathfrak{q}$ and b can be 0. Therefore we assume that $a' \notin \mathfrak{q}$. Let $\sigma_1, \ldots, \sigma_n$ ($\sigma_1 = 1$) be such that G is the disjoint union of the $H\sigma_i$. Then $\mathfrak{p}'^{\sigma_i}$ are all distinct from each other, whence $a'^{\sigma_i} \in \mathfrak{p}'$ except for $i = 1$, whence if we set $b = \sum a'^{\sigma_i}$ then $b \in R$ and $a' - b \in \mathfrak{p}' \cap S = \mathfrak{q}$, which proves (2). Since (2) is settled, it is sufficient to show that $\mathfrak{p}S_{\mathfrak{q}} = \mathfrak{q}S_{\mathfrak{q}}$ in order to prove (3), hence, considering an arbitrary element of $\mathfrak{q}$, we can reduce to the almost finite case, as in (2), and we assume again that G is finite. Let c be an element of $\mathfrak{q}$ which is not in any other maximal ideal of S. Then, with the σ_i as above, c^{σ_i} is not in $\mathfrak{p}'$ for $i \neq 1$, whence the product $c' = c^{\sigma_2} \cdots c^{\sigma_n}$ is not in $\mathfrak{p}'$. Since $cc' \in R$ and c' is integral over R, we see that $c' \in S$. Since $c' \notin \mathfrak{p}'$, we see that $c' \notin \mathfrak{q}$, whence $c \in \mathfrak{p}S_{\mathfrak{q}}$ because $cc' \in \mathfrak{p}$. Let c^* be an arbitrary element of $\mathfrak{q} \cap \mathfrak{a}$ (= Jacobson radical of S).

Then $c + c^*$ satisfies the same condition for c above, whence $c \mid c^*$ in $\mathfrak{p}R_\mathfrak{q}$ and therefore $c^* \in \mathfrak{p}R_\mathfrak{q}$. Since $(\mathfrak{q} \cap \mathfrak{a})R_\mathfrak{q} = \mathfrak{q}R_\mathfrak{q}$, we see that $\mathfrak{p}R_\mathfrak{q} = \mathfrak{q}R_\mathfrak{q}$, which proves (3). (5) is easily seen. We see, by the definitions of unramifiedness and Galois groups, that if (4) and (6) are proved for the almost finite case, then the general case follows. Thus we may assume again that G is finite. In order to prove (4), it suffices to show that $\mathfrak{q}'$ is unramified over S, and we may assume that $R = S$. Since I is the Galois group of R' over I, $R'_{\mathfrak{p}'}/\mathfrak{p}'R'_{\mathfrak{p}'}$ is purely inseparable over $T_{\mathfrak{q}'}/\mathfrak{q}'T_{\mathfrak{q}'}$, hence we may assume that $R' = T$ (for both (4) and (6)). Let $1, a, \ldots, a^{m-1}$ be such that their residue classes modulo $\mathfrak{q}'$ form a linearly independent base of a maximal simple subextension L of $T/\mathfrak{q}'$ over $S/\mathfrak{q}$ and set $T' = \sum_0^{m-1} Ra^i$. Since $I = \{1\}$ by our assumption, every element ($\neq 1$) of $G = H$ induces a non-trivial automorphism of $T/\mathfrak{q}'$ over $S/\mathfrak{q}$, whence $m \geq$ order of G. Since $1, a, \ldots, a^{m-1}$ must be linearly independent over R, we see that $m \leq$ order of G, whence $m =$ order of G. Furthermore, we see at the same time that L must be separable over $S/\mathfrak{q}$, whence $T/\mathfrak{q}'$ must be separable over $S/\mathfrak{q}$, and $T/\mathfrak{q}' = L$, which proves (6). Furthermore, we see that the degree of irreducible monic polynomial $f(x)$ over R which has a as a root is equal to m, whence T' is a ring. Since $T/\mathfrak{q}'$ is separable over $S/\mathfrak{q}$, $f(x)$ modulo $\mathfrak{q}$ is separable, whence the discriminant d of $f(x)$ is a unit in R, whence T' is a normal ring, and therefore $T' = T$. Since $f(x)$ is irreducible modulo $\mathfrak{q}$, we see that $\mathfrak{q}T$ is prime, which proves (4). Thus the proof of (41.2) is completed.

Let $a_1, \ldots, a_n$ be linearly independent elements of R' over R such that $\sum Ra_i$ is a ring. Let G^* be the subgroup of G which is the set of σ such that $\sigma(a_i) = a_i$ for every i, and let $\sigma_1, \ldots, \sigma_m$ ($\sigma_1 = 1$) be such that G is the disjoint union of the $G^*\sigma_i$. Since $\sum Ra_i$ is free, we have $m = n$. Then the square of the determinant $|a_i^{\sigma_j}|$ is called the *discriminant* of the elements $a_1, \ldots, a_n$. Note that if the a_i are $1, a, a^2, \ldots, a^{n-1}$ for some a, then the discriminant of these elements is the discriminant of the irreducible monic polynomial which has a as a root. If A is a matrix of linear transformation over R acting on $\sum Ra_i$ and if $A(\sum Ra_i)$ is a ring which has the same field of quotients as $\sum Ra_i$, then we see obviously that (discriminant of $A(a_1), \ldots, A(a_n)$) = (det A)^2 (discriminant of $a_1, \ldots, a_n$). In particular, the discriminant of a linearly independent base of $\sum Ra_i$ is unique up to units, whence it is called the *discriminant of* $\sum Ra_i$.

(41.3) *With the notation as above, assume that the discriminant d of $\sum Ra_i$ is not in $\mathfrak{p}$. Then every prime ideal $\mathfrak{p}''$ of $\sum Ra_i$ which lies over $\mathfrak{p}$ is unramified over R.*

Proof. We may assume that R' is the smallest Galois extension of R containing $\sum Ra_i$ and that $\mathfrak{p}$ is the unique maximal ideal of R. If $I \nsubseteq G^*$, then we may assume that $\sigma_2 \in I$, which implies that $d \equiv 0 \pmod{\mathfrak{p}'}$, whence $d \equiv 0 \pmod{\mathfrak{p}}$, which is a contradiction. Thus $I \subseteq G^*$. The same is applied to every maximal ideal $\mathfrak{p}''$ of R' and we see that $\sigma^{-1}I\sigma \subseteq G^*$. Thus G^* contains the normalsubgroup generated by I, whence $I = \{1\}$, i.e., $T = R'$, which proves that $\sum Ra_i/\mathfrak{p}''$ is separable over $R/\mathfrak{p}$ by (41.2). Let a_i' be the residue classes of a_i modulo the Jacobson radical $\mathfrak{n}$ of $\sum Ra_i$. If the a_i' are linearly dependent over $R/\mathfrak{p}$, then considering a linear transformation on $\sum Ra_i$, we may assume that $a_1 \in \mathfrak{n}$, whence a_1^q is in the Jacobson radical of R', which implies that $d \in \mathfrak{p}$ and gives a contradiction. Thus the a_i' are linearly independent, whence length $\sum Ra_i/\mathfrak{n} =$ length $\sum Ra_i/\mathfrak{p}(\sum Ra_i)$, and therefore $\mathfrak{n} = \mathfrak{p}(\sum Ra_i)$. Thus $\mathfrak{p}(\sum Ra_i)_{\mathfrak{p}''} = \mathfrak{n}(\sum Ra_i)_{\mathfrak{p}''} = \mathfrak{p}''(\sum Ra_i)_{\mathfrak{p}''}$ and the assertion is proved completely.

On the other hand, we prove the following lemma:

(41.4) *Let R' be a finite separable integral extension of a normal ring R. Let $\mathfrak{p}$ be a prime ideal in R. If every prime ideal $\mathfrak{p}'$ which lies over $\mathfrak{p}$ is unramified over R and if $R/\mathfrak{p}$ contains infinitely many elements, then there exists an element a of R' such that R' and $R[a]$ have the same field of quotients and such that the discriminant d, of the irreducible monic polynomial $f(x)$ over R such that $f(a) = 0$, is not in $\mathfrak{p}$.*

Proof. Let S be the complement of $\mathfrak{p}$ in R. Then $R_S'/\mathfrak{p}R_S'$ is the direct sum of fields $L_i' = R_S'/\mathfrak{p}_i'R_S'$ which are separable over $L = R_S/\mathfrak{p}R_S$. Let a_i be an element of L_i' which generates L_i' over L. Let $g_i(x)$ be the irreducible monic polynomial over L which has a_i as a root. Since L contains infinitely many elements, considering $a_i - b_i$ with $b_i \in L$, we may assume that the $g_i(x)$ are different from each other. Let a^* be an element of R_S' such that a^* modulo $\mathfrak{p}R_S'$ is the direct sum of the elements a_i. Let s be an element of S such that $a = a^*s$ is in R'. Then a modulo $\mathfrak{p}_i'$ is a root of $g_i(x/s)s^{d_i}$ ($d_i = \deg g_i$). Let $f(x)$ be the irreducible monic polynomial over R which has a as a root, and let $f'(x)$ be the derivative of $f(x)$. Then, by virtue of (38.6) applied to each $\mathfrak{p}_i'$, we see that $f'(a)$ is not in $\mathfrak{p}_i'$, and that R' and $R[a]$ have the same field of quotients. Let R^* be a finite Galois extension of R which contains R', and let $\mathfrak{p}^*$ be a prime ideal of R^*

which lies over $\mathfrak{p}$. Then $f'(a)$ is not in $\mathfrak{p}^*$. Since $\mathfrak{p}^*$ is arbitrary, we see that any conjugate of $f'(a)$ is not in $\mathfrak{p}^*$ by (10.12), whence the discriminant d of $f(x)$ is not in $\mathfrak{p}^*$, whence not in $\mathfrak{p}$, by (10.17).

(41.5) THEOREM. *Let R' be a finite separable integral extension of a Krull ring R. If R' is a free R-module and if every prime ideal of height 1 in R' is unramified over R, then every prime ideal $\mathfrak{p}'$ of R' is unramified over R.*

Proof. Set $\mathfrak{p} = \mathfrak{p}' \cap R$. Then, considering $R_{\mathfrak{p}}$ and $R'_{(R-\mathfrak{p})}$, we may assume that $\mathfrak{p}$ is the unique maximal ideal of R. If height $\mathfrak{p} = 1$, then the assertion is obvious, and we assume that height $\mathfrak{p} > 1$. Let d be the discriminant of R'. Assume that d is a non-unit. Then there is a prime ideal $\mathfrak{q}$ of height 1 in R which contains d. Let a be such an element as given by (41.4) applied to $\mathfrak{q}$. Then the discriminant d', of the irreducible monic polynomial $f(x)$ such that $f(a) = 0$, is not in $\mathfrak{q}$. As was remarked before (41.3), d' is the discriminant of $R[a]$ and is in dR, which is a contradiction, whence d is a unit in R, which proves the assertion by virtue of (41.3).

(41.6) *Let $(R, \mathfrak{m})$ be a regular local ring with a regular system of parameters $x_1, \ldots, x_r$ and let $(V, \mathfrak{n})$ be a valuation ring which dominates R. Set $\mathfrak{a} = x_1R + \cdots + x_sR$ $(2 \leq s \leq r)$. If $x_2/x_1, \ldots, x_s/x_1$ modulo $\mathfrak{n}$ are algebraically independent over $R/\mathfrak{m}$ and if R^* is the dilatation of R by the ideal $\mathfrak{a}$ with respect to V, then R is a subspace of R^*.*

Proof. Set $R' = R[x_2/x_1, \ldots, x_s/x_1]$. Then x_1R' is a prime ideal and $x_1R' = \mathfrak{a}R'$. Set $R'' = R'_{\mathfrak{a}R'}$. Then R'' is a Noetherian valuation ring. Obviously R^* is dominated by R'' and R'' is a quadratic dilatation of both R and R^*. For an element f of R, $f \in \mathfrak{m}^n$ if and only if $f \in x_1^nR''$, and, if we denote by $\mathfrak{m}^*$ the maximal ideal of R^*, then for an element f of R^*, $f \in \mathfrak{m}^{*n}$ if and only if $f \in x_1^nR''$. Therefore $\mathfrak{m}^{*n} \cap R = \mathfrak{m}^n$ and we complete the proof.

We need one more preliminary:

(41.7) THEOREM. *Let $(R, \mathfrak{m})$ be a complete regular local ring with a regular system of parameters $x_1, \ldots, x_r$ with $r \geq 3$. Let P be a normal local ring which is a finite separable integral extension of R. Then there is a finite number of elements $a_1, \ldots, a_s$ of R such that, letting y be a transcendental element over R, and c an element of R, the local ring $P_c = P(y)/(x_3y - x_1 - cx_2)P(y)$ is analytically irreducible, whenever c is such that $\prod (c - a_i) \notin \mathfrak{m}$.*

Proof. Let b be an element of P such that P is the derived normal

ring of $R[b]$ and let $f(X)$ be the irreducible monic polynomial over R such that $f(b) = 0$. Set $R_c = R(y), (x_3 y, \ldots, x_1 - cx_2)R(y)$. Then it is obvious that P_c is generated by R_c and P, whence P_c is a finite integral extension of R_c and has the same quotient field as $R_c[b]$. Therefore the completions of P_c and $R_c[b]$ have the same total quotient ring, whence the analytic irreducibility of P_c is equivalent to that of $R_c[b]$. Therefore it is sufficient to show that $f(X)$ is irreducible over the completion R_c^* of R_c if $\prod (c - a_i) \notin \mathfrak{m}$. Assume the contrary, namely, assume that there are infinitely many c, say $c_1, c_2, \ldots$, whose residue classes modulo $\mathfrak{m}$ are different from each other, such that $f(X)$ is reducible over R_c^*.

Before proceeding with the proof, we make some remarks. For a $c \in R$, we set $u_c = (x_1 + cx_2)/x_3$. For two $c, d \in R$ such that $c - d \notin \mathfrak{m}$, set $R_{c,d} = R[u_c, u_d]_{\mathfrak{m}'}$ with $\mathfrak{m}' = \mathfrak{m}R[u_c, u_d]$; note that $R_{c,d}$ is a dilatation of both R_c and R_d of the type in (41.6) (and therefore $\mathfrak{m}'$ is a prime ideal). Therefore R_c and R_d are subspaces of $R_{c,d}$. Assume that $e \in R$ is such that $(e - c)(e - d) \notin \mathfrak{m}$. Then we can consider $R_{c,e}$ and $R_{d,e}$. Set $\alpha = (d - e)/(d - c)$, $\beta = (e - c) \div (d - c)$. Then we have $u_e = \alpha u_c + \beta u_d$. Therefore $u_e \in R_{c,d}$ and, u_c, u_e modulo $\mathfrak{m}R_{c,d}$ are algebraically independent over $R/\mathfrak{m}$. Thus $R_{c,d}$ dominates $R_{c,e}$. Symmetrically, $R_{c,e}$ dominates $R_{c,d}$ and we have $R_{c,e} = R_{c,d}$. Therefore $R_{c,d} = R_{d,e} = R_{c,e}$. We apply this fact to $R_{c_1}, R_{c_2}, \ldots$ and we have that the R_{c_i} are subspaces of $R'' = R_{c_1,c_2}$. Let the completions of R'', R_{c_i} be R''^*, $R_{c_i}^*$, respectively. Then $R_{c_i}^* \leq R''^*$.

Therefore we can consider factorization of $f(X)$ in the algebraic closure of R''^*. Since there is only a finite number of ways in which the polynomial $f(X)$ splits into two monic factors, there are at least three mutually distinct elements among the c_i, say d_1, d_2, d_3, such that $f(X)$ has the same factorization $f(X) = g(X)h(X)$ over all $R_{d_i}^*$. For simplicity of notation, we denote u_{d_i} by u_i. Let Q be a complete set of representatives of the residue class field of R. $Q[u_1, u_2]$ denotes the set of all polynomials in u_1, u_2 with coefficients in Q. $Q(u_1, u_2)$ denotes the set of all F/G such that $F, G \in Q[u_1, u_2]$, whose residue classes modulo $\mathfrak{m}$ have no common factor, and such that the coefficient of the lexicographical highest term in G is 1. Then every element of R''^* is uniquely expressed as a power series in $x_3, \ldots, x_r$ with coefficient in $Q(u_1, u_2)$. Thus we may write (formally) $R''^* = R_{d_1,d_2}^* = Q(u_1, u_2)[[x_3, \ldots, x_r]]$. $Q(u_1)$ and $Q(u_2)$ being defined similarly,

$R^*_{d_1}$ is the set of power series in $u_3x_3, x_3, \ldots, x_r$ with coefficients in $Q(u_1)$ and $R^*_{d_1} \quad Q(u_1)[[u_3x_3, x_3, \ldots, x_r]]$; similarly

$$R^*_{d_2} = Q(u_2)[[u_1x_3, x_3, \ldots, x_r]].$$

Let a be an arbitrary coefficient in $g(X)$ and let $\sum a_{n_3\cdots n_r}x_3^{n_3}\cdots x_r^{n_r}$ be the power series expansion of a in

$$Q(u_1, u_2)[[x_3, \ldots, x_r]].$$

Since a is in $R^*_{d_1}$, $a = \sum a'_{n_3\cdots n_r}(u_2x_3)^{n_2}x_3^{n_3}\cdots x_r^{n_r}$ with the coefficients in $Q(u_1)$. Hence $a = \sum(\sum_{i=0}^{n_3} a_{i(n_3-i)n_4\cdots n_r}u_2^i)x_3^{n_3}\cdots x_r^{n_r}$. From this expression, we derive an expression for a as a power series in $x_3, \ldots, x_r$ with coefficients in $Q(u_1, u_2)$. By the uniqueness of the expression, we see inductively on n_3 that $a_{n_3\cdots n_r} = F_{(n)}/G_{(n)}$, $G_{(n)} \in Q[u_1]$ and $F_{(n)}$ is a polynomial in u_2 of degree at most n_3 with coefficients in $Q[u_1]$. Considering $R^*_{d_2}$, we see that $G_{(n)} \in Q[u_2]$ and $F_{(n)}$ is a polynomial in u_1 of degree at most n_3 with coefficients in $Q[u_2]$. Thus $G_{(n)} = 1$ and $a_{n_3\cdots n_r}$ is a polynomial in u_1 and u_2 with coefficients in Q and its degree on each u_i is at most n_3. Set $\alpha = (d_3 - d_2)/(d_3 - d_1)$ and $\beta = (d_2 - d_1)/(d_3 - d_1)$. Then α, β are units in R and $u_2 = \alpha u_1 + \beta u_3$. If we substitute for u_2 the expression $du_1 + eu_3$ in $a_{n_3\cdots n_r}$, we obtain a polynomial $a^*_{n_3\cdots n_r}$ in u_1 and u_3 with coefficients in R; we can choose d_3 so that the degree of $a^*_{n_3\cdots n_r}$ in u_1 is equal to the total degree $d(n_3, \ldots, n_r)$ of $a_{n_3\cdots n_r}$ for a given $a_{n_3\cdots n_r}$. The expression $a = \sum a^*_{n_3\cdots n_r}x_3^{n_3}\cdots x_r^{n_r}$ is then a power series expansion of a with coefficients in $R[u_1, u_3]$. Assume that there is a $d(n_3, \ldots, n_r)$ which is greater than n_3, and let $a_{m_3\cdots m_r}$ be one which has the lexicographically smallest suffix $m_3, \ldots, m_r$ among those $a_{m_3\cdots m_r}$ such that $d(m_3, \ldots, m_r) > m_3$. We choose d_3 so that $a^*_{m_3\cdots m_r}$ is of degree $d(m_3, \cdots, m_r)$ in u_1. Let the expression of a in $R^*_{d_1,d_3} = Q(u_1, u_3)[[x_3, \ldots, x_r]]$ be $\sum a''_{n_3\cdots n_r}x_3^{n_3}\cdots x_r^{n_r}$. Then, as is obvious, each $a''_{n_3\cdots n_r}$ is the coefficient of $x_3^{n_3}\cdots x_r^{n_r}$ in the re-expression of $\sum_{s_i\le n_i} a^*_{s_3\cdots s_r}x_3^{s_3}\cdots x_r^{s_r}$. Therefore, by the choice of $m_3, \ldots, m_r$, the property that $a^*_{m_3\cdots m_r}$ has degree in u_1 greater than m_3 is carried over $a''_{m_3\cdots m_r}$. On the contrary, applying the result on the expression of a in $Q(u_1, u_2)[[x_3, \ldots, x_r]]$, we see that $a''_{m_3\cdots m_r}$ must be of degree at most m_3 in u_1, which is a contradiction. Thus $d(n_3, \ldots, n_r) \le n_3$ for any $a_{n_3\cdots n_r}$. This means that $a_{n_3\cdots n_r}x_3^{n_3}$ is in R, and is in $\mathfrak{m}^{n_3}$, which implies that a is in R because R is complete, whence $g(X) \in R[X]$ and this is a contradiction. Thus the proof is complete.

We note that:

(41.8) *Assume that a quasi local ring* $(R', \mathfrak{m}')$ *dominates a quasi local ring* $(R, \mathfrak{m})$. *If* R' *is unramified over* R *and if* $R'/\mathfrak{m}'$ $R/\mathfrak{m}$, *and if* R' *is a finite* R*-module, then* R' R.

Proof. Since $R'/\mathfrak{m}R'$ $R/\mathfrak{m}$, it follows that $R' = \mathfrak{m}R' + R$, whence R R' by the lemma of Krull-Azumaya.

Now we are to prove (41.1). Considering pairs (R, P) of local rings as in (41.1), we say in the present proof that (R, P) is *equivalent* to (R', P') if it holds that P is unramified over R if and only if P' is unramified over R' (hence, we see, when (41.1) is proved, that all pairs are equivalent to each other). The first step of our proof is to show that:

(*) *For any given pair* (R, P), *there is an equivalent pair* (R^*, P^{**}) *such that* R^* *is the completion of* R.

We denote in general by c an element of P which is integral over R and which generates the field of quotients L of P over the field of quotients K of R, and by $f(x; c)$ the irreducible monic polynomial in an indeterminate x over R which has c as a root. Furthermore, we denote by $g_i(x; c)$ $(i = 1, \ldots, n(c))$ the irreducible monic factors of $f(x; c)$ over the completion R^* of R. Let P^* be the completion of P and let $\mathfrak{q}_1^*, \ldots, \mathfrak{q}_m^*$ be the prime divisors of zero in P^*. Let P' be the integral closure of R in P. Then, since P is separable over R, P' is a finite R-module by (10.16), whence the completion P'^* of P' has the same total quotient ring as $R^*[c]$, whence P'^* has no nilpotent elements except zero and the prime divisors of zero in P'^* corresponds in a one to one way to $g_i(x; c)$. Since P is a ring of quotients of P' with respect to a maximal ideal, P^* is a direct summand of P'^*. Therefore, we see that $0 = \mathfrak{q}_1^* \cap \cdots \cap \mathfrak{q}_m^*$ and, after a suitable renumbering of the g_i, $g_i(c;c) \in \mathfrak{q}_i^*$ for $i \leq m$, and $g_j(c; c) \notin \mathfrak{q}_i^*$ if $j \neq i$. We shall show that $m = 1$. Assume for a moment that $m > 1$. Set $\mathfrak{a}_i^* = \mathfrak{q}_i^* + (\bigcap_{j \neq i} \mathfrak{q}_j^*)$ and $\mathfrak{a}^* = \bigcap \mathfrak{a}_i^*$. Assume that there is a prime ideal $\mathfrak{p}^*$ of P^* containing $\mathfrak{a}^*$ such that height $(\mathfrak{p}^* \cap P) \leq 1$. Since $\mathfrak{p}^*$ contains at least two of the $\mathfrak{q}_i^*$, $f(x; c)$ modulo $\mathfrak{p}^*$ has a multiple root for any possible c, whence, if $f'(x; c)$ denotes the derivative of $f(x; c)$, then $f'(c; c) \in \mathfrak{p}^*$ for any c. Thus $f'(c; c) \in \mathfrak{p}^* \cap P$, and $\mathfrak{p}^* \cap P$ is ramified over R by (38.6), which is a contradiction. Thus there is no such $\mathfrak{p}^*$. Let d be the discriminant of $f(x; c)$ for a fixed c, and let S be the set of elements s of P such that $dP:sP = dP$. Since P is normal, every prime divisor of dP is of height 1. Therefore the non-existence of $\mathfrak{p}^*$ above shows that S meets every prime ideal of P^*

containing $\mathfrak{a}^*$, hence P_S^* contains an idempotent element e which is not the identity. Since e is integral over R^*, we have $de \in P^*$ by (10.15). Since $e \in P_S^*$, there is an element s of S such that $es \in P^*$. Therefore we see that $e \in P^*$ by (37.1), which is a contradiction because P^* is a local ring. Thus $m = 1$, and P^* is an integral domain.

Let P^{**} be the derived normal ring of P^*. Assume that there is a prime ideal $\mathfrak{p}^*$ of height 1 in P^{**} which is ramified over R^*. Then $f'(c; c) \in \mathfrak{p}^*$ for any c by (38.6), and $\mathfrak{p}^* \cap P$ is ramified over R, which is a contradiction. Thus R^*, P^{**} satisfy the conditions in (41.1). If P is unramified over R, then P is regular, and $P^* = P^{**}$ by (25.11), hence P^{**} is unramified over R^*. Assume that P is ramified over R and that P^{**} is unramified over R^*. Then $P^{**}/\mathfrak{m}P^{**} \neq P/\mathfrak{n}$ by (41.8). Let a' be an element which generates $P^{**}/\mathfrak{m}P^{**}$ over $R/\mathfrak{m}$, and let $h(x)$ be a monic polynomial over R such that h modulo $\mathfrak{m}$ is the irreducible monic polynomial for a'. Let $\mathfrak{n}'$ be the maximal ideal of $P[x]/h(x)P[x]$ which corresponds to the irreducible factor $h^*(x)$ of ($h(x)$ modulo $\mathfrak{n}$) over $P/\mathfrak{n}$ of which a' is a root. Then we see that $h^*(x)$ has a linear factor $x - a'$ over $P^{**}/\mathfrak{m}P^{**}$. The completion Q^* of $Q = (P[x]/h(x)P[x])_{\mathfrak{n}'}$ coincides with $P^*[x]/h''(x)P^*[x]$ with a factor $h''(x)$ of $h(x)$ over P^*. Since P^{**} is Henselian, and since $h(x)$ is separable, the factor h'' of $h(x)$ has a linear factor $x - a$ over P^{**} with an $a \in a'$, which shows that Q is analytically reducible because $a \notin P^*$ and $\deg h'' > 1$. Since the discriminant of $h(x)$ is a unit, it is obvious that Q satisfies the conditions in (41.1) with respect to R. Then, as we have proved above, Q must be analytically irreducible, which is a contradiction. Thus the pair (R^*, P^{**}) is equivalent to (R, P) and the statement (*) is proved.

We remark here that:

(**) *For a given pair* (R, P), *if* x *is a transcendental element over* P, *then* $(R(x), P(x))$ *is equivalent to* (R, P).

The proof of this statement is straightforward and we omit it.

By virtue of (*) and (**), we may assume, in order to prove (41.1), that R is a complete regular local ring and that $R/\mathfrak{m}$ contains infinitely many elements. Let L be the maximal separable subextension of $P/\mathfrak{n}$ over $R/\mathfrak{m}$ and let a' be an element which generates L over $R/\mathfrak{m}$. Let $h(x)$ be a monic polynomial over R such that h modulo $\mathfrak{m}$ is the irreducible polynomial for a'. Then, since P is Henselian by (30.3), $h(x)$ has a root a such that $a \in a'$. Then $(R[a], P)$ is obviously equivalent to (R, P). Therefore we may assume furthermore that $P/\mathfrak{n}$ is purely inseparable over $R/\mathfrak{m}$.

We shall prove (41.1) by induction on altitude R. If altitude $R \leq 1$, then there is nothing to prove. If $R \geq 2$, then, since P is normal, P is a Macaulay ring, whence P is a free R-module by (25.16), and the assertion follows from (41.5). Therefore we assume that $r \geq 3$. Let x be an element of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be prime divisors of xP. By the assumption on P, we have $xP = \bigcap \mathfrak{q}_i$. Set $Q_i = P/\mathfrak{q}_i$ and let Q_i' be the derived normal ring of Q_i. Since Q_i is complete, Q_i' is a normal local ring. By the induction assumption, if $\mathfrak{r}$ is a prime ideal of P different from $\mathfrak{n}$, then $P_{\mathfrak{r}}$ is unramified over $R_{(\mathfrak{r} \cap R)}$. Applying this fact to those $\mathfrak{r}$ containing $\mathfrak{q}_i$, we have: (1) $\mathfrak{r}/\mathfrak{q}_i$ is unramified over R/xR; hence $(Q_i)_{\mathfrak{r}/\mathfrak{q}_i}$ is a regular local ring, and consequently (2) the conductor of Q_i in Q_i' contains a power of the maximal ideal; and (3) Q_i' is unramified over R/xR. In particular, the residue class field L_i' of Q_i' is separable over $R/\mathfrak{m}$, whence $P/\mathfrak{n} = R/\mathfrak{m}$ by our assumption made above. If $Q_1 \neq Q_1'$, then $L_1' \neq P/\mathfrak{n}$ by (41.7). Then, taking an element a' which generates L_i' over $P/\mathfrak{n} = R/\mathfrak{m}$, we extend both P and R so that their residue class fields become L_1' by the method we used above. Namely, let $f(x)$ be a monic polynomial over R such that f modulo $\mathfrak{m}$ is the irreducible monic polynomial for a'. Set $P_1 = P[x]/f(x)P[x]$, $R_1 = R[x]/f(x)R[x]$. Since the discriminant of f is unit in R, it follows that P_1 and R_1 are normal and are unramified over P and R, respectively. $\mathfrak{m}P \neq \mathfrak{n}$ if and only if $\mathfrak{m}P_1 \neq \mathfrak{n}P_1$ and therefore (R_1, P_1) is equivalent to (R, P). Furthermore, $f(x)$ modulo $\mathfrak{q}_1$ is reducible over Q_1, and we see that $\mathfrak{q}_1$ splits into several prime ideals. Since the total number s of the $\mathfrak{q}_i$ does not exceed the degree of extension of the field of quotients L of P over the field of quotients K of R, we see that, after a finite number of steps, we come to the case where $Q_1 = Q_1'$, whence $Q_1 = R/xR$. Thus we may assume that there is an element x of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$ such that xP has a prime divisor $\mathfrak{q}_1$ with the property that $Q/\mathfrak{q}_1 = R/xR$. Now let c, y and $x_1, \ldots, x_r$ be as in (41.6) and consider $(R(y), P(y))$, which is equivalent to (R, P). Set $z = x_3y - x_1 - cx_2$. Then $zP(y)$ is prime, and our observation for x can be applied to z and we have: (1′) if $\mathfrak{r}'$ is a prime ideal of $P(y)$ such that $z \in \mathfrak{r}' \subset \mathfrak{n}P(y)$, then $\mathfrak{r}/zP(y)$ is unramified over $R(y)/zR(y)$ and consequently (2′) the conductor of $P(y)/zP(y)$ in its derived normal ring P'' contains a power of the maximal ideal $\mathfrak{n}P(y)/zP(y)$. Since $P(y)/zP(y)$ is analytically irreducible, the completion of P'' is an integral domain, which implies that P'' is a local ring. By our induction assumption, we have (3′) P'' is unramified over $R(y)/zR(y)$.

We have only to show that P'' $P(y)/zP(y)$. Let the maximal ideal of P'' be $\mathfrak{n}''$. Let $\mathfrak{r}''$ be a minimal prime divisor of $\mathfrak{q}_1P(y) + zP(y)$. Then the conductor of $P(y)/zP(y)$ in P'' is not contained in $\mathfrak{r}''/zP(y)$, whence the derived normal ring of $P(y)/\mathfrak{r}''$ has a residue class field which contains $P''/\mathfrak{n}''$. On the other hand, since $P/\mathfrak{q}_1$ R/xR, $P(y)/\mathfrak{q}_1P(y) = R(y)/xR(y)$, and therefore $P(y)/\mathfrak{r}''$ is a regular local ring, whence $P(y)/\mathfrak{r}''$ is normal. Therefore $P''/\mathfrak{n}'' = R/\mathfrak{m}$, whence $P(y)/zP(y) = R(y)/zR(y)$ by (41.8) and P is unramified over R. Thus the proof of (41.1) is complete.

EXERCISES. *1.* Show by an example that the normality of P in (41.1) is important.

2. Show by an example that the regularity of R in (41.1) is important. (Hint. Consider an extension R' of the following type. Let R be a normal local ring in which there is a prime ideal $\mathfrak{p}$ of height 1 such that $\mathfrak{p}$ itself is not principal, but there is an e such that $\mathfrak{p}^{(e)}$ is principal. Take the smallest e. Let R' be the derived normal ring of $R[a]$ with a such that $a^eR = \mathfrak{p}^{(e)}$.)

42. Tensor products

(42.1) *Let L and L' be fields containing an integral domain I which has field of quotients K. If L is finitely generated over K, then $L \otimes_I L'$ is Noetherian, $L \otimes_I L' = L \otimes_K L'$, and the zero ideal in $L \otimes L'$ has no imbedded prime divisor.*

Proof. L is of finitely generated type over K, whence $L \otimes L'$ is of finitely generated type over L', which proves that $L \otimes L'$ is Noetherian. Since L and L' contain K, we see that $L \otimes_I L' = L \otimes_K (K \otimes_I L') = L \otimes_K L'$. Let $(x) = (x_1, \ldots, x_n)$ be a transcendence base of L' over K. Then $L \otimes L' = (L \otimes_K K(x)) \otimes_{K(x)} L'$. Let K' $(=L(x))$ be the field of quotients of $L \otimes_K K(x)$. Since $K(x)$ is a field, $L \otimes L'$ is a subring of $K' \otimes_{K(x)} L'$. Therefore the total quotient ring of $K' \otimes L'$ contains $K' \otimes_{K(x)} L'$. Since L' is a finite algebraic extension of $K(x)$, we see that $K' \otimes_{K(x)} L'$ is a finite K'-module, whence $K' \otimes_{K(x)} L'$ satisfies the minimum condition for ideals, which proves the last assertion.

Let $(R, \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ and $(R', \mathfrak{p}'_1, \ldots, \mathfrak{p}'_n)$ be semi-local rings which are modules over a ring I. Let ϕ and ϕ' be the natural mappings from I into R and R', respectively $(\phi(a) = a \cdot 1$ for $a \in I$ and the identity 1 of R; similarly for $\phi')$. Set $\mathfrak{q}_i = \phi^{-1}(\mathfrak{p}_i)$, $\mathfrak{q}'_j = \phi'^{-1}(\mathfrak{p}'_j)$ and $T = R \otimes_I R'$. Then we have the following lemma.

(42.2) $\mathfrak{p}_iT + \mathfrak{p}'_jT \neq T$ *if and only if* $\mathfrak{q}_i = \mathfrak{q}'_j$. *In this case, if one of $R/\mathfrak{p}_i$ and $R'/\mathfrak{p}'_j$ is of finitely generated type over $I/\mathfrak{q}_i$, then*: (1)

$T/(\mathfrak{p}_i T + \mathfrak{p}_j' T)$ *is Noetherian*, (2) *every prime divisor* $\mathfrak{P}$ *of* $\mathfrak{p}_i T + \mathfrak{p}_j' T$ *is a minimal prime divisor, and* (3) $\mathfrak{P}$ *has a finite basis.*

Proof. If $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j'$, then $\mathfrak{p}_i T + \mathfrak{p}_j' T$ contains $\mathfrak{p}_j' T + \mathfrak{q}_i T = R'T = T$, and we prove the first assertion easily. Since $T/(\mathfrak{p}_i T + \mathfrak{p}_j' T) = (R/\mathfrak{p}_i) \otimes_{I/\mathfrak{q}_i} (R'/\mathfrak{p}_j')$, we prove (1) and (2) by (42.1). Since $\mathfrak{p}_i T + \mathfrak{p}_j' T$ has a finite basis, (3) follows from (1).

With the same notation as above, we assume that every $R/\mathfrak{p}_i$ is of finitely generated type over $I/\mathfrak{q}_i$. Let S be the intersection of complements of prime divisors of $\mathfrak{p}_i T + \mathfrak{p}_j' T$ for all pairs $(\mathfrak{p}_i, \mathfrak{p}_j')$ such that $\mathfrak{p}_i T + \mathfrak{p}_j' T \neq T$. Then T_S is called the *local tensor product* of R and R' over I and is denoted by $R \times_I R'$ or by $R \times R'$. By this definition and by (42.2), $R \times R'$ is a quasi-semi-local ring and the maximal ideals of $R \times R'$ have finite bases.

We note that if R and R' are of finitely generated type over I, then so is $R \times R'$. If R is of finitely generated type over I, then $R \times R'$ is of finitely generated type over R', whence in this case $R \times R'$ is a semi-local ring.

Now we go back to the general case where $R \times R'$ is defined. Let $\mathfrak{M}$ be the Jacobson radical of $R \times R'$. Set $\mathfrak{n} = \bigcap_n \mathfrak{M}^n$. Then $R \times R'/\mathfrak{n}$ is a semi-local ring which may not be Noetherian. Then the completion of $R \times R'/\mathfrak{n}$ is called the *complete tensor product* of R and R' over I and is denoted by $R \bar{\otimes}_I R'$ or by $R \bar{\otimes} R'$.

(42.3) THEOREM. *$R \bar{\otimes} R'$ is a semi-local ring (which is Noetherian).*

Proof. Every maximal ideal of $R \times R'$ has a finite basis, hence every maximal ideal of $R \bar{\otimes} R'$ has a finite basis. Therefore the assertion is proved by (31.7).

(42.4) *With the same notation as above, if R^* and R'^* are semi-local rings which contain R and R' respectively, as dense subspaces, then $R^* \bar{\otimes} R'^* = R \bar{\otimes} R'$.*

Proof. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the Jacobson radicals of R and R', respectively, and let $\mathfrak{a}(n)$ be the ideal of $R \bar{\otimes} R'$ generated by $\mathfrak{m}^n$ and $\mathfrak{m}'^n$. Then $\mathfrak{a}(1)$ contains a power of the Jacobson radical $\mathfrak{a}$ of $R \bar{\otimes} R'$ by (42.1). It is obvious that $\mathfrak{a}(1)$ is contained in $\mathfrak{a}$. Since $\mathfrak{a}(1)^{2n} \subseteq \mathfrak{a}(n) \subseteq \mathfrak{a}(1)$, we see that the system $\{\mathfrak{a}(n)\}$ is a base of neighborhoods of zero of $R \bar{\otimes} R'$. The same is true for $R^* \bar{\otimes} R'^*$, i.e., the system of $\mathfrak{a}^*(n)$, which are the ideals of $R^* \bar{\otimes} R'^*$ generated by $\mathfrak{m}^n R^*$ and $\mathfrak{m}'^n R^*$, forms a basis for the neighborhoods of zero. Therefore the assertion follows from the fact that $R^* \bar{\otimes} R'^*/\mathfrak{a}^*(n) = (R^*/\mathfrak{m}^n R^*) \times (R'^*/\mathfrak{m}'^n R'^*) = (R/\mathfrak{m}^n) \times (R'/\mathfrak{m}'^n) = R \bar{\otimes} R'/\mathfrak{a}(n)$.

(42.5) COROLLARY. *With the notation as above, if R_i is the completion of $R_{\mathfrak{P}_i}$ and if R_j' is the completion of $R'_{\mathfrak{P}'_j}$ for every (i, j), then $R \otimes R'$ is naturally isomorphic to the direct sum of $R_i \otimes R_j'$ for all (i, j) such that $\mathfrak{p}_i T + \mathfrak{p}_j' T \neq T$, and each $R_i \otimes_I R_j'$ coincides with $R_i \bar{\otimes}_{I_i} R_j'$ if I_i denotes the completion of $I_{\mathfrak{q}_i}$.*

We say that a field K is a *basic field* of a semi-local ring $(R, \mathfrak{p}_1, \ldots, \ldots, \mathfrak{p}_n)$ if K is a subfield of R and if every $R/\mathfrak{p}_i$ is a finite algebraic extension of K.

(42.6) THEOREM. *Assume that R and R' are semi-local rings and that a field K is a basic field of both R and R'. Set $R^* = R \bar{\otimes}_K R'$. Then* altitude R^* = altitude R + altitude R' *and, for any ideals $\mathfrak{a}$ and $\mathfrak{a}'$ of R and R', respectively, such that* depth $\mathfrak{a}$ = *depth* $\mathfrak{a}' = 0$, *we have* $\mu_K(\mathfrak{a}R^* + \mathfrak{a}'R^*) = \mu_K(\mathfrak{a}) \cdot \mu_K(\mathfrak{a}')$.

Proof. Set $f(n) = \text{length}_K\, \mathfrak{a}^n/\mathfrak{a}^{n+1}$ and $g(n) = \text{length}_K\, \mathfrak{a}'^n/\mathfrak{a}'^{n+1}$. If we consider $R/\mathfrak{a}^n$ and $R'/\mathfrak{a}'^n$ as K-modules, then they are direct sums $\sum_{i<n} (\mathfrak{a}^i/\mathfrak{a}^{i+1})$ and $\sum_{j<n} (\mathfrak{a}'^j/\mathfrak{a}'^{j+1})$. $R^*/(\mathfrak{a}R^* + \mathfrak{a}'R^*)^n$ is the homomorphic image of $R^*/(\mathfrak{a}^n R^* + \mathfrak{a}'^n R^*) = (R/\mathfrak{a}^n) \otimes (R'/\mathfrak{a}'^n)$ with kernel $\sum_{i+j=n} (\mathfrak{a}^i/\mathfrak{a}^n) \otimes (\mathfrak{a}'^j/\mathfrak{a}'^n)$. Therefore $R^*/(\mathfrak{a}R^* + \mathfrak{a}'R^*)^n$ is the direct sum $\sum_{i+j<n} (\mathfrak{a}^i/\mathfrak{a}^{i+1}) \otimes (\mathfrak{a}'^j/\mathfrak{a}'^{j+1})$, which shows that length $R^*/(\mathfrak{a}R^* + \mathfrak{a}'R^*)^n = \sum_{i+j<n} f(i)g(j)$. Let r and r' be the altitudes of R and R', respectively. It is sufficient to show that $s(n) = \sum_{i+j<n} f(i)g(j)$ is, for sufficiently large n, a polynomial of degree $r + r'$ in n in which the coefficient of $n^{r+r'}$ is $\mu_K(\mathfrak{a}) \cdot \mu_K(\mathfrak{a}')/((r + r')!)$. In this form, we can forget the structures of R and R', and we consider only polynomials—we may assume that $f(n)$ and $g(n)$ are really polynomials. Namely, we shall prove that:

If $f(n) = (a/(r-1)!)n^{r-1}$ + (a polynomial of lower degree), $g(n) = (b/(r'-1)!)n^{r'-1}$ + (a polynomial of lower degree), and if $s(n) = \sum_{i+j<n} f(i)g(j)$, then $s(n) = cn^{r+r'}$ + (a polynomial of lower degree) with $c = ab/((r + r')!)$.

We prove the above assertion by induction on $r + r'$. If $r + r' = 0$, then the assertion is obvious. Set $f^*(n) = \binom{n + r - 1}{r - 1}$ and $g^*(n) = \binom{n + r' - 1}{r' - 1}$. Then $f(n) = af^*(n)$ + (polynomial of lower degree), $g(n) = bg^*(n)$ + (polynomial of lower degree), whence, by induction, $s(n) = \sum_{i+j<n} f(i)bg^*(j)$ + (a polynomial of degree at most $r + r' - 1$) $= \sum_{i+j<n} abf^*(i)g^*(j)$ + (a polynomial of de-

gree at most $r + r' - 1$). Thus we have reduced to the case where $f = f^*$ and $g = g^+$. This last case is realized by the case where R and R' are the formal power series rings in r and r' letters, respectively, in which case R^* is obviously the formal power series ring in $r + r'$ letters, which proves the assertion.

A Noetherian valuation ring I is called a *basic valuation ring* of a local ring R if R dominates I and if the residue class field of R is a finite algebraic extension of that of I.

(42.7) *If R and R' are local rings which have a common basic valuation ring I with a prime element p, if* altitude R/pR = altitude $R - 1$, *and if* altitude R'/pR' = altitude $R' - 1$, *then* altitude $(R \bar{\otimes}_I R')$ = altitude R + altitude $R' - 1$.

Proof. Let r and r' be the altitudes of R and R', respectively. Then there are systems of parameters $p, x_2, \ldots, x_r$ and $p, x_2', \ldots, x_{r'}'$ of R and R', respectively. We may assume that R and R' are complete, whence they are finite modules over $S = I[[x_2, \ldots, x_r]]$ and $S' = I[[x_2', \ldots, x_{r'}']]$, respectively. Then, as is easily seen, $R \bar{\otimes} R'$ contains the formal power series ring $S^* = I[[x_2, \ldots, x_r, x_2', \ldots, x_{r'}']]$ and is a finite S^*-module. Thus we prove the assertion.

(42.8) THEOREM. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in an unramified regular local ring R, then* height $(\mathfrak{a} + \mathfrak{b}) \leq$ height $\mathfrak{a}$ + height $\mathfrak{b}$ *and* altitude $(\mathfrak{a} + \mathfrak{b}) \leq$ altitude $\mathfrak{a}$ + altitude $\mathfrak{b}$.

Proof. We prove the first formula first. Let $\mathfrak{a}'$ and $\mathfrak{b}'$ be minimal prime divisors of $\mathfrak{a}$ and $\mathfrak{b}$, respectively, such that height $\mathfrak{a}'$ = height $\mathfrak{a}$, height $\mathfrak{b}'$ = height $\mathfrak{b}$ and let $\mathfrak{p}$ be a minimal prime divisor of $\mathfrak{a}' + \mathfrak{b}'$. Then it suffices to show that height $\mathfrak{p} \leq$ height $\mathfrak{a}'$ + height $\mathfrak{b}'$. Since $R_\mathfrak{p}$ is an unramified regular local ring by (28.4), we may replace R with $R_\mathfrak{p}$, and we may assume that $\mathfrak{p}$ is the maximal ideal of R. Furthermore, we may replace R with its completion, whence R is the power series ring in analytically independent elements, say $x_1, \ldots, \ldots, x_r$ over a coefficient ring I. Let $y_1, \ldots, y_r$ be indeterminates and let σ be the isomorphism from $R = I[[x_1, \ldots, x_r]]$ onto $I[[y_1, \ldots, y_r]]$ such that $\sigma(x_i) = y_i$. Set $R^* = I[[x_1, \ldots, x_r, y_1, \ldots, y_r]]$. Then $R^*/(\mathfrak{a}'R^* + \sigma(\mathfrak{b}')R^*)$ is identified with the complete tensor product of $R/\mathfrak{a}'$ and $R/\mathfrak{b}'$ over I. Let $\mathfrak{d}$ be the ideal of R^* generated by $x_i - y_i$ $(i = 1, \ldots, r)$. Then, since $\mathfrak{a}' + \mathfrak{b}'$ is primary to $\mathfrak{p}$, since $R^*/(\mathfrak{a}'R^* + \sigma(\mathfrak{b}')R^* + \mathfrak{d})$ is isomorphic to $R/(\mathfrak{a}' + \mathfrak{b}')$, and since $\mathfrak{d}$ is generated by r elements, we see that altitude $R^*/(\mathfrak{a}'R^* + \sigma(\mathfrak{b}')R^*) \leq r$. If I is

a field, then altitude $R^*/(\mathfrak{a}'R^* + \sigma(\mathfrak{b}')R^*) \geq$ depth $\mathfrak{a}'$ + depth $\mathfrak{b}'$ by (42.6) and it is equal to $(r -$ height $\mathfrak{a}') +$ $(r -$ height $\mathfrak{b}')$ by the validity of the chain condition for prime ideals, which implies height $\mathfrak{a}'$ + height $\mathfrak{b}' \geq r$, and the assertion is proved in this case. Assume now that I is not a field, and let p be a prime element of I. If p is in none of $\mathfrak{a}'$ and $\mathfrak{b}'$, then we see that altitude $R^*/(\mathfrak{a}'R^* + \sigma(\mathfrak{b}')R^*) =$ depth $\mathfrak{a}'$ + depth $\mathfrak{b}' - 1$ by (42.7), and we see the assertion similarly. If p is in both $\mathfrak{a}'$ and $\mathfrak{b}'$, then considering R/pR instead of R, we prove the assertion easily and we see in this case that height $\mathfrak{p} + 1 \leq$ height $\mathfrak{a}'$ + height $\mathfrak{b}'$. Assume that $p \in \mathfrak{a}'$ and that $p \notin \mathfrak{b}'$. Then, set $\mathfrak{b}'' = pR + \mathfrak{b}'$. Then height $\mathfrak{b}'' =$ altitude $\mathfrak{b}'' =$ height $\mathfrak{b}' + 1$ by (9.2), and height $\mathfrak{p} + 1 \leq$ height $\mathfrak{a}'$ + height $\mathfrak{b}''$ by the case stated just above, which proves this case. Thus the formula for heights is proved completely. Now we prove the last formula. Let $\mathfrak{p}$ be a minimal prime divisor of $\mathfrak{a} + \mathfrak{b}$ such that height $\mathfrak{p} =$ altitude $(\mathfrak{a} + \mathfrak{b})$ and let $\mathfrak{a}^*$ and $\mathfrak{b}^*$ be minimal prime divisors of $\mathfrak{a}$ and $\mathfrak{b}$, respectively, which are contained in $\mathfrak{p}$. Since $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}^* + \mathfrak{b}^*$, whence altitude $(\mathfrak{a} + \mathfrak{b}) =$ height $\mathfrak{p} \leq$ height $\mathfrak{a}^*$ + height $\mathfrak{b}^* \leq$ altitude $\mathfrak{a}$ + altitude $\mathfrak{b}$, and the assertion is proved.

Next we consider tensor products of normal rings. We begin with the following lemma:

(42.9) *Let R be a normal ring which contains a field K. If a field L is separably generated over K, and if $L \otimes_K R$ is an integral domain, then $L \otimes_K R$ is a normal ring.*

Proof. $L \otimes_K R$ is the union of all $L' \otimes R$ with finitely generated subfields L', so we may assume that L is finitely generated over K. Then L has a separating transcendence base $x_1, \ldots, x_n$ over K. Set $R' = R[x_1, \ldots, x_n]$, $K' = K(x_1, \ldots, x_n)$ (with regard to the fact that K and R are subrings of $L \otimes R$). Since the x_i are algebraically independent over R and since R is a normal ring, R' is a normal ring. Since $K'[R]$ is a ring of quotients of R', we see that $K'[R]$ is a normal ring. Since every element of L is a root of a monic polynomial over K' (hence over $K'[R]$) whose discriminant is a unit in K' (hence in $K'[R]$), we see that $L[R] = L \otimes R$ is a normal ring by (10.15).

(42.10) THEOREM. *Let R and R' be normal rings which contain a field K. If R and R' are separably generated over K and if $R \otimes R'$ is an integral domain, then $R \otimes R'$ is a normal ring.*

Proof. Let L and L' be the fields of quotients of R and R', respec-

tively. $L \otimes R'$ and $R \otimes L'$ are normal rings by (12.9). Therefore it suffices to show that $(L \otimes R') \cap (R \otimes L') = R \otimes R'$. Let $\{u_\lambda\}$ and $\{u'_{\lambda'}\}$ be linearly independent bases of R and R' over K, and let $\{v_\mu\}$ and $\{v'_{\mu'}\}$ be linearly independent bases of L and L' over K which contain $\{u_\lambda\}$ and $\{u'_{\lambda'}\}$, respectively. Then every element b of $L \otimes L'$ is expressed uniquely in the form $\sum a_{\mu\mu'} v_\mu \otimes v'_{\mu'}$ $(a_{\mu\mu'} \in K)$. If b is in $L \otimes R'$, then in this expression $v'_{\mu'}$ is in $\{u'_{\lambda'}\}$ for every μ' such that $a_{\mu\mu'} \neq 0$ (for some μ): if b is in $R \otimes L'$, then v_μ is in $\{u_\lambda\}$ for every μ such that $a_{\mu\mu'} \neq 0$ (for some μ'). Therefore, if b is in $(L \otimes R') \cap (R \otimes L')$, then the expression must be of the form $\sum a_{\lambda\lambda'} u_\lambda \otimes u'_{\lambda'}$, which implies that $b \in R \otimes R'$. Thus $(L \otimes R') \cap (R \otimes L') = R \otimes R'$, and the proof is complete.

The analogue of (42.10) does not hold in general for tensor products over a ring which is not a field, even if the ring is a Noetherian valuation ring. A generalization in that case can be stated as follows:

(42.11) THEOREM. *Let R and R' be normal Noetherian rings which contain a Noetherian valuation ring I with a prime element x. Assume that $R^* = R \otimes_I R'$ is a Noetherian integral domain and that both R and R' are separably generated over I. Then R^* is a normal ring if and only if $R^*_{\mathfrak{p}^*}$ is a normal ring for every prime divisor $\mathfrak{p}^*$ of xR^*.*

Proof. The *only if* part is obvious and we prove the *if* part. Let K be the field of quotients of I. Then $K = I[1/x]$ and $R^*[1/x] = R[1/x] \otimes_I R'[1/x] = R[1/x] \otimes_K R'[1/x]$. Thus $R^*[1/x]$ is a normal ring by (42.10), which implies that R^* is a normal ring by virtue of (35.4).

(42.12) COROLLARY. *Let R and R' be as above and assume furthermore that for every prime divisor $\mathfrak{p}$ of xR, $R/\mathfrak{p}$ is separably generated over I/xI and that $xR_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Then $R \otimes_I R'$ is a normal ring.*

This follows immediately from (42.11) and the following:

(42.13) *Let K' and L be fields which contain a field K. If L is separably generated over K, then $K' \otimes_K L$ has no nilpotent element except zero.*

Proof. By the definition of tensor products, we may assume that L is finitely generated over K, whence L has a separating transcendence base $u_1, \ldots, u_n$ over K. Then $K' \otimes_K L$ has the same total quotient ring with $K'(u) \otimes_{K(u)} L$, and we may assume that L is algebraic over K. Let a be such that $L = K(a)$. Then a is a root of

a separable monic polynomial $f(x)$ over K, and $K' \otimes L$ is isomorphic to $K'[x]/f(x)K'[x]$. Therefore we prove the assertion.

Lastly, we introduce the notion of an order of inseparability, which is of geometric interest. We begin with the following lemma:

(42.14) *Let R and R' be rings such that R' is an R-module. If, for any finite number of elements of R', there is a free R-module containing these elements and contained in R', then $\otimes_R R'$ is exact. In particular, if R contains a Noetherian valuation ring I, if I' is a ring containing I and such that every non-zero element of I is not a zero divisor in I', and if $R' = R \otimes_I I'$, then $\otimes_R R'$ is exact.*

The proof is straightforward and we omit it.

Assume that fields K' and L have a common subfield K and that one of K' and L is a function field over K. Let $\mathfrak{p}^*$ be a prime ideal of the local tensor product $L^* = L \times_K K'$ and set $m = \text{length } L^*_{\mathfrak{p}^*}$. Then, obviously m is uniquely determined by the fields K, K', L and $L^*/\mathfrak{p}^*$. This m is called the *order of inseparability of the pair (K', L) over K with respect to $L^*/\mathfrak{p}^*$, and is denoted by* $i_K(L, K'; L^*/\mathfrak{p}^*)$. Note that if L' is a field composed of L and K' and if either trans. $\deg_K L = $ trans. $\deg_{K'} L' < \infty$ or trans. $\deg_K K' = $ trans. $\deg_L L' < \infty$, then L' is naturally isomorphic to $L^*/\mathfrak{p}^*$ (with regard to the composition) with a suitable $\mathfrak{p}^*$ and the order of inseparability $i_K(L, K'; L')$ is well defined. Note also that the above condition on the transcendence degrees is equivalent to the two conditions that trans. $\deg_K L = $ trans. $\deg_{K'} L'$ and trans. $\deg_K K' = $ trans. $\deg_L L'$.

(42.15) (1) *If one of K', L is separably generated over K, then $i_K(L, K'; L^*/\mathfrak{p}^*) = 1$.* (2) *If K is of characteristic $p \neq 0$, then $i_K(L, K'; L^*/\mathfrak{p}^*)$ is a power of p.* (3) *If K is of characteristic $p \neq 0$, if K' contains $K^{1/p}$, and if $i_K(L, K'; L^*/\mathfrak{p}^*) = 1$, then L is separably generated over K.*

Proof. (1) is immediate from (42.13). As for (2), we may assume by symmetry that L is a function field over K. Let L'' be a subfield of L such that L'' is separably generated over K and such that L is purely inseparable over L''. Then $L'' \times K'$ has no nilpotent elements, whence $(L'' \times K')_{\mathfrak{p}''}$ is a field $K'(L'')$, where $\mathfrak{p}'' = \mathfrak{p}^* \cap (L'' \times K')$. Obviously, $K'(L'') \otimes_{L''} L$ is a local ring and coincides with $L^*_{\mathfrak{p}^*}$. Therefore $i_K(L, K'; L^*/\mathfrak{p}^*) \cdot [L^*/\mathfrak{p}^* : K'(L'')] = \text{length}_{K'(L'')} L^*_{\mathfrak{p}^*} = [L : L'']$, and we prove (2). As for (3), we see that $L \otimes K^{1/p}$ has no nilpotent elements, and is a local ring, whence it is a field, hence the assertion is proved.

(42.16) THEOREM. *Let K, K', L, L^* and $\mathfrak{p}^*$ be as above. Assume that $(I, \mathfrak{q})$ is a Noetherian valuation ring such that $K = I/\mathfrak{q}$ (I may coincide with K). Assume also that $(R, \mathfrak{m})$ and $(I', \mathfrak{q}')$ are local rings which dominate I such that $L = R/\mathfrak{m}$, $K' = I'/\mathfrak{q}'$, $\mathfrak{q}'/\mathfrak{q}I'$ is nilpotent and such that no non-zero element of I is a zero divisor in I'. Let $\mathfrak{P}^*$ be the prime ideal of $R^* = R \otimes_I I'$ such that $\mathfrak{P}^*/(\mathfrak{m}R^* + \mathfrak{q}'R^*) = \mathfrak{p}^*$. Then, for every primary ideal $\mathfrak{n}$ of R belonging to $\mathfrak{m}$, we have*

$$\mu(\mathfrak{n}R^*_{\mathfrak{P}^*}) = (\text{length } I'/\mathfrak{q}I') \cdot i_K(L, K'; L^*/\mathfrak{p}^*) \cdot \mu(\mathfrak{n}),$$

$$\text{length } (R^*_{\mathfrak{P}^*}/\mathfrak{n}R^*_{\mathfrak{P}^*}) = (\text{length } I'/\mathfrak{q}I') \cdot i_K(L, K'; L^*/\mathfrak{p}^*) \cdot \text{length } (R/\mathfrak{n})$$

If $R \times_I I'$ is Noetherian, hence in particular if one of R and I' is of finitely generated type over I, then R^* may be replaced by $R \times_I I'$.

Proof. $R^{**} = R \times_I I'$ is a ring of quotients of $R^{***} = R \otimes_I I'$. $\otimes_R R^{***}$ is exact by (42.14), whence $\otimes_R R^{**}$ is exact. Let $\mathfrak{P}^{**}$ be the prime ideal of R^{**} such that $\mathfrak{P}^{**}R^* = \mathfrak{P}^*$. Then we see that $\otimes_R (R^{**}_{\mathfrak{P}^{**}})$ is exact, whence $\otimes_{R/\mathfrak{n}} (R^{**}_{\mathfrak{P}^{**}}/\mathfrak{n}R^{**}_{\mathfrak{P}^{**}})$ is exact by (18.10). Since $R^{**}_{\mathfrak{P}^{**}}/\mathfrak{n}R^{**}_{\mathfrak{P}^{**}} = R^*_{\mathfrak{P}^*}/\mathfrak{n}R^*_{\mathfrak{P}^*}$ and since the above is true for any $\mathfrak{n}$, we see that the theorem of transition holds for R and $R^*_{\mathfrak{P}^*}$ by virtue of (19.1), hence $\mu(\mathfrak{n}R^*_{\mathfrak{P}^*}) = (\text{length } R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*}) \cdot \mu(\mathfrak{n})$ and

$$\text{length } (R^*_{\mathfrak{P}^*}/\mathfrak{n}R^*_{\mathfrak{P}^*}) = (\text{length } R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*}) \cdot \text{length } (R/\mathfrak{n}).$$

If the same is applied to K, $I'/\mathfrak{q}I'$ and L instead of I, R and I', respectively, then we have length $R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*} = \mu(0 \cdot R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*}) =$ length $(R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*})/\mathfrak{q}'(R^*_{\mathfrak{P}^*}/\mathfrak{m}R^*_{\mathfrak{P}^*}) \cdot \mu(0 \cdot I'/\mathfrak{q}I') = i_K(L, K'; L^*/\mathfrak{p}^*) \cdot$ length $I'/\mathfrak{q}I'$, and the equalities are proved. The last remark is obvious.

(42.17) THEOREM. *Assume that $L' = K'(L)$ is the field described just before (42.15). If K'' is a field between K and K', then $i_K(L, K''; K''(L))$ and $i_{K''}(K''(L), K'; L')$ are well defined, and we have $i_K(L, K'; L') = i_K(L, K''; K''(L)) \cdot i_{K''}(K''(L), K'; L')$.*

Proof. Since trans. deg$_K$ $L \geq$ trans. deg$_{K''}$ $K''(L) \geq$ trans. deg$_{K'}$ L', we have trans. deg$_K$ $L =$ trans. deg$_{K''}$ $K''(L) =$ trans. deg$_{K'}$ L'. Since trans. deg$_K K'' \geq$ trans. deg$_L$ K'' (L) and since trans. deg$_{K''}$ $K' \geq$ trans. deg$_{K''(L)}$ L', we see that the above inequalities are equalities. Therefore the first assertion is proved. Let $\mathfrak{p}^*$ be the prime ideal of $L^* = L \times K'$ such that $L' = L^*/\mathfrak{p}^*$ and set $L^{**} = L \times K''$, $\mathfrak{p}^{**} =$

$\mathfrak{P}^* \cap L^{**}$. Then we apply (42.16) to $R = L_{\mathfrak{P}^{**}}^{**}$, $n = 0$ and $l' = K'$, K there being K'' here. Then R^* there becomes $R \otimes K'$, which is a ring of quotients of L^*, whence $R_{\mathfrak{P}^*}^*$ there coincides with our $L_{\mathfrak{P}^*}^*$. Therefore $i_K(L, K'; L') \cdot \text{length } L_{\mathfrak{P}^*}^*$ (left-hand side of the equality in (42.16)) $= i_{K''}(L, K'; L') \cdot \text{length } R = i_{K''}(L, K'; L') \cdot i_K(L, K''; K''(L))$, which completes the proof.

(42.18) COROLLARY. *Assume furthermore that K' is a Galois extension of K. Let K'' be a maximal purely inseparable subextension of K' over K. Then $i_K(L, K'; K'(L))$ is independent of the choice of the composed field $K'(L)$ and is equal to $i_K(L, K''; K''(L))$.*

In this case, $i_K(L, K'; K'(L))$ may be denoted by $i_K(L, K')$.

Proof. Since K' is a Galois extension of K, we see that K' is separable over K'', whence the equality $i_K(L, K'; K'(L)) = i_K(L, K''; K''(L))$ follows from (42.17). Since K'' is purely inseparable, there is only one composed field $K''(L)$ of K'' and L, and the proof is complete.

Assume that L is a function field over the field K and let K^* be the algebraic closure of K. Then $i_K(L, K^*)$ is well defined; it is called the *order of inseparability* of L over K, and is denoted by $[L:K]_i$.

(42.19) *Let L be a function field over a field K of characteristic $p \neq 0$. If $[L:K]_i = p^m \neq 1$, then $i_K(L, K^{1/p}) > 1$ (hence $\geq p$) and $L(K^{p^{-m}})$ is separably generated over $K^{p^{-m}}$, i.e., $i_K(L, K^{p^{-m}}) = p^m$.*

Proof. Since L is not separably generated over K, $L \otimes K^{1/p}$ is not an integral domain, and $i_K(L, K^{1/p}) > 1$, hence the order of inseparability of $L(K^{1/p})$ over $K^{1/p}$ is p^n with $n < m$, hence by induction we complete the proof.

(42.20) *Assume furthermore that $L = K(x_1, \ldots, x_{r+1})$ and that* trans. $\deg_K L = r$. *Let m be such that $[L:K]_i = p^m$. Let F, G, H be the irreducible polynomials in indeterminates $X_1, \ldots, X_{r+1}$ for $(x_1, \ldots, x_{r+1})$ over K, $K^{p^{-m}}$, the algebraic closure K^* of K respectively. Then we have, except for constant factors, $F = G^{p^m}$ and $G = HH'$ with a polynomial H' over K^* such that $H'(x_1, \ldots, x_{r+1}) \neq 0$.*

Proof. Set $A = K[X_1, \ldots, X_{r+1}]$, $A' = K^{p^{-m}}[X_1, \ldots, X_{r+1}]$, and $A^* = K^*[X_1, \ldots, X_{r+1}]$. length $L \otimes K^{p^{-m}} = p^m$ by (42.19) and $L \otimes K^{p^{-m}}$ is a ring of quotients of A'/FA'. Therefore we see that $FA' = G^{p^m}A'$ because $K^{p^{-m}}$ is purely inseparable over K, which proves the first factorization. Since $L(K^{p^{-m}})$ is separably generated over $K^{p^{-m}}$ by (42.19), GA^* is semi-prime, and we prove the last factorization.

EXERCISES. *1.* Generalize (42.6) to the case where K is a common subfield of R and R' such that residue class fields of R and R' are finitely generated over K.

2. Generalize (42.7) to the case where I is a valuation ring dominated by R and R' and such that $R \otimes_I R'$ is defined.

3. Assume that L, L' are function fields over a field K such that $L \subseteq L'$, and let K^* be the algebraic closure of K. Prove that $[L':K]_i/[L:K]_i = [L':L]_i \div [K^*(L'):K^*(L)]_i = i_L(L', K^*(L); K^*(L'))$.

4. Generalize the last half of (42.14) to the case where I is a Dedekind domain.

CHAPTER VII

Henselian Rings and Weierstrass Rings

43. Henselization

We begin with a supplementary remark to Galois theory, discussed in §41.

(43.1) *Let R be a normal ring, let R' be an almost finite separable Galois extension of R with Galois group G, let $\mathfrak{p}$ be a prime ideal of R and let $\mathfrak{p}_1', \ldots, \mathfrak{p}_n'$ be all of the prime ideals in R' which lie over $\mathfrak{p}$. Let R'' be the splitting ring of $\mathfrak{p}_1'$ and set $\mathfrak{p}'' = \mathfrak{p}_1' \cap R''$. Then:* (1) *if $a \in R''$ is in $\mathfrak{p}_1'$ and is not in any of $\mathfrak{p}_2', \ldots, \mathfrak{p}_n'$, then a is a root of an irreducible monic polynomial $f(x) = x^r + c_1x^{r-1} + \cdots + c_r$ such that $c_r \in \mathfrak{p}$, $c_{r-1} \notin \mathfrak{p}$ and $R''_{\mathfrak{p}''}$ is a ring of quotients of $R[a]$ and* (2) *if $b \in R''$ is not in $\mathfrak{p}_1'$ and is in all of $\mathfrak{p}_2', \ldots, \mathfrak{p}_r'$, then b is a root of an irreducible monic polynomial $g(x) = x^r + d_1x^{r-1} + \cdots + d_r$ such that $d_1 \notin \mathfrak{p}$, $d_2, \ldots, d_r \in \mathfrak{p}$ and $R''_{\mathfrak{p}''}$ is a ring of quotients of $R[b]$.*

Proof. $\mathfrak{p}''$ is unramified over R by (41.2), whence the assertions follows from (38.6).

By virtue of the above result, we have the following lemma which will be generalized later:

(43.2) *Let $\mathfrak{p}$ be a prime ideal of a normal ring R. Then the following four conditions are equivalent to each other:*

(1) *$R_{\mathfrak{p}}$ is a Henselian ring.*

(2) *Every integral extension of R has only one prime ideal which lies over $\mathfrak{p}$.*

(3) *Every monic polynomial $f(x) = x + c_1x^{r-1} + \cdots + c_r$ over R, such that $c_r \in \mathfrak{p}$ and $c_{r-1} \notin \mathfrak{p}$, has a linear factor $x + a$ with $a \in \mathfrak{p}$.*

(4) *Every monic polynomial $g(x) = x^r + d_1x^{r-1} + \cdots + d_r$ over R, such that $d_1 \notin \mathfrak{p}$, and $d_2, \ldots, d_r \in \mathfrak{p}$, has a linear factor $x + b$ with b such that $b - d_1 \in \mathfrak{p}$.*

Proof. We note that, denoting by S the complement of $\mathfrak{p}$ in R, the set of integral extensions of $R_{\mathfrak{p}}$ coincides with the set of R_S' where

R' runs over all integral extensions of R. Therefore (2) follows from (1) by virtue of (30.5). Conversely, if $R_{\mathfrak{p}}$ is not Henselian, then there is an irreducible monic polynomial $F(x)$ over $R_{\mathfrak{p}}$ such that $F(x)$ modulo $\mathfrak{p}R_{\mathfrak{p}}[x]$ splits into two factors which have no common root. Then $R_{\mathfrak{p}}[x]/(F(x)R_{\mathfrak{p}}[x])$ is an integral extension of $R_{\mathfrak{p}}$ which is not quasi-local, whence the integral closure of R in that integral extension of $R_{\mathfrak{p}}$ has at least two prime ideals which lie over $\mathfrak{p}$. Thus (1) and (2) are equivalent to each other. By the same reason, we see that non-validity of one of (3), (4) implies the non-validity of (2). Conversely, assume that (2) is not true; let R^* be a separable integral extension of R which has at least two prime ideals $\mathfrak{p}_1^*$, $\mathfrak{p}_2^*$ which lie over $\mathfrak{p}$. Let a be an element of $\mathfrak{p}_1^*$ which is not in $\mathfrak{p}_2^*$ and consider an almost finite Galois extension R' of R which contains a. Then (43.1) implies the non-validity of (3) and (4). Therefore the assertion is proved completely.

When R is an integral domain, the *separable integral closure* of R is the set of separably algebraic elements which are integral over R (in a fixed algebraic closure).

Now we shall define the notion of *Henselization*.

We consider first the case of normal rings: Let R be a quasi-local normal ring. Let R' be the separable integral closure of R and let $\mathfrak{p}'$ be a maximal ideal of R'. Let R'' be the splitting ring of $\mathfrak{p}'$ and set $\mathfrak{p}'' = R'' \cap \mathfrak{p}'$. Then $R''_{\mathfrak{p}''}$ is uniquely determined up to isomorphisms over R, for, if H is the splitting group of $\mathfrak{p}'$ and if $\mathfrak{p}_1'$ is another maximal ideal of R', then $\mathfrak{p}_1' = \mathfrak{p}'^{\sigma}$ with an element σ of the Galois group G of R' by (10.12) and the splitting group of $\mathfrak{p}_1'$ is $\sigma^{-1}H\sigma$. This $R''_{\mathfrak{p}''}$ is called the Henselization of R.

Now we consider the general case. Let R be a quasi-local ring. Then there is a normal quasi-local ring S which has an ideal $\mathfrak{a}$ such that $S/\mathfrak{a}$ is isomorphic to R. Let S^* be the Henselization of S. Then $S^*/\mathfrak{a}S^*$ is uniquely determined up to isomorphism over $S/\mathfrak{a}$ as will be shown below, hence, identifying $S/\mathfrak{a}$ with R, we call $S^*/\mathfrak{a}S^*$ the Henselization of R.

Before proving the uniqueness, we note that:

(43.3) *If R^* is a Henselization of a quasi-local ring $(R, \mathfrak{m})$, then R^* is a Henselian ring. Furthermore $R/\mathfrak{m} = R^*/\mathfrak{m}R^*$ and R^* is unramified over R.*

Proof. The last assertion follows from (41.2) in the normal case, whence in the general case by the definition. If R is normal, then

we prove the first assertion by the definition and by (43.2), whence the general case follows from the following obvious fact:

(43.4) *Every homomorphic image of a Henselian ring is a Henselian ring.*

In order to prove the uniqueness of a Henselization of R, we prove the following theorem:

(43.5) THEOREM. *If a Henselian ring H dominates a quasi-local ring R, then there is one and only one R-homomorphism ϕ from a given Henselization R^* of R into H such that $\phi(R^*) \leq H$. If R is a normal ring, then ϕ is an isomorphism.*

Proof. Let S be the normal ring which is employed in order to define R^* and let $\mathfrak{a}$ be the ideal such that $R = S/\mathfrak{a}$. Let S^* be the Henselization of S. Let F be the set of pairs (T, σ) of subrings T of S^* and homomorphisms σ such that: (1) T is a quasi-local normal ring dominated by S^* and dominating S and (2) σ is a homomorphism from T into H whose restriction on S coincides with the natural homomorphism from S onto R and such that $\sigma(T) \leq H$. Let F' be the subset of F consisting of such (T, σ) that $(T, \sigma) \in F$ and $(T, \sigma') \in F$ imply $\sigma = \sigma'$. Defining $(T, \sigma) \geq (T', \sigma')$ if $T \supseteq T'$ and if the restriction of σ on T' coincides with σ', we make F' an ordered set. Then it is easily seen that F' is an inductive set, whence there is a maximal member (T^*, σ^*) of F'. Assume that $S^* \neq T^*$. Then, by the definition of the Henselization of a normal quasi-local ring, we see that the separable integral closure of T^* has at least two maximal ideals, whence T^* is not Henselian by (43.2). Therefore there is an irreducible monic polynomial $f(x) = x^r + a_1x^{r-1} + \cdots + a_r$ over T^* such that a_r is in the maximal ideal $\mathfrak{M}^*$ of T^* and a_{r-1} is not. Since H is Henselian, there is a root a' of $\sigma^*(f(x))$ such that a' is in the maximal ideal $\mathfrak{m}$ of H, whence $\sigma^*(f(x)) = (x - a')g^*(x)$ with a monic polynomial $g^*(x)$ such that $g^*(0) \notin \mathfrak{m}$. By the existence of a', we can extend σ^* to a homomorphism σ^{**} from $T^{**} = T^*[a]_{(\mathfrak{M}^*+aT^*[a])}$ into H so that $\sigma^{**}(a) = a'$, a being a root of $f(x)$ which is in the maximal ideal of S^*. Thus $(T^{**}, \sigma^{**}) \in F$. By the maximality of (T^*, σ^*), there is a $(T^{**}, \sigma'') \in F$ such that $\sigma'' \neq \sigma^{**}$. Since $(T^*, \sigma^*) \in F'$, the restriction of σ'' on T^* must be σ^*. Therefore $\sigma'' \neq \sigma^{**}$ implies $\sigma''(a) \neq a'$. Since a is in the maximal ideal of T^{**}, $\sigma''(a)$ must be in $\mathfrak{m}$, hence $g^*(\sigma''(a))$ is a unit in H. Since $f(a) = 0$, it follows that $\sigma''(a) - a' = 0$, which is a contradiction. Thus $T^* = S^*$, and the existence and the uniqueness of ϕ are proved completely.

Now we assume that R is normal. We consider the case where $R \subset S$. Then S^* is an integral domain which is algebraic over R. Therefore an ideal $\mathfrak{a}^*$ of S^* is zero if and only if $\mathfrak{a}^* \cap R = 0$. Applying this fact to the kernel of ϕ, we see that ϕ is an isomorphism. Thus the proof is completed by the following proof of the uniqueness of Henselization:

Proof of the uniqueness of Henselization: Let R^* and R^{**} be Henselizations of R. Then, applying (43.5) with $R^{**} = H$, we see that there is a homomorphism ϕ from R^* into R^{**} and, symmetrically, that there is a homomorphism ϕ' from R^{**} into R^*. Then $\phi \cdot \phi'$ is a homomorphism from R^{**} into itself. Since there is the identity map, the uniqueness in (43.5) implies that $\phi \cdot \phi' = 1$, and symmetrically $\phi' \cdot \phi = 1$. Therefore we see that ϕ and ϕ' are isomorphisms.

Next we note that:

(43.6) *If $f(x)$ is a monic polynomial over a ring R and if R' is a ring of quotients of $R[x]/f(x)R[x]$, then $\otimes_R R'$ is exact.*

Proof. $R[x]/f(x)R[x]$ is a free R-module, whence $\otimes_R (R[x]/f(x)R[x])$ is exact. Since $\otimes_{R[x]/f(x)R[x]} R'$ is exact, we prove the assertion.

On the other hand, it is obvious that:

(43.7) *Let a ring R' be a module over a ring R. If, for any finite number of elements $a_1, \ldots, a_n$ of R', there is a submodule R'' which contains $a_1, \ldots, a_n$ such that $\otimes_R R''$ is exact, then $\otimes_R R'$ is exact.*

Now we come to an interesting result:

(43.8) THEOREM. *Let R be a quasi-local ring and let R^* be its Henselization. Then $\otimes_R R^*$ is exact.*

Proof. If R is normal, then the assertion is obvious by (43.1), (43.6), and (43.7), whence the general case follows from the definition and (18.10).

(43.9) *Let $(R, \mathfrak{m})$ be a quasi-local ring and let R^* be its Henselization. For a finite number of elements b_i of R^*, there is an element α of $\mathfrak{m}R^*$ which is a root of a monic polynomial $f(x) = x^r + c_1 x^{r-1} + \cdots + c_r$ over R with $c_{r-1} \notin \mathfrak{m}$, $c_r \in \mathfrak{m}$, such that the ring $R' = R[\alpha]_{(\mathfrak{m}+\alpha R[\alpha])}$ contains b_i. R^* is the Henselization of R'.*

Proof. Let $(S, \mathfrak{M})$ be a normal quasi-local ring which has an ideal $\mathfrak{a}$ such that $R = S/\mathfrak{a}$. Let T be the separable integral closure of S and let $\mathfrak{p}$ be a maximal ideal of T. Let T' be the splitting ring of $\mathfrak{p}$ and set $\mathfrak{p}' = \mathfrak{p} \cap T'$. Then $S^* = T'_{\mathfrak{p}'}$ is the Henselization of S, and $R^* = S^*/\mathfrak{a}S^*$. Let b_i' be an element of S^* whose residue class modulo $\mathfrak{a}S^*$ is b_i for each i and let S' be an almost finite separable Galois extension of S containing all the b_i'. Let S'' be the splitting ring of $\mathfrak{p} \cap S'$ and

let a' be an element of $\mathfrak{p} \cap S''$ which is not in any other maximal ideal of S''. Then $a \equiv a' \bmod \mathfrak{a}S^*$ is the required element by virtue of (43.1). Assume next that there is an a as stated in the assertion. Let $F(x)$ be a monic polynomial over S such that $F(x) \bmod \mathfrak{a} = f(x)$. Let a' be a root of $F(x)$ such that $a' \in \mathfrak{M}S^*$ (the existence follows from the fact that S^* is Henselian). Then $U = S[a']_{(\mathfrak{M}+a'S[a'])}$ is a normal ring by virtue of (38.10) and is dominated by S^*. Let U^* be the Henselization of U. Since U and S are normal, we see that $U^* = S^*$ by (43.5). Therefore $R^* = S^*/\mathfrak{a}S^* = U^*/\mathfrak{a}U^*$ is the Henselization of $U/(\mathfrak{a}S^* \cap U) = R[a]_{(\mathfrak{m}+aR[a])}$.

(43.10) THEOREM. *If $(R, \mathfrak{m})$ is a local ring, then its Henselization R^* is a local ring and contains R as a dense subspace.*

Proof. $R^*/\mathfrak{m}R^* = R/\mathfrak{m}$ by the construction. Since $\otimes_R R^*$ is exact, we have $\mathfrak{m}^n R^* \cap R = \mathfrak{m}^n$ by (18.3). Assume that $b \in \bigcap \mathfrak{m}^n R^*$. Let a be as in (43.9) applied to this b. Then $R' = R[a]_{(\mathfrak{m}+aR[a])}$ is Noetherian, whence $\bigcap \mathfrak{m}^n R' = 0$. Since R^* is the Henselization of R', $\otimes_{R'} R^*$ is exact, which implies that $\mathfrak{m}^n R^* \cap R' = \mathfrak{m}^n R'$, whence $b \in \bigcap \mathfrak{m}^n R' = 0$. Thus $b = 0$ and R^* is a local ring which may not be Noetherian. Therefore the facts remarked at the beginning imply that R is a dense subspace of R^*. Now we want to prove that R^* is Noetherian. Since the maximal ideal of R^* is $\mathfrak{m}R^*$, it has a finite basis. Let R^{**} be the completion of R^*. Then R^{**} is the completion of R by what we have proved above. Let $\mathfrak{b}^*$ be an ideal of R^* which has a finite basis, say $b_1, \ldots, b_s$ and let c be an arbitrary element of $\mathfrak{b}^* R^{**} \cap R^*$. Let a be as in (43.9), applied to $c, b_1, \ldots, b_s$. Then, since R^* is the Henselization of $R' = R[a]_{(\mathfrak{m}+aR[a])}$, R^{**} is the completion of R', and since R' is Noetherian, $c \in \mathfrak{b}^* R^{**} \cap R' = (\sum b_i R^{**}) \cap R' = \sum b_i R'$, whence $c \in \sum b_i R^*$. Thus $\mathfrak{b}^*$ is a closed subset of R^*, and therefore R^* is Noetherian by (31.8).

Now we derive some properties of Henselian rings.

(43.11) *Let R be a Henselian ring. Then the Henselization of R coincides with R, whence R is a homomorphic image of a Henselian normal ring.*

Proof. Let R^* be the Henselization of R. Then there is a unique homomorphism ϕ from R^* into R by (43.5). ϕ is a homomorphism from R^* into R^*, whence by the uniqueness, ϕ must be the identity, and $R^* = R$.

(43.12) THEOREM. *A quasi-local integral domain R is Henselian if and only if every integral extension of R is quasi-local.*

Proof. The *only if* part was proved in §30, and we have to prove the *if* part. But we are not giving any complete proof here, because a complete proof can be given easily using (43.15) below.

(43.13) Corollary. *If R is a Henselian integral domain and if R' is an integral extension of R, then R' is Henselian.*

In order to adapt (43.12) and to generalize (43.13) to non-integral domains, we prove the following:

(43.14) Theorem. *Let $(R, \mathfrak{m})$ be a quasi-local ring and let $f(x)$ be a monic polynomial in an indeterminate x. Set $R^* = R[x]/fR[x]$. If $g(x)$ and $h(x)$ are monic polynomials such that $gh = f$ and such that g, h modulo $\mathfrak{m}$ have no common root, then R^* is the direct sum of gR^* and hR^*. Conversely, if R^* is the direct sum of ideals $\mathfrak{a}$ and $\mathfrak{b}$, then there are g and h as above and such that $\mathfrak{a} = gR^*$, $\mathfrak{b} = hR^*$.*

Proof. We note first that since R^* is integral over R, every maximal ideal $\mathfrak{m}^*$ of R^* lies over $\mathfrak{m}$, hence the Jacobson radical of R^* contains $\mathfrak{m}R^*$. Now, since g, h modulo $\mathfrak{m}$ have no common root, we see that they generate $R^*/\mathfrak{m}R^*$, which proves by virtue of the above remark that $gR^* + hR^* = R^*$, hence $gR^* \cap hR^* = ghR^* = fR^* = 0$ by (1.3). It follows that R^* is the direct sum of gR^* and hR^*. Conversely, assume that R^* is the direct sum of ideals $\mathfrak{a}$ and $\mathfrak{b}$. Set $x^* = x$ modulo $fR[x]$. Let ϕ be the natural homomorphism from R^* onto $R^*/\mathfrak{m}R^*$. Since $R^*/\mathfrak{m}R^*$ is a homomorphic image of the Euclidean ring $(R/\mathfrak{m})[x]$, there are monic polynomials g'', h'' in $\phi(x^*)$ over $R/\mathfrak{m}$ such that $\phi(\mathfrak{a}) = g''(R^*/\mathfrak{m}R^*)$, $\phi(\mathfrak{b}) = h''(R^*/\mathfrak{m}R^*)$. Let r and s be the degrees of g'' and h'', respectively, and let g^* and h^* be polynomials in x^* over R such that $\phi(g^*) = g''$, $\phi(h^*) = h''$, $g^* \in \mathfrak{a}$ and such that $h^* \in \mathfrak{b}$. Set $A = \sum_0^{s-1} x^{*i} g^* R^*$, $B = \sum_0^{r-1} x^{*i} h^* R^*$. Since the $r + s$ polynomials g'', $\phi(x^*)g''$, $\dots$, $\phi(x^*)^{s-1}g''$, h'', $\dots$, $\dots$, $\phi(x^*)^{r-1}h''$ form a linearly independent base of $\phi(R^*)$ over $R/\mathfrak{m}$, it follows that $A + B + \mathfrak{m}R^* = R^*$. Since R^* is a finite R-module, we see that $A + B = R^*$ by the lemma of Krull-Azumaya, whence $A = \mathfrak{a}$, $B = \mathfrak{b}$, and $x^{*s}g^* = \sum_0^{s-1} a_i x^{*i} g^*$. Set $h = x^s - \sum_0^{s-1} a_i x^i$. Then $h(x^*)g^*R^* = 0$, and $h(x^*)R^* \subseteq 0 : \mathfrak{a} = \mathfrak{b}$. Since $\phi(x^*)^i h''$ $(i = 0, \dots, r-1)$ form a linearly independent base of $\phi(\mathfrak{b})$ over $R/\mathfrak{m}$ and since they are monic polynomials of mutually distinct degrees, we see that $\phi(h(x^*)) = h''$. Thus we may employ $h(x^*)$ instead of h^* above. Similarly, we may assume that $g(x^*) = g^*$. Since $g(x^*)h(x^*)R^* = 0$, i.e., $gh \in fR[x]$ and since f is of degree $r + s$, we

see that $gh \equiv f$. Since $R^*/\mathfrak{m}R^*$ is the direct sum of $\phi(\mathfrak{a})$ and $\phi(\mathfrak{b})$, we see that g, h modulo $\mathfrak{m}$ have no common root, and the assertion is proved completely.

(43.15) THEOREM. *A quasi-local ring $(R, \mathfrak{m})$ is Henselian if and only if every ring R', which contains R and is a finite module over R, is the direct sum of a finite number of quasi-local rings.*

Proof. We want to prove the *if* part first: Let $f(x)$ be a monic polynomial over R such that $f(x)$ modulo $\mathfrak{m}$ splits into a product of two polynomials g'', h'' which have no common root. $R^* = R[x]/f(x)R[x]$is the direct sum of quasi-local rings $(R_1, \mathfrak{m}_1), \ldots, (R_n, \mathfrak{m}_n)$ by our assumption. Let the maximal ideals of R^* be $\mathfrak{m}_1^*, \ldots, \mathfrak{m}_n^*$ $(\mathfrak{m}_i^* R_i = \mathfrak{m}_i)$. We may assume that $g'' \in \mathfrak{m}_i^*/\mathfrak{m}R^*$ if and only if $i \leq r$. Then, as is easily seen, $\mathfrak{a} = R_1 + \cdots + R_r$ and $\mathfrak{b} = R_{r+1} + \cdots + R_n$ are such that $\mathfrak{a}$ modulo $\mathfrak{m}R^*$ and $\mathfrak{b}$ modulo $\mathfrak{m}R^*$ are generated by g'' and h'', whence we see the factorization $f = gh$ such that g modulo $\mathfrak{m} = g''$, h modulo $\mathfrak{m} = h''$ by virtue of (43.14). We shall prove the converse. Assume therefore that R is Henselian. Let $\mathfrak{m}_1', \ldots, \mathfrak{m}_n'$ be the maximal ideals of R'. Considering direct summands of R', we may assume that R' is not a direct sum of two rings. We have only to prove that $n = 1$. Assume for a moment that $n \geq 2$. Let a be an element of $\mathfrak{m}_1'$ which is not in $\mathfrak{m}_2'$. Set $R'' = R[a]$. Since R' is integral over R'', $\mathfrak{m}_i' \cap R''$ is maximal, whence R'' is not quasi-local. Let $f(x)$ be a monic polynomial over R which has a as a root. Then the maximal ideals of $R^* = R[x]/f(x)$ corresponds in a one to one way to the mutually distinct irreducible factors of f modulo $\mathfrak{m}$, it follows that R^* is the direct sum of quasi-local rings by (43.14). Since R'' is a homomorphic image of R^*, we see that R'' is the direct sum of quasi-local rings, whence R'' has an idempotent e which is not the identity, and $e \in R'$, which implies that R' is the direct sum of eR' and $(1 - e)R'$ and we have a contradiction. Thus $n = 1$, and the assertion is proved completely.

(43.16) COROLLARY. *If R is a Henselian ring and if a quasi-local ring R' is integral over R, then R' is Henselian.*

(43.17) THEOREM. *Assume that a quasi-local ring $(R', \mathfrak{m}')$ is integral over a quasi-local ring $(R, \mathfrak{m})$. If R^* is the Henselization of R, the $R' \otimes_R R^*$ is the Henselization of R'.*

Proof. Every maximal ideal of $R' \otimes R^*$ contains $\mathfrak{m}(R' \otimes R^*)$ because of integral dependence. Since $(R' \otimes R^*)/\mathfrak{m}(R' \otimes R^*) =$

$(R', \mathfrak{m}R') \otimes (R, \mathfrak{m}) \quad R'/\mathfrak{m}R'$, we see that $R' \otimes R^*$ is quasi-local, whence $R' \otimes R^*$ is Henselian by (43.16). Let R'^* be the Henselization of R'. Then there is an R-homomorphism ϕ from R^* into R'^* by (43.5). Let R'' be the subring of R'^* generated by $\phi(R^*)$ and R'. Then R'' is Henselian because R'' is a homomorphic image of $R' \otimes R^*$. Therefore we must have $R'' = R'^*$ and R'^* is a homomorphic image of $R' \otimes R^*$. Since there is one and only one R'-homomorphism from R'^* into $R' \otimes R^*$ by (43.5), we see that R'^* and $R' \otimes R^*$ must be isomorphic, and the proof is complete.

(43.18) THEOREM. *Assume that a quasi-local ring $(R', \mathfrak{m}')$ dominates a quasi-local ring $(R, \mathfrak{m})$ and that R' is of finite type over R. Then the Henselization R'^* of R' is a finite module over the Henselization R^* of R.*

Proof. R'^* dominates R', whence it dominates R, too. Therefore there is a uniquely determined R-homomorphism ϕ from R^* into R'^* by (43.5). Let $a_1, \ldots, a_n$ be elements of R' such that they are integral over R and such that R' is a ring of quotients of $R[a_1, \ldots, a_n]$. Let R^{**} be the subring of R'^* generated by the a_i over $\phi(R^*)$. Then R^{**} is Henselian by (43.16), and we see that $R^{**} = R'^*$ by virtue of (43.5). Thus R'^* is a finite module over $\phi(R^*)$, and the assertion is proved.

In order to investigate Henselizations of quasi-local integral domains, we prove the following auxiliary result:

(43.19) *Let $(R, \mathfrak{m})$ be a quasi-local normal ring and let $\mathfrak{p}$ be a prime ideal of R. Let R' be an almost finite separable Galois extension of R with Galois group G and let $\mathfrak{m}'$ be a maximal ideal of R'. Let R'' be the splitting ring of $\mathfrak{m}'$, set $\mathfrak{m}'' = \mathfrak{m}' \cap R''$ and set $R^* = R''_{\mathfrak{m}''}$. Let $\mathfrak{p}^*$ be an arbitrary prime divisor of $\mathfrak{p}R^*$ and let S be the complement of $\mathfrak{p}$ in R. Then:* (1) $\mathfrak{p}^* \cap R = \mathfrak{p}$, (2) $\mathfrak{p}^*$ *is unramified over* R, (3) $R^*_S/\mathfrak{p}R^*_S$ *is Noetherian, and* (4) $\mathfrak{p}R^*$ *is semi-prime.*

Proof. Let a be an element of $\mathfrak{m}''$ which is not in any maximal ideal of R'' other than $\mathfrak{m}''$ and let $f(x)$ be the irreducible monic polynomial for a over R. R^* is a ring of quotients of $R[a]$ by (43.1), whence $\otimes_R R^*$ is exact by (43.6). Therefore no element of S is a zero divisor modulo $\mathfrak{p}R^*$ by (18.1), which proves (1). By the choice of a, a (modulo $\mathfrak{p}^*$) is a simple root of $f(x)$ modulo $\mathfrak{p}$, hence (2) is true by (38.6) and by the fact that R^* is a ring of quotients of $R[a]$. Furthermore, $R^*_S/\mathfrak{p}R^*_S$ is a ring of quotients of a Noetherian ring

$$(R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}})[x]/\mathfrak{f},$$

where $\mathfrak{f}$ is the ideal generated by f modulo $\mathfrak{p}$, which proves (3). Since $\mathfrak{p}^*$ is arbitrary, (2) and (3) imply (4). Thus the assertion is proved completely.

Now we come to the following interesting result:

(43.20) THEOREM. *Let $(R, \mathfrak{m})$ be a quasi-local integral domain and let R^* be the Henselization of R. Then:* (1) *a prime ideal $\mathfrak{p}^*$ of R^* is a prime divisor of zero if and only if $\mathfrak{p}^* \cap R = 0$,* (2) *the zero ideal of R^* is semi-prime, and* (3) *there is a one to one correspondence between maximal ideals of the derived normal ring R' of R and prime divisors of zero of R^*.*

Proof. Since $\otimes_R R^*$ is exact by (43.7), every prime divisor of zero in R^* lies over zero of R by (18.11). Since R^* is a ring of quotients of a ring which is integral over R, every prime ideal of R^* which lies over zero of R is a minimal prime divisor of zero, and therefore (1) is true. Let T be a normal quasi-local ring which has a prime ideal $\mathfrak{p}$ such that $T/\mathfrak{p} = R$. Let U be the separable integral closure of T and let T^* be the Henselization of T which is defined by employing a maximal ideal $\mathfrak{u}$. Since $R^* = T^*/\mathfrak{p}T^*$ by definition, we want to prove (2) and (3) in terms of T^* and $\mathfrak{p}$. Assume that an element a of T^* is nilpotent modulo $\mathfrak{p}T^*$. Let T' be an almost finite separable Galois extension of T containing a, set $\mathfrak{M}' = \mathfrak{u} \cap T'$ and let T'' be the splitting ring of $\mathfrak{M}'$. Then $T''_{(\mathfrak{M}' \cap T'')} \leq T^*$. Since $\mathfrak{p}T''_{(\mathfrak{M}' \cap T'')}$ is semi-prime by (43.19), we have $a \in \mathfrak{p}T''_{(\mathfrak{M}' \cap T'')}$, whence $a \in \mathfrak{p}T^*$. Thus $\mathfrak{p}T^*$ is semi-prime, which proves (2). Let G be the Galois group of U over T, let H be the splitting group of $\mathfrak{u}$, and let U' be the splitting ring of $\mathfrak{u}$, whence $T^* = U'_{(\mathfrak{u} \cap U')}$. On the other hand, let $\mathfrak{q}$ be a prime ideal of U which lies over $\mathfrak{p}$ and let K and I be the splitting group and the inertia group respectively, of $\mathfrak{q}$. Then the Galois group of $U/\mathfrak{q}$ over R' is K/I by (41.2). Therefore we see that:

(*) The set of maximal ideals $\mathfrak{v}$ of U which contain $\mathfrak{q}$ and such that $\mathfrak{v}/\mathfrak{q}$ contains a given maximal ideal $\mathfrak{m}'$ of R' is the set of $\mathfrak{u}^\sigma$ with $\sigma \in H\sigma(\mathfrak{m}')K$ with an element $\sigma(\mathfrak{m}')$ of G.

On the other hand, let $\mathfrak{p}^*$ be a prime divisor of $\mathfrak{p}T^*$ and set $\mathfrak{p}'' = \mathfrak{p}^* \cap U'$. Then it is easy to see that:

(**) The set of prime ideals of U which are contained in the maximal ideal $\mathfrak{u}$ and lie over $\mathfrak{p}''$ is the set of $\mathfrak{q}^\sigma$ with $\sigma \in K\tau(\mathfrak{p}^*)H$ with an element $\tau(\mathfrak{p}^*)$ of G.

Now, let $\mathfrak{p}^*$ correspond to the two-sided class $K\tau(\mathfrak{p}^*)H$ of G. Let σ^{-1} be an element of the two-sided class and let $\mathfrak{m}'$ be $(\mathfrak{u}^\sigma/\mathfrak{q}) \cap R'$.

By (*) and (**) we see that $\mathfrak{m}'$ is uniquely determined by $\mathfrak{p}^*$ and that this correspondence gives a one to one correspondence between the set of prime divisors $\mathfrak{p}^*$ of $\mathfrak{p}'R'^*$ and the set of maximal ideals $\mathfrak{m}'$ of R'. Thus the assertion is proved completely.

EXERCISES. *1.* Let R, R', R'', $\mathfrak{p}$, and $\mathfrak{p}'$ be as in (43.1) and let S be a normal ring such that $R \subseteq S \subseteq R'$. Let $\mathfrak{q}_1 = \mathfrak{p}' \cap S$, $\mathfrak{q}_2, \ldots, \mathfrak{q}_m$ be all the maximal ideals of S which lie over $\mathfrak{p}$. Prove that: (1) if a is an element of $\mathfrak{q}_1 \cap R''$ such that a is not in any of $\mathfrak{q}_2, \ldots, \mathfrak{q}_m$, then a is a root of a monic polynomial $x^r + c_1x^{r-1} + \cdots + c_r$ over R such that $c_r \in \mathfrak{p}$, $c_{r-1} \notin \mathfrak{p}$, and (2) if b is an element of $\mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_m \cap R''$ and if b is not in $\mathfrak{q}_1$, then b is a root of a monic polynomial $x^s + d_1x^{s-1} + \cdots + d_s$ over R such that $d_1 \notin \mathfrak{p}$, $d_2, \ldots, d_s \in \mathfrak{p}$.

2. With the notation in (43.20), assume that a maximal ideal $\mathfrak{m}'$ of R' corresponds to a prime divisor $\mathfrak{p}^*$ of zero in R^* by the correspondence given in the proof. Prove that the derived normal ring of $R^*/\mathfrak{p}^*$ is the Henselization of $R'_{\mathfrak{m}'}$.

3. Assume that R is a quasi-local integral domain and that the derived normal ring of R is quasi-local. Prove that if a Henselian ring H dominates R, then H dominates the Henselization of R.

4. Let V be a valuation ring and let V^* be the Henselization of V. Prove that V^* is a valuation ring, and that every principal ideal of V^* is generated by an element of V (or equivalently, that the value group of a valuation defined by V^* is naturally identical with that defined by V).

5. Let $\mathfrak{p}$ be a prime ideal of a Henselian valuation ring V. Prove that $V_{\mathfrak{p}}$ is Henselian.

44. Hensel lemma

We begin with the following corollary to (37.9):

(44.1) THEOREM. *If R is a Henselian pseudo-geometric analytically normal ring, then every finite integral extension R' of R is analytically irreducible and is algebraically closed in its completion R'^* (i.e., every element of R'^* which is algebraic over R' is already in R').*

Proof. Analytic irreducibility is an immediate consequence of (37.8). Let a be an element of R'^* which is algebraic over R'. Let $b \neq 0$ be an element of R' such that the element $ab = c$ is integral over R'. Then the completion of $R'[c]$ is $R'[c] \otimes_{R'} R'^*$ by (17.8). The first assertion, applied to $R'[c]$, implies that $R'[c]$ is analytically irreducible, and $R'[c] \otimes R'^*$ is an integral domain, which implies that $c \in R'$. Therefore a is in the field of quotients K of R' and $a \in K \cap R'^* = R'$ by (18.4), which proves the assertion.

(44.2) THEOREM. *If R is a pseudo-geometric local ring, then the Henselization R^* of R is pseudo-geometric.*

Proof. Let $\mathfrak{p}^*$ be an arbitrary prime ideal of R^* and set $\mathfrak{p} = \mathfrak{p}^* \cap R$. It is easy to see that every finite integral extension R^{**} of $R^*/\mathfrak{p}^*$ is generated over $R^*/\mathfrak{p}^*$ by a local ring R' which dominates $R/\mathfrak{p}$ and which is of finite type over $R/\mathfrak{p}$. Since R is pseudo-geometric, the derived normal ring of R' is of finite type over $R/\mathfrak{p}$. Let I be the derived normal ring of R^{**}. Then I is a Henselian normal ring and I dominates a ring of quotients J of the derived normal ring of R'. Then there is a uniquely determined J-homomorphism from the Henselization J^* of J into I by (43.5). Since J^* is a normal ring, our construction of J and I implies that $J^* = I$. Since J is of finite type over $R/\mathfrak{p}$, we see that J^* is a finite module over $R^*/\mathfrak{p}^*$ by (43.18), which proves that R^* is pseudo-geometric.

(44.3) COROLLARY. *Let R be a pseudo-geometric analytically normal ring and let R^* be the Henselization of R. Then every integral extension R' of R^* is analytically irreducible and is algebraically closed in its completion.*

We note that normal localities, over a field or a Dedekind domain which satisfies the finiteness condition for integral extensions, are pseudo-geometric analytically normal rings, as was proved in §37. This fact and (44.3) will be used in the proof of the following theorem which may be called the *Hensel lemma*:

(44.4) THEOREM. *Let $(R, \mathfrak{m})$ be a Henselian ring and let $f(x)$ be a polynomial over R in an indeterminate x. Assume that there are polynomials $h_0(x)$ and $g_0(x)$ over R such that:* (1) $f(x) - g_0(x)h_0(x) \in \mathfrak{m}R[x]$, (2) *$g_0$ modulo $\mathfrak{m}$ and h_0 modulo $\mathfrak{m}$ have no common root (i.e., $g_0R[x] + h_0R[x] + \mathfrak{m}R[x] = R[x]$), and* (3) *$g_0$ is a monic polynomial. Then $f(x)$ has a monic factor $g(x)$ such that $g - g_0 \in \mathfrak{m}R[x]$, and $f = gh$ with $h(x)$ such that $h - h_0 \in \mathfrak{m}R[x]$.*

Proof. R is a homomorphic image of a Henselian normal ring by (43.11), hence we may assume that R is a normal ring. Let I be the ring generated by the coefficients of f, g_0, and h_0 over the prime integral domain and let I' be the derived normal ring of I. Then since R is normal, I' is contained in R. On the other hand, since I is pseudo-geometric ring, so is I'. Set $P = I'_{(\mathfrak{m} \cap I')}$. Then P is a normal locality over the prime integral domain, whence it is analytically normal by (37.5). Let P^* be the Henselization of P and let P^{**} be the completion of P. Then there are g and h as in the assertion but with coefficients in P^{**} by (30.4). Since g is monic, the coefficients of g and h

are algebraic over I', hence over I'^*. I'^* is contained in R by (43.5), whence g and h are the required polynomials. Thus the proof is complete.

EXERCISE. Let $(R, \mathfrak{m})$ be a Henselian valuation ring and let $f(x)$ be a polynomial over R in an indeterminate x. Assume that $g(x)$, $h(x)$, $k(x)$, $a(x)$, $b(x)$, $c(x) \in R[x]$ and $d, e \in \mathfrak{m}$ are such that: (1) $f(x) - g_0(x)h_0(x) \mid k(x)$, (2) $g(x)$ is monic, (3) $a(x)g_0(x) + b(x)h_0(x) \equiv d + c(x)$, (4) e is nilpotent modulo dR, (5) $c(x) \in deR[x]$, and (6) $k(x) \in d^2eR[x]$. Prove that there are polynomials $g(x)$ and $h(x)$ over R such that $f(x) = g(x)h(x)$, $g(x)$ is monic and such that $g(x) - g_0(x)$ and $h(x) - h_0(x)$ are in $(deR_\mathfrak{p} \cap R)R[x]$, where $\mathfrak{p}$ is the minimal prime divisor of dR.

45. Convergent power series rings

We say that a ring R is a *Weierstrass ring* if R is a pseudo-geometric Henselian ring such that, for every prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ is a finite integral extension of a regular local ring.

We note first the following general property of Weierstrass rings:

(45.1) *If $\mathfrak{p}$ is a prime ideal of a Weierstrass ring R, then $\mathfrak{p}$ is analytically irreducible and $R/\mathfrak{p}$ is algebraically closed in its completion.*

This follows immediately from (44.3).

On the other hand, it is obvious that:

(45.2) *If R is a Weierstrass ring, then every ring which is a finite R-module is a Weierstrass ring.*

In order to introduce the notion of convergent power series, we introduce the notion of multiplicative valuations.

Let K be a field. A map v from K into the set of nonnegative real numbers is called a *multiplicative valuation* of K if it satisfies the following three conditions:

(1) $v(a) = 0$ if and only if $a = 0$.

(2) $v(ab) = v(a)v(b)$ for any $a, b \in K$.

(3) $v(a + b) \leq v(a) + v(b)$.

We note that if there is an isomorphism ϕ from K into the field of complex numbers, then v such that $v(a)$ is the absolute value of $\phi(a)$ is a multiplicative valuation of K. We note also that if v^* is an additive valuation of K whose value group can be imbedded in the additive group of real numbers, then, with a real number c such that $0 < c < 1$, the map v such that $v(a) = c^{v^*(a)}$ becomes a multiplicative valuation of K.

Let K be a field with a multiplicative valuation v, and let $x_1, \ldots, x_r$ be indeterminates. A formal power series $\sum a_{n_1 \cdots n_r} x_1^{n_1} \cdots x_r^{n_r}$

$K[[x_1, \ldots, x_r]]$ is called a *convergent power series* (with respect to v) if there are positive real numbers $r_1, \ldots, r_r, M$ such that $v(a_{n_1 \cdots n_t}) r_1^{n_1} \cdots r_r^{n_r} \leq M$ for every $(n_1, \ldots, n_r)$.

The set of convergent power series, in indeterminates $x_1, \ldots, x_t$, forms a subring of $K[[x_1, \ldots, x_r]]$, is called the *convergent power series ring* in the variables $x_1, \ldots, x_r$ over K, and is denoted by $K\langle\langle x_1, \ldots, x_r \rangle\rangle$. Note that if v is such that $v(a) = 1$ for every a $(\neq 0)$ of K, then $K\langle\langle x_1, \ldots, x_r \rangle\rangle = K[[x_1, \ldots, x_r]]$.

We note that, as is easily seen, an invertible linear transformation of the variables defines an automorphism of $K\langle\langle x_1, \ldots, x_n \rangle\rangle$.

(45.3) THEOREM. *Let K and $x_1, \ldots, x_r$ be as above. Let $f = \sum a_{d_1 \cdots d_r} x_1^{d_1} \cdots x_r^{d_r}$ be an element of $K[[x_1, \ldots, x_r]]$ such that $a_{0 \cdots 0i} = 0$ for $i = 0, 1, \ldots, n-1$ $(n \geq 1)$ and such that $a_{0 \cdots 0n} \neq 0$. Then for every element g of $K[[x_1, \ldots, x_r]]$, there is a uniquely determined element q of $K[[x_1, \ldots, x_r]]$ such that $g - qf$ is a polynomial in x_r of degree at most $n-1$ with coefficients in $K[[x_1, \ldots, x_{r-1}]]$. If f and g are convergent power series, then $q \in K\langle\langle x_1, \ldots, x_r \rangle\rangle$ and $g - qf$ is polynomial (of degree at most $n-1$) in x_r with coefficients in $K\langle\langle x_1, \ldots, x_{r-1} \rangle\rangle$.* (WEIERSTRASS PREPARATION THEOREM)

Proof. Set $R = K[[x_1, \ldots, x_r]]$. Since $R/(\sum_1^{r-1} x_i R + fR)$ is a K-module generated by $1, x_r, \ldots, x_r^{n-1}$ modulo $\sum_1^{r-1} x_i R + fR$, it follows from (30.6) that R is a module over $K[[x_1, \ldots, x_{r-1}, f]]$ generated by $1, x_r, \ldots, x_r^{n-1}$, which proves the existence of q. The uniqueness may be proved easily by induction on r (considering $R/x_1 R$ if $r \geq 2$). But for convenience in proving the last assertion, we give a more complicated proof of the uniqueness. (Also the existence may be proved in this fashion.)

We may assume that $a_{0 \cdots 0n} = 1$. Set $g = \sum b_{d_1 \cdots d_r} x_1^{d_1} \cdots x_r^{d_r}$, $q = \sum q_{d_1 \cdots d_r} x_1^{d_1} \cdots x_r^{d_r}$. Then, since $g - qf$ has no term of degree greater than $n-1$ in x_r, we see that

$$b_{d_1 \cdots d_r} = \sum_{i_1 \cdots i_r} a_{(d_1 - i_1) \cdots (d_r - i_r)} q_{i_1 \cdots i_r} \quad \text{if} \quad d_r \geq n.$$

We prove the uniqueness of $q_{d_1 \cdots d_r}$ by induction on $w(q_{d_1 \cdots d_r}) = d_r + (n+1) \cdot \sum_1^{r-1} d_i$. If $w(q_{d_1 \cdots d_r}) = 0$, then all d_i are zero, and the above condition implies that $b_{d_1 \cdots d_{r-1}(d_r+n)} = q_{d_1 \cdots d_r}$ because $a_{0 \cdots 0} = \cdots = a_{0 \cdots 0(n-1)} = 0$, $a_{0 \cdots 0n} = 1$. Assume that $q_{d_1 \cdots d_r}$ such that $w(q_{d_1 \cdots d_r}) < t$ are unique and consider a $q_{d_1 \cdots d_r}$ such that $w(q_{d_1 \cdots d_r}) = t$. Then, the condition

$$b_{d_1\cdots d_r}(d_r+n) \qquad \sum a_{(d_1-e_1)\cdots(d_{r-1}-e_{r-1})(d_r+n-e_r)}q_{e_1\cdots e_r},$$

gives $q_{d_1\cdots d_r}$ uniquely, and the uniqueness is proved. Now we assume that g and f are in $K\langle\langle x_1, \ldots, x_r\rangle\rangle$. Then there are positive real numbers M, y, and z such that

$$v(a_{d_1\cdots d_r})y^{d_1+\cdots+d_{r-1}}z^{d_r} \leq M, \qquad v(b_{d_1\cdots d_r})y^{d_1+\cdots+d_{r-1}}z^{d_r} \leq M$$

for every $(d_1, \ldots, d_r)$. Let N, y^*, z^* be positive real numbers such that $N \geq (3M/z^n) + 1$, $zz^* \geq (3M/z^n) + 1$, $1/yy^* \leq 1 - (1 + (zz^*)^{-(n+1)})^{-1/(r-1)}$. We want to prove that $v(q_{d_1\cdots d_r}) \leq Ny^{*d_1+\cdots+d_{r-1}}z^{*d_r}$ by induction on $w = w(q_{d_1\cdots d_r}) = d_r + (n+1)\times\sum_1^{r-1} d_i$. If $w = 0$, then we have $v(q_{d_1\cdots d_r}) = v(b_{d_1\cdots(d_r+n)}) < M/z^n < N$, and we consider the case where $w \geq 1$. By the equality $b_{d_1\cdots d_{r-1}(d_r+n)} = \sum a_{(d_1-i_1)\cdots(d_{r-1}-i_{r-1})(d_r+n-i_i)}q_{i_1\cdots i_r}$, we see that

$$v(q_{d_1\cdots d_r}) \leq$$

$$v(b_{d_1\cdots d_{r-1}(d_r+n)}) + \sum{}^* v(q_{e_1\cdots e_r})v(a_{(d-e_1)\cdots(d_{r-1}-e_{r-1})(d_r+n-e_r)}),$$

where $\sum^*$ is the sum of all possible terms except for the one with $(e_1, \ldots, e_r) = (d_1, \ldots, d_r)$.

$$\begin{aligned}
&\sum{}^* v(q_{e_1\cdots e_r})v(a_{(d-e_1)\cdots(d_{r-1}-e_{r-1})(d_r+n-e_r)}) \\
&\leq \sum_{e_i\leq d_i, t\leq d_r+n} MNy^{*e_1+\cdots+e_{r-1}}z^{*t}/y^{d_1+\cdots+d_{r-1}-e_1-\cdots-e_{r-1}}z^{d_r+n-t} \\
&\qquad - \sum_{t=d_r}^{d_r+n} MNy^{*d_1+\cdots+d_{r-1}}z^{*t}/z^{d_r+n-t} \\
&= (MN/y^{d_1+\cdots+d_{r-1}}z^{d_r+n})((zz^*)^{d_r+n+1} - 1)/(zz^* - 1) \\
&\qquad \times \prod_{i=1}^{r-1}[((yy^*)^{d_i+1} - 1)/(yy^* - 1)] \\
&\qquad - MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r}z^{-n}((zz^*)^{n+1} - 1)/(zz^* - 1) \\
&< MNy^{-d_1-\cdots-d_{r-1}}z^{-d_r-n}(yy^*)^{d_1+\cdots+d_{r-1}+r-1}(yy^* - 1)^{-r+1} \\
&\qquad \times (zz^*)^{d_r+n+1}(zz^* - 1)^{-1} \\
&\qquad - MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r}z^{-n}(zz^*)^{n+1}(zz^* - 1)^{-1} \\
&\qquad + MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r}z^{-n}(zz^* - 1)^{-1} \\
&= MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r+n+1}z(zz^* - 1)^{-1}[(1 - y^{-1}y^{*-1})^{-r+1} - 1]
\end{aligned}$$

$$
\begin{aligned}
&\cdots + MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r}y^{*n}(yy^*)^{n-1} \\
&+ MNy^{*d_1+\cdots+d_{r-1}}z^{*d_r+n}(zz^*)^{n-1} \\
&+ z^{*n-1}z^{n-3}M^{*}z^{n}(zz^*)^{n-1} \\
&+ z^{*n-1}z^{n-3}M^{*}z^{n}] \\
&= 2Ny^{*d_1+\cdots+d_{r-1}}z^{*d_r}/3.
\end{aligned}
$$

$$
\begin{aligned}
&v(b_{d_1\cdots d_{r-1}(d_r+n)}) \leq M/y^{d_1+\cdots+d_{r-1}}z^{d_r+n} \\
&= Ny^{*d_1+\cdots+d_{r-1}}z^{*d_r}\cdot M/z^{n}N(yy^*)^{d_1+\cdots+d_{r-1}}(zz^*)^{d_r} \\
&< Ny^{*d_1+\cdots+d_{r-1}}z^{*d_r}/3
\end{aligned}
$$

Thus we have $v(q_{d_1\cdots d_r}) \leq Ny^{*d_1+\cdots+d_{r-1}}z^{*d_r}$, and the assertion is proved.

As a corollary to (45.3), we have the following lemma:

(45.4) *Let $f(y)$ and $g(y)$ be monic polynomials in an indeterminate y over $K\ll x_1, \ldots, x_r\gg$. Assume that $f(y) = y^n + c_1y^{n-1} + \cdots + c_n$ with $c_1, \ldots, c_n \in \sum x_iK\ll x_1, \ldots, x_r\gg$. If $f(y)$ is a factor of $g(y)$ in $K\ll x_1, \ldots, x_r, y\gg$, then $f(y)$ is a factor of $g(y)$ in $K\ll x_1, \ldots, \ldots, x_r\gg[y]$.*

Proof. Let $h \in K\ll x_1, \ldots, x_r, y\gg$ be such that $g = fh$. On the other hand, let $q, s \in K\ll x_1, \ldots, x_r\gg[y]$ be such that $g = qf + s$ and such that s is of lower degree than f (in y). Then this q is the one in (45.3), applied to our f and g in $K\ll x_1, \ldots, x_r, y\gg$. By the uniqueness in (45.3), we have $h = q$, whence $r = 0$ and the assertion is proved.

(45.5) THEOREM. *With the same K and the x_i as above, we have:* (1) *$K\ll x_1, \ldots, x_r\gg$ is a Henselian regular local ring of altitude r, whence the completion of $K\ll x_1, \ldots, x_r\gg$ is $K[[x_1, \ldots, x_r]]$, and* (2) *if $\mathfrak{a}$ is an ideal of $K\ll x_1, \ldots, x_r\gg$, then $K\ll x_1, \ldots, x_r\gg/\mathfrak{a}$ contains $K\ll y_1, \ldots, y_s\gg$ with suitable variables y_i and is a finite module over $K\ll y_1, \ldots, y_s\gg$. Here, if K contains infinitely many elements, then the y_i can be linear combinations of the x_i with coefficients in K.* (NORMALIZATION THEOREM FOR CONVERGENT POWER SERIES RINGS)

Proof. If K contains only a finite number of elements, then $v(a) = 1$ for any $a \neq 0$, and $K\ll x_1, \ldots, x_r\gg = K[[x_1, \ldots, x_r]]$ in this case. Therefore the assertion in this case follows easily from the theory of complete local rings. Thus we assume that K contains infinitely many elements. Since $K\ll x_1, \ldots, x_r\gg/\sum_{i+1}^{r} x_iK\ll x_1, \ldots, x_r\gg = K\ll x_1, \ldots, x_i\gg$, we see that altitude $K\ll x_1, \ldots, x_r\gg \geq r$. There-

fore in order to prove the regularity, we have only to prove that $K\langle\langle x_1, \ldots, x_r\rangle\rangle$ is Noetherian. We shall prove it and (2) by induction on r. It is sufficient to show the assertion (2) and that $\mathfrak{a}$ has a finite base. If $\mathfrak{a} = 0$, then the assertions are obvious, and we assume that $\mathfrak{a} \neq 0$. Let $f \neq 0$ be an element of $\mathfrak{a}$. Then, by a suitable linear transformation of the variables, we may assume that f is of the form as in (45.3), whence $\mathfrak{a}/fK\langle\langle x_1, \ldots, x_r\rangle\rangle$ is an ideal of a ring R which contains $K\langle\langle x_1, \ldots, x_{r-1}\rangle\rangle$ and which is a finite module over $K\langle\langle x_1, \ldots, x_{r-1}\rangle\rangle$. Since R is Noetherian by induction, $\mathfrak{a}$ has a finite base. $K\langle\langle x_1, \ldots, x_r\rangle\rangle/\mathfrak{a}$ is a finite module over $K\langle\langle x_1, \ldots, \ldots, x_{r-1}\rangle\rangle/((\mathfrak{a} \text{ modulo } f) \cap K\langle\langle x_1, \ldots, x_{r-1}\rangle\rangle$, and (2) is proved by induction. Thus the regularity and (2) are proved. In order to prove that $K\langle\langle x_1, \ldots, x_r\rangle\rangle$ is Henselian, it is sufficient, by virtue of (43.2), to show that if $F(y) = y^n + c_1y^{n-1} + \cdots + c_n$ is such that $c_i \in K\langle\langle x_1, \ldots, x_r\rangle\rangle$, $c_n \in \sum x_iK\langle\langle x_1, \ldots, x_r\rangle\rangle$, and such that $c_{n-1} \notin \sum x_iK\langle\langle x_1, \ldots, x_r\rangle\rangle$, then $F(y)$ has a factor $y - g$ with $g \in \sum x_iK\langle\langle x_1, \ldots, x_r\rangle\rangle$. It follows from (45.3) (cf. Exercise 1, below) that $F(y)$ has such a factor in $K\langle\langle x_1, \ldots, x_r, y\rangle\rangle$, and the assertion is proved by (45.4). Thus the proof of (45.5) is complete.

The following corollary, together with (45.1), clarifies the relationship between formal and convergent power series rings.

(45.6) COROLLARY. *Assume that K is a perfect field. Then any ring which is a finite module over a convergent power series ring in a finite number of variables with coefficients in K is a Weierstrass ring.*

EXERCISES. *1.* With the notation of (45.3), prove that there are a monic polynomial $f^* = x_r^n + c_1x_r^{n-1} + \cdots + c_n$ with $c_i \in \sum_1^{r-1} x_iK\langle\langle x_1, \ldots, x_{r-1}\rangle\rangle$ and a unit q in $K\langle\langle x_1, \ldots, x_r\rangle\rangle$ such that $f^* = qf$.

2. Let a local ring R be a ring of quotients of a complete local ring. Prove that the Henselization of R is a Weierstrass ring.

3. Let K be a field of characteristic $p \neq 0$ and let $x_1, \ldots, x_r$ be indeterminates. Prove that $K\langle\langle x_1, \ldots, x_r\rangle\rangle$ is a Weierstrass ring if $[K:K^p]$ is finite.

4. Let I be a field or a pseudo-geometric Dedekind domain and let R be a locality over I. Prove that the Henselization of R is a Weierstrass ring.

5. Let R be a Weierstrass ring which has no nilpotent elements, and let R^* be the completion of R. Let a be a given element of R^*. Assume that for every minimal prime divisor $\mathfrak{p}^*$ of zero in R^*, a modulo $\mathfrak{p}^*$ is algebraic over $R/(\mathfrak{p}^* \cap R)$. Prove that a is an element of R.

46. Jacobian criterion of simple points

We begin with a remark on derivations of a local ring:

(46.1) *Let $(R, \mathfrak{m})$ be a local ring and let R' be a subring of R. As-*

same that a subset M of R generates a ring R'' over R' such that $R/\mathfrak{m} = R''/(\mathfrak{m} \cap R'')$. Let $f_1, \ldots, f_r$ be a basis for $\mathfrak{m}$. If D, D' are derivations of R over R' such that $Dm = D'm$ for all $m \in M$ and such that $Df_i = D'f_i$ for every i, then we have $D = D'$.

Proof. By the definition of derivations, we may assume that D and D' are integral derivations of R, whence $D\mathfrak{m}^n \subseteq \mathfrak{m}^{n-1}$, $D'\mathfrak{m}^n \subseteq \mathfrak{m}^{n-1}$. Since every element of R is expressed as a power series in the f_i with coefficients in R'', the above result implies that $Da = D'a$ for any $a \in R$.

Let $\mathfrak{a}$ be an ideal of a ring R and let D be a derivation of R. Assume that there is an element d of R, which is not a zero divisor modulo $\mathfrak{a}$, such that dD is an integral derivation of R and such that $dD\mathfrak{a} \subseteq \mathfrak{a}$. Then, denoting by ϕ the natural homomorphism from R onto $R/\mathfrak{a}$, we can define a uniquely determined derivation D' of $R/\mathfrak{a}$ such that $D'(\phi(x)) = \phi(dDx)/\phi(d)$ for every $x \in R$ (and D' is independent of the particular choice of d). The derivation obtained in this manner is called the derivation *induced* in $R/\mathfrak{a}$ by D.

When K is a field of characteristic $p \neq 0$ and if K^* is a subfield of K, then elements $z_1, \ldots, z_n$ of K are said to be *p-independent* over K^* if $[K^*(K^p)(z_1, \ldots, z_n) : K^*(K^p)] = p^n$.

(46.2) *Let $X_1, \ldots, X_r$ be indeterminates and let K be a field with a multiplicative valuation v. Let A be any one of $K[X_1, \ldots, X_r]$, $K[[X_1, \ldots, X_r]]$, and $K\langle\langle X_1, \ldots, X_r\rangle\rangle$. If K^* is a subfield of K such that $[K : K^*]$ is finite and if $\mathfrak{a}$ is an ideal $(\neq A)$ of A, then every derivation of $A/\mathfrak{a}$ over K^* is induced by a derivation of A over K^*.*

Proof. Assume first that K is of characteristic $p \neq 0$. Then every derivation of A or of $A/\mathfrak{a}$ is a derivation over K^p, and therefore we may assume that K^* contains K^p. Let $z_1, \ldots, z_n$ be p-independent elements of K over K^* such that $K = K^*(z_1, \ldots, z_n)$. Let D_i be the derivation of A over K^* such that $D_iX_j = 0$ for any j and such that $D_iz_i = 1$, $D_iz_j = 0$ if $i \neq j$. Let D' be an integral derivation of $R/\mathfrak{a}$ over K^*. Set $u_i' = D'z_i$ and $v_j' = D'x_j$, where $x_j = X_j$ modulo $\mathfrak{a}$. Let u_i and v_j be representatives of u_i' and v_j' in A and set $D = \sum u_iD_i + \sum v_j\partial/\partial X_j$. Then D induces D' by (46.1). Thus every integral derivation of $R/\mathfrak{a}$ over K^* is induced by an integral derivation of R over K^*, which proves the assertion in this case. Assume now that K is of characteristic 0. Then K is separably algebraic over K^*, whence we may assume that $K = K^*$, and we can prove the assertion in the same way as above using only the partial derivations $\partial/\partial X_i$.

With the same notation as above, if $f_1, \ldots, f_m$ are elements of A, then the matrix $(D_k f_i, f_i \partial X_k)$ (i and k for rows and j for columns) is called a *mixed Jacobian matrix* and is denoted by $J^*(f_1, \ldots, f_m; K^*)$. Note that $J^*(f_1, \ldots, f_m; K^*)$ is unique up to linear transformations and that $J^*(f_1, \ldots, f_m; K)$ is a Jacobian matrix.

We consider, from now on, the case where the f_i form a basis for $\mathfrak{a}$. Let $\mathfrak{p}$ be a prime divisor of $\mathfrak{a}$ and let $\mathfrak{q}$ be a prime ideal containing $\mathfrak{a}$. Set $R = A_{\mathfrak{q}}$. By the normalization theorems, we see that there are variables $y_1, \ldots, y_n$ such that $A/\mathfrak{q}$ is a finite integral extension of the ring A' which is of the same type as A but with variables y_i. Now we assert that:

(46.3) THEOREM. *When A' can be chosen so that $A/\mathfrak{q}$ is separable over A', then $R/\mathfrak{a}R$ is regular if and only if* rank $(J(f_1, \ldots, f_m)$ *modulo* $\mathfrak{q}) =$ height $\mathfrak{p}$. *When K is of characteristic $p \neq 0$, then $R/\mathfrak{a}R$ is regular if and only if there is a subfield K^* of K such that $[K:K^*]$ is finite and such that* rank $(J^*(f_1, \ldots, f_m; K^*)$ *modulo* $\mathfrak{q}) =$ height $\mathfrak{p}$.

Proof. We begin with a very special case where $\mathfrak{a} = \mathfrak{p} = \mathfrak{q}$. In this case $R/\mathfrak{a}R$ is a field, whence it is regular. Assume first that $A/\mathfrak{q}$ is separable over A'. (46.1) and the last half of (39.4) imply that $\mathfrak{Der}((A/\mathfrak{q})/K)$ is generated by the partial derivations of A', whence setting $x_i = X_i$ modulo $\mathfrak{q}$, we see that the set of vectors $(Dx_1, \ldots, Dx_r)$ with $D \in \mathfrak{Der}((A/\mathfrak{q})/K)$ is a vector space of dimension s over $R/\mathfrak{q}R$. Since $J(f_1, \ldots, f_m)$ modulo $\mathfrak{q}$ is the matrix of coefficients of linear equations of $(Dx_1, \ldots, Dx_r)$ by virtue of (46.2) (cf. (39.3)), we see that rank $(J(f_1, \ldots, f_m)$ modulo $\mathfrak{q}) = r - s =$ height $\mathfrak{q}$, which settles this case. Assume next that K is of characteristic $p \neq 0$. We need the following lemma:

(46.4) *Set $L' = R/\mathfrak{q}R$ and let L be a field such that $A' \subseteq L \subseteq L'$. Let K^* be a subfield of K such that $[K:K^*] < \infty$ and such that $K^p \subseteq K^*$. Then there is a subfield K^{**} of K^* such that $[K:K^{**}] < \infty$ and such that* length $\mathfrak{Der}(L'/L^{**}) =$ length $\mathfrak{Der}(L/L^{**})$, *where L^{**} is the field of quotients of A^{**} which is the ring of the same type as A with variables $y_1^p, \ldots, y_s^p$ over K^{**}.*

Proof. We use induction on $[L':L]$. If $[L':L] = 1$, then the assertion is obvious. Assume that $L' \neq L$. If a is an element of L' which is not in L, then, by our induction, there exists a field K^{**} ($K^{**} \subseteq K^*$, $[K:K^{**}] < \infty$) such that

$$\text{length } \mathfrak{Der}(L'/L^{**}) = \text{length } \mathfrak{Der}(L(a)/L^{**}).$$

If a is separable over L, then length $\mathfrak{Der}(L/L^{**}) =$ length

$\mathfrak{Der}(L(a)/L^{++})$ by (39.4), and the case is settled. Thus we may assume that L' is purely inseparable over L. Let a, as above, be such that $a^p \in L$. Since $a \notin L$, $a^p \notin L^p$. We may assume that $a \in A/\mathfrak{q}$. Let A^* and L^* be such as A^{**} and L^{**}, respectively, in the case where $K^{**} = K^*$. If $a^p \in L^*(L^p) = L^p(K^*)$, then, since $a^p \notin L^p$, we see that there is a field K^{**} ($K^p \subseteq K^{**} \subseteq K^*$, $[K:K^{**}] < \infty$) such that $a^p \notin L^{**}(L^p) = L^p(K^{**})$. Replacing then K^* with K^{**}, we may assume that $a^p \notin L^*(L^p)$. As was noted above, there is a field K^{**} ($K^{**} \subseteq K^*$, $[K:K^{**}] < \infty$) such that length $\mathfrak{Der}(L'/L^{**}) =$ length $\mathfrak{Der}(L(a)/L^{**})$. Since $a^p \in L$, a derivation D of L has an extension D'' to $L(a)$ if and only if $D(a^p) = 0$, and when that is so, $D''a$ can be assigned arbitrarily in $L(a)$ by (39.3). Hence

$$\text{length } \mathfrak{Der}(L(a)/L^{**}) = 1 + \text{length } \mathfrak{Der}(L/L^{**}(a^p)).$$

Since $a^p \notin L^*(L^p)$, we have $a^p \notin L^{**}(L^p)$ and

$$\text{length } \mathfrak{Der}(L/L^{**}) = 1 + \text{length } \mathfrak{Der}(L/L^{**}(a^p)).$$

Thus length $\mathfrak{Der}(L(a)/L^{**})$ = length $\mathfrak{Der}(L/L^{**})$. Therefore length $\mathfrak{Der}(L'/L^{**})$ = length $\mathfrak{Der}(L(a)/L^{**})$, which implies the required equality. Thus (46.4) is proved completely.

Now we go back to the proof of (46.3). Let K^{**}, A^{**} and L^{**} be as in (46.4), applied to the case where L is the field of quotients of A' and $K^* = K$. Let $z_1, \ldots, z_t$ be p-independent elements of K over K^{**} such that $K = K^{**}(z_1, \ldots, z_t)$, and consider the set of vectors $(Dx_1, \ldots, Dx_r, Dz_1, \ldots, Dz_t)$ with $D \in \mathfrak{Der}(L'/L^{**})$. Since length $\mathfrak{Der}(L/L^{**}) = s + t$ by the proof of (46.2), we have length $\mathfrak{Der}(L'/L^{**}) = s + t$, and therefore the rank of $J^*(f_1, \ldots, \ldots, f_m; K^{**}) = (r + t) - (s + t) = r - s =$ height $\mathfrak{q}$. Thus this case is settled.

Next we consider the general case. Let $g_1, \ldots, g_n$ be elements of $\mathfrak{q}$ such that $\mathfrak{a} + \sum g_i A = \mathfrak{q}$. Then the above result shows that $J(f, \ldots, f_m, g_1, \ldots, g_n)$ or $J^*(f_1, \ldots, f_m, g_1, \ldots, g_n; K^{**})$ modulo $\mathfrak{q}$ is of rank equal to height $\mathfrak{q}$. We treat here the second case, because the first case can be treated as a special case where $K = K^{**}$. Assume first that $R/\mathfrak{a}R$ is regular. Then there is a regular system of parameters $u_1, \ldots, u_b$ of R such that $u_1, \ldots, u_a$ generate $\mathfrak{a}R$ by virtue of (25.18). On the other hand, since $\mathfrak{p}$ is a prime divisor of $\mathfrak{a}$ contained in $\mathfrak{q}$, we have $\mathfrak{a}R = \mathfrak{p}R$. That rank $(J^*(f_1, \ldots, f_m, g_1, \ldots, \ldots, g_n; K^{**})$ modulo $\mathfrak{q}) = b$ implies that rank $(J^*(u_1, \ldots, u_b; K^{**})$ modulo $\mathfrak{q}) =$ height $\mathfrak{q} = b$, hence rank $(J^*(u_1, \ldots, u_a; K^{**})$ mod-

ulo q) a height p. Since $\mathfrak{a}R = \sum_1^a u_i R$, we have rank $(J^*(f_1, \ldots, f_m; K^{**})$ modulo q) height p. Conversely, assume that rank $(J^*(f_1, \ldots, f_m; K^{**})$ modulo q) height p. We may assume that rank $(J^*(f_1, \ldots, f_a; K^{**})$ modulo q) a height p. Assume that $c_1, \ldots, c_a$ are elements of R such that $\sum_1^a c_i f_i \in \mathfrak{q}^2 R$. Then for every integral derivation D of A, $D(\sum c_i f_i) \in \mathfrak{q}R$. But, $D(\sum c_i f_i) = \sum f_i Dc_i + \sum c_i Df_i = \sum c_i Df_i$ (modulo $\mathfrak{q}R$). Since $J^*(f_1, \ldots, f_a; K^{**})$ modulo q is of rank equal to a, we have $c_i \in \mathfrak{q}R$ for every i. Therefore there exists a regular system of parameters of R which contains $f_1, \ldots, f_a$ as a subset, whence $R/\sum_1^a f_i R$ is regular. Since a = height p, we have $\mathfrak{p}R = \sum_1^a f_i R$ whence $\mathfrak{a}R = \mathfrak{p}R$, and $R/\mathfrak{a}R$ is regular. Thus the proof is completed.

(46.5) COROLLARY. *Let I be a Noetherian valuation ring with a prime element p and let $x_1, \ldots, x_r$ be indeterminates. Let A be either $I[x_1, \ldots, x_r]$ or $I[[x_1, \ldots, x_r]]$, and let $f_1, \ldots, f_m$ be elements of A. Set $\mathfrak{a} = \sum f_i A$, let $\mathfrak{p}$ be a prime divisor of $\mathfrak{a}$ and let $\mathfrak{q}$ be a prime ideal of A containing $\mathfrak{p} + pA$. Set $R = A_{\mathfrak{q}}$. Assume that $\mathfrak{p} \cap I = 0$. If* rank $(J(f_1, \ldots, f_m)$ *modulo* $\mathfrak{q}) =$ height $\mathfrak{p}$, *then $R/\mathfrak{a}R$ is a regular local ring in which p is a member of a regular system of parameters. The converse is true if $A/\mathfrak{q}$ is a finite separable integral extension of a ring A' which is either the polynomial ring or the power series ring in some variables over I/pI.*

On the other hand, applying (46.3) to the case where $\mathfrak{a} = \mathfrak{p}$ and $A/\mathfrak{p}$ is a purely inseparable extension of a ring A'' which is of the same type as A, we see, at first that rank $(J^*(f_1, \ldots, f_m; K^{**})$ modulo $\mathfrak{p}) =$ height $\mathfrak{p}$, whence:

(46.6) COROLLARY. *If A is as in* (46.3) *and if A is pseudo-geometric, then A satisfies the condition for I in* (40.3).

Note that A may not be pseudo-geometric only when A is a convergent power series ring over a field K of characteristic $p \neq 0$ such that $[K:K^p] = \infty$ (cf. Exercise 3 in §45).

(46.7) COROLLARY. *A complete local ring satisfies the condition for I in* (40.3).

EXERCISES. *1.* Let $x_1, \ldots, x_r$ be indeterminates and let R be a ring. Prove that the partial derivations $\partial/\partial x_i$ generate $\mathfrak{Der}(R[[x_1, \ldots, x_r]]/R)$.

2. Let D be a derivation of a Zariski ring R. Prove that D can be extended uniquely to a derivation of the completion of R.

3. Let K be a field of characteristic $p \neq 0$, K' a finite algebraic extension of

K, and let K^* be a subfield of K such that $|K : K^*|$ is finite. Prove that there is a subfield K^{**} of K^* such that $|K : K^{**}| < \infty$ and such that length $\mathfrak{Der}(K/K^{**})$ = length $\mathfrak{Der}(K'/K^{**})$.

47. *Analytic tensor product*

Let K be a field with a multiplicative valuation v.

We say that a ring R is an *analytic ring* over K if there are indeterminates $x_1, \ldots, x_n$ and an ideal $\mathfrak{a}$ of $K\ll x_1, \ldots, x_n\gg$ such that $R \cong K\ll x_1, \ldots, x_n\gg/\mathfrak{a}$. The normalization theorem for convergent power series ring implies that a local ring R with coefficient field K is an analytic ring over K if and only if it is a finite module over a subring which is a convergent power series ring in a finite number of analytically independent elements over K.

An analytic integral domain R over K is said to be *analytically separably generated* over K if there is a system of parameters $x_1, \ldots, \ldots, x_r$ of R such that R is separable over $K\ll x_1, \ldots, x_r\gg$. This definition is applied also to complete local integral domains with a basic field considering $K[[x_1, \ldots, x_r]]$ instead of $K\ll x_1, \ldots, x_r\gg$.

Let R and R' be analytic rings over K. Then there are indeterminates $x_1, \ldots, x_n, y_1, \ldots, y_m$ such that $R \cong K\ll x_1, \ldots, x_n\gg/\mathfrak{a}$, $R' \cong K\ll y_1, \ldots, y_m\gg/\mathfrak{b}$ with suitable ideals $\mathfrak{a}$ and $\mathfrak{b}$. The analytic ring $K\ll x_1, \ldots, x_n, y_1, \ldots, y_m\gg/\mathfrak{c}$, with the ideal $\mathfrak{c}$ generated by $\mathfrak{a}$ and $\mathfrak{b}$, is uniquely determined within isomorphisms by R and R'. The new ring is called the *analytic tensor product* of R and R' (over K) and is denoted by $R \hat{\otimes} R'$. One sees immediately that:

(47.1) *The complete tensor product $R \overline{\otimes}_K R'$ is the completion of $R \hat{\otimes} R'$.*

In order to investigate analytic tensor products, we prove some results on complete tensor products over a field.

(47.2) THEOREM. *Let $(R, \mathfrak{m})$ be a complete local ring with a basic field K and let $(R', \mathfrak{m}')$ be a complete local ring which contains K. Let A be the total quotient ring of R'. Then $R' \overline{\otimes}_K R$ is naturally identified with a subring of $A \overline{\otimes}_K R$.*

Proof. Since K is a field, $\otimes_K R$ is exact, and $R' \otimes R \subseteq A \otimes R$. Let $\mathfrak{n}$ be the Jacobson radical of A. Since $\bigcap \mathfrak{n}^n = 0$, we see that, for each natural number m, there is an $n(m)$ such that $\mathfrak{n}^{n(m)} \bigcap R' \subseteq \mathfrak{m}'^m$ by (30.1). It follows that the topology on $R' \otimes R$ induced by $A \overline{\otimes} R$ is stronger than or equal to that induced by $R' \overline{\otimes} R$. Therefore there is a natural homomorphism from the closure B, of the

subring generated by R' and R in $L \supset R$, into $R' \supset R$. Since K is a basic field of R, R $\mathfrak{m}''$ is a finite K module, whence $R' \supset (R/\mathfrak{m}'')$ is a complete semi local ring, and, since $B/\mathfrak{m}''B \cong R' \supset (R/\mathfrak{m}'')$, B $\mathfrak{m}''B$ is complete. B is complete under $\mathfrak{m}B$ adic topology, and therefore B is a complete semi-local ring. Therefore, by the definition of a complete tensor product, there must be a natural homomorphism from $R' \otimes R$ onto B. Therefore we see that B is naturally identified with $R' \otimes R$, which completes the proof.

(47.3) THEOREM. *Assume that a complete local integral domain R is analytically separably generated over its basic field K. If R' is a complete local integral domain such that K is separably algebraically closed in the field of quotients L of R', then $R' \overline{\otimes}_K R$ is a complete local integral domain.*

Proof. We may assume, by virtue of (47.2), that $R' = L$. Let $x_1, \ldots, x_r$ be a system of parameters of R and let c be an element of R such that c is separable over $K[[x_1, \ldots, x_r]]$ and such that $K[[x_1, \ldots, x_r]][c]$ has the same field of quotients as R. Let $f(X)$ be the irreducible monic polynomial for c over $K[[x_1, \ldots, x_r]]$. We have only to show that $f(X)$ is irreducible over $L[[x_1, \ldots, x_r]]$. Assume the contrary and let $g(X)$ and $h(X)$ be monic factors of $f(X)$ such that $f = gh$. Coefficients of g and h are integral over $K[[x_1, \ldots, x_r]]$ (because so is c), whence they are in the integral closure of $K[[x_1, \ldots, \ldots, x_r]]$ in $L[[x_1, \ldots, x_r]]$. By our assumption on L, we see that the coefficients of g and h are in a suitable purely inseparable extension of $K[[x_1, \ldots, x_r]]$. Since c is separable over $K[[x_1, \ldots, x_r]]$, $f(X)$ is irreducible over any purely inseparable extension of $K[[x_1, \ldots, x_r]]$ by (39.9), which is a contradiction, and the proof is complete.

(47.4) COROLLARY. *If K is an algebraically closed field, if R is a complete local domain which has K as a basic field, and if R' is a complete local integral domain containing K, then $R' \overline{\otimes}_K R$ is a complete local integral domain.*

The above result yields the following by virtue of (47.1) and (45.6):

(47.5) THEOREM. *Let K be an algebraically closed field. If R and R' are analytic integral domains over K, then $R \hat{\otimes} R'$ is an analytic integral domain.*

Next we prove some lemmas.

(47.6) *If R is a Noetherian normal ring and if $x_1, \ldots, x_n$ are indeterminates, then $R[[x_1, \ldots, x_n]]$ is also a normal ring.*

Proof. We have only to prove the case where $n \geq 1$. On the other hand, $R = \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$ where $\mathfrak{p}$ runs over all prime ideals of height 1, whence $R[[x_1]] = \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}[[x_1]]$. Since $R_{\mathfrak{p}}$ is a valuation ring, $R_{\mathfrak{p}}[[x_1]]$ is a regular local ring, hence is a normal ring by (25.14). Therefore $R[[x_1]]$ is normal, which proves the assertion.

(47.7) *Let R and R' be semi-local rings containing a common field K and such that $R^* = R \overline{\otimes}_K R'$ is well defined. If $f \in R$ and if $f' \in R'$, then $fR^* \cap f'R^* = ff'R^*$.*

Proof. There is a linearly independent base of R over K containing such one of fR and the same is true for R' and fR'. Therefore we see easily that $f(R \otimes R') \cap f'(R \otimes R') = ff'(R \otimes R')$. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the Jacobson radicals of R and R', respectively, and apply the above fact to $R^*/(\mathfrak{m}^n R^* + \mathfrak{m}'^n R^*)$. We obtain that $(fR^* + \mathfrak{m}^n R^* + \mathfrak{m}'^n R^*) \cap (f'R^* + \mathfrak{m}^n R^* + \mathfrak{m}'^n R^*) = ff'R^* + \mathfrak{m}^n R^* + \mathfrak{m}'^n R^*$ for every natural number n. Therefore $fR^* \cap f'R^* \subseteq \bigcap_n (ff'R^* + \mathfrak{m}^n R^* + \mathfrak{m}'^n R^*)$. This last intersection coincides with $ff'R^*$ by (16.7), hence $fR^* \cap f'R^* \subseteq ff'R^*$, which proves the assertion. The same proof gives also the following lemma:

(47.8) *Let R and R' be analytic rings over a field K. If $f \in R$ and if $f' \in R'$, then, setting $R^* = R \hat{\otimes} R'$, we have $fR^* \cap f'R^* = ff'R^*$.*

Now we shall prove the following theorem:

(47.9) THEOREM. *Assume that R and R' are analytic rings over a field K. If R and R' are normal rings and are analytically separably generated over K and if $R \hat{\otimes} R'$ is an integral domain, then $R \hat{\otimes} R'$ is a normal ring.*

Proof. Let b be an arbitrary element of the derived normal ring of $R \hat{\otimes} R'$. Let $x_1, \ldots, x_r, c \in R$ be such that the x_i form a system of parameters of R, such that R is separable over $K\langle\langle x_1, \ldots, x_r\rangle\rangle$ and such that R has the same field of quotients as $K\langle\langle x_1, \ldots, x_r\rangle\rangle[c]$. Let d be the discriminant of the irreducible monic polynomial for c over $K\langle\langle x_1, \ldots, x_r\rangle\rangle$. Since $K\langle\langle x_1, \ldots, x_r\rangle\rangle \hat{\otimes} R'$ is a dense subspace of $R'[[x_1, \ldots, x_r]]$, and since this last ring is normal by (47.6), we see that $K\langle\langle x_1, \ldots, x_r\rangle\rangle \otimes R'$ is normal by (18.4). Since b is in the derived normal ring of $(K\langle\langle x_1, \ldots, x_r\rangle\rangle \hat{\otimes} R')[c]$, we see that db is in $(K\langle\langle x_1, \ldots, x_r\rangle\rangle \hat{\otimes} R')[c]$ by (10.15), whence $db \in R \hat{\otimes} R'$. Similarly, there is an element $d' \neq 0$ of R' such that $d'b \in R \hat{\otimes} R'$. Then $dd'b \in d(R \hat{\otimes} R') \cap d'(R \hat{\otimes} R')$. This last intersection coincides with $dd'(R \hat{\otimes} R')$ by (47.8), and therefore we see that $b \in R \hat{\otimes} R'$, which completes the proof.

(47.10) COROLLARY. *If R and R' are normal analytic rings over an algebraically closed field K, then $R \otimes_K R'$ is also normal.*

EXERCISES. *1.* Let R be a complete local integral domain with a basic field K. Prove that the following four conditions are equivalent to each other:

(i) R is analytically separably generated over K.

(ii) For any field K' which is a purely inseparable extension of K, $R \otimes_K K'$ is an integral domain.

(iii) The length of $\mathfrak{Der}(R/K)$ over the field of quotients of R coincides with altitude R.

(iv) For any complete local integral domain R' containing K, the ring $R \otimes_K R'$ has no nilpotent element except zero.

2. Let R be an analytic ring over a field K. Assume that R is analytically irreducible (as it is when K is perfect). Prove that R is analytically separably generated over K if and only if the completion of R is.

3. Let R be a complete local integral domain with a basic field K. Prove that the following two conditions are equivalent to each other:

(i) R is analytically separably generated over K and K is algebraically closed in the field of quotients of R.

(ii) For any complete local integral domain R' containing K, the ring $R \overline{\otimes}_K R'$ is a complete local integral domain.

4. Let R be a complete local integral domain with a basic field K.

(i) Prove that if R is analytically separably generated over K, then R is separably generated over K. Prove also that the converse is true if $[K : K^p]$ is finite, where p is the characteristic of K. Show by an example that the above converse is not true in general.

(ii) Prove that if R satisfies the conditions in Exercise 3 and if K' is a field containing K, then $R \overline{\otimes}_K K'$ satisfies the same conditions with K' instead of K.

5. Prove (47.6) without assuming that R is Noetherian.

Appendix

A1. Examples of bad Noetherian rings

EXAMPLE 1. *A Noetherian ring whose altitude is infinite.*

Let K be a field and let $x_1, \ldots, x_n, \ldots$ be infinitely many algebraically independent elements over K. Let $m_1, \ldots, m_i, \ldots$ be a sequence of natural numbers such that $0 < m_i - m_{i-1} < m_{i+1} - m_i$ for every i. Let $\mathfrak{p}_i$ be the prime ideal of $K[x_1, \ldots, x_n, \ldots]$ generated by all the x_j such that $m_i \leq j < m_{i+1}$, and let S be the intersection of complements of $\mathfrak{p}_i$ in $K[x_1, \ldots, x_n, \ldots]$. Then $R = K[x_1, \ldots, \ldots, x_n, \ldots]_S$ is the required example.

Proof. $R_{\mathfrak{p}_i R}$ is a Noetherian ring of altitude $m_{i+1} - m_i$, whence it is obvious that altitude $R = \infty$. That R is Noetherian follows from the following lemma:

(E1.1) *Let R be a ring. Assume that:* (1) *if $\mathfrak{m}$ is a maximal ideal of R, then $R_{\mathfrak{m}}$ is Noetherian and* (2) *if f is an element of R which is different from zero, then there is only a finite number of maximal ideals of R which contain f. Then R is Noetherian.*

Proof. Let $\mathfrak{a}$ be an arbitrary ideal of R such that $\mathfrak{a} \neq 0$. By our assumption, there is only a finite number of maximal ideals which contain $\mathfrak{a}$; let them be $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. There are finite number of elements $a_1, \ldots, a_s$ of $\mathfrak{a}$ such that there is no maximal ideal of R, other than the $\mathfrak{m}_i$, which contains all the a_j. Since each $R_{\mathfrak{m}_i}$ is Noetherian, there is a finite number of elements $a_{s+1}, \ldots, a_t$ of $\mathfrak{a}$ which generate $\mathfrak{a}R_{\mathfrak{m}_i}$ for every i. Then $\sum a_i R_{\mathfrak{m}} = \mathfrak{a}R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R. Therefore $\sum a_i R = \mathfrak{a}$ by (8.9). Thus $\mathfrak{a}$ has a finite basis and (E1.1) is proved.

We note by the way that the above result shows the following fact:

(E1.2) *Let $(R, \mathfrak{m}_1, \ldots, \mathfrak{m}_r)$ be a quasi-semi-local ring. If $R_{\mathfrak{m}_i}$ is Noetherian for every i, then R is Noetherian.*

EXAMPLE 2. *A local integral domain of multiplicity 1 which is not regular, which is at the same time an example of the chain condition for prime ideals.*

We first prove a lemma:

(32.1) *Let* $(R, \mathfrak{p}_1, \ldots, \mathfrak{p}_t)$ *be a semi local ring. Assume that* R *dominates a local ring* $(K, \mathfrak{m})$ *such that every* $R/\mathfrak{p}_i$ *is a finite algebraic extension of* $K/\mathfrak{m}$. *Let* $\mathfrak{j}$ *be the Jacobson radical of* R *and set* $S = K + \mathfrak{j}$. *Then* S *is a local ring and* R *is a finite* S *module, and* R *is integral over* S.

Proof. It is obvious that S is a ring. If $m \in \mathfrak{j}$, then $1/(1 + m) = 1 + m'$ for some m' of $\mathfrak{j}$, which implies that $\mathfrak{j}$ is the unique maximal ideal of S. Let $e_1, \ldots, e_t$ be elements of R whose residue classes modulo $\mathfrak{j}$ form a basis for $R/\mathfrak{j}$ over $K/\mathfrak{m} = S/\mathfrak{j}$. If $a \in R$, then a modulo $\mathfrak{j}$ is integral over $S/\mathfrak{j}$, whence a is integral over S (because $\mathfrak{j}$ is common). Thus R is integral over S. Therefore $S[e_1, \ldots, e_t, a]$ is a finite S-module. Furthermore $S[e_1, \ldots, e_t, a] = \sum e_i S + \mathfrak{j}S[e_1, \ldots, e_t, a]$ (because this last term is $\mathfrak{j}$), which implies that $\sum e_i S = S[e_1, \ldots, e_t, a]$ by the lemma of Krull-Azumaya. Since a is arbitrary, we see that $R = \sum e_i S$. Thus it remains only to prove that S is Noetherian. Let $\mathfrak{p}$ be an arbitrary prime ideal of S. Since R is integral over S, there is a prime ideal $\mathfrak{p}'$ of R which lies over $\mathfrak{p}$. Since $\mathfrak{j} \subseteq S$, we have $\mathfrak{p} = \mathfrak{p}' \cap \mathfrak{j}$. Therefore $\mathfrak{p}$ is an ideal of R, whence it has a finite basis, say $a_1, \ldots, a_n$ as an ideal of R. Let $\mathfrak{a}$ be the ideal of S generated by all the $a_i e_j$. Let b be an arbitrary element of $\mathfrak{p}$. Then $b = \sum c_i a_i$ with $c_i \in R$. Then $c_i = \sum d_{ij} e_j$ with $d_{ij} \in S$ and $b = \sum d_{ij} e_j a_i \in \mathfrak{a}$. Thus we see that $\mathfrak{a} = \mathfrak{p}$, and $\mathfrak{p}$ has a finite basis. Therefore S is Noetherian by the theorem of Cohen, and the proof is complete.

Now we construct a local integral domain R as follows:

Let K be a field and let x be an indeterminate. Consider the formal power series ring $K[[x]]$ and let $z_i = \sum a_{ij} x^j$ $(a_{ij} \in K;\ i = 1, 2, \cdots, r,\ r > 0)$ be algebraically independent elements over $K(x)$. Set $z_{ij} = (z_i - \sum_{k<j} a_{ik} x^k)/x^{j-1}$. Furthermore let $y_1, \ldots, y_m$ (there may be none) be algebraically independent elements over $K[x, z_1, \ldots, z_r]$. Let R_1 be the ring generated by all the z_{ij} and x over K and set $R_2 = R_1[y_1, \ldots, y_m]$.

Then xR_1 is a maximal ideal of R_1, because $xz_{i,j+1} = z_{ij} - a_{ij}x$, hence $z_{ij} \in xR_1$. Therefore $(R_1)_{xR_1}$ is dominated by $K[[x]]$, hence is a local ring which may not be Noetherian. Therefore $(R_1)_{xR_1}$ is a local ring by (31.5). Let $\mathfrak{m}$ be the ideal of R_2 generated by $x, y_1, \ldots, y_m$. $\mathfrak{m}$ is a maximal ideal of height $m + 1$ and $V = (R_2)_{\mathfrak{m}}$ is a regular local ring of altitude $m + 1$, because V is a ring of quotients of the Noetherian ring $(R_1)_{xR_1}[y_1, \ldots, y_m]$. $R_1[1/x] = K[x, 1/x, z_1, \ldots,$

$\ldots, z_r]$, hence the ideal $\mathfrak{n}$ of R_2 generated by $x-1, z_1, \ldots, z_r, y_1, \ldots, y_m$ is a maximal ideal of R_2 and the ring $W = (R_2)_{\mathfrak{n}}$ is a regular local ring of altitude $r+m+1$. Let S be the intersection of the complements of $\mathfrak{m}$ and $\mathfrak{n}$ in R_2 and set $R' = (R_2)_S$. The maximal ideals of R' are $\mathfrak{m}R'$ and $\mathfrak{n}R'$, and it holds that $V = R'_{\mathfrak{m}R'}$, $W = R'_{\mathfrak{n}R'}$. Therefore R' is Noetherian by (E1.2). Let $\mathfrak{j}$ be the Jacobson radical of R' and set $R = K + \mathfrak{j}$. Since $R'/\mathfrak{m}R' = R'/\mathfrak{n}R' = K$, we see that R is Noetherian and R' is the derived normal ring of R by (E2.1).

Thus the ring R is a local ring of altitude $r+m+1$ with maximal ideal $\mathfrak{j}$. The derived normal ring R' of R is a finite R-module, has two maximal ideals $\mathfrak{m}R'$ and $\mathfrak{n}R'$, and $\mathfrak{j} = \mathfrak{m}R' \cap \mathfrak{n}R'$. Furthermore $R'_{\mathfrak{m}R'}$ and $R'_{\mathfrak{n}R'}$ are regular local rings of altitudes $m+1$ and $r+m+1$, respectively.

Thus the chain condition for prime ideals is not satisfied by R, whence R is not unmixed. Furthermore $\mu(\mathfrak{j}) = \mu(\mathfrak{j}R') = \mu(\mathfrak{j}R'_{\mathfrak{n}R'}) = \mu(\mathfrak{n}R'_{\mathfrak{n}R'}) = 1$. Thus R is an example of a non-regular local integral domain of multiplicity one.

We note here that: (1) *if* $m = 0$, *then the first chain condition for prime ideals is satisfied by* R, *and* (2) *if* $m > 0$, *then* R *does not satisfy the first chain condition for prime ideals.*

Proof. Assume that $m = 0$. Then $\mathfrak{m}R'$ is of height 1, whence there is a one to one correspondence between prime ideals of $R'_{\mathfrak{n}R'}$ and those of R such that $\mathfrak{q}'$ corresponds to $\mathfrak{p}$ if and only if $\mathfrak{q}' \cap R = \mathfrak{q}$. Since $R'_{\mathfrak{n}R'}$ is regular, the chain condition is satisfied by $R'_{\mathfrak{n}R'}$, whence (1) is proved. Assume that $m > 0$. Set $\mathfrak{q} = xR' \cap R$. Then obviously $\mathfrak{q} = xR' \cap \mathfrak{n}R'$. Therefore $\mathfrak{q}R'_{\mathfrak{n}R'} = \mathfrak{n}R'_{\mathfrak{n}R'}$ (because $x \notin \mathfrak{n}R'$), which shows that there is no prime ideal of R' contained in $\mathfrak{n}R'$ which lies over $\mathfrak{q}$ (because, since $m > 0$, xR' is not a maximal ideal of R', hence $\mathfrak{q}$ is not a maximal ideal of R). Therefore we see that $R'_{xR'}$ is the derived normal ring of $R_{\mathfrak{q}}$, hence height $\mathfrak{q}$ = height $xR' = 1$. Now, let $0 \subset \mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_v$ be a maximal chain of prime ideals in R such that $\mathfrak{q}_1 = \mathfrak{q}$. Let $0 \subset \mathfrak{q}'_1 \subset \mathfrak{q}'_2 \subset \cdots \subset \mathfrak{q}'_v$ be a chain of prime ideals of R' such that $\mathfrak{q}'_i \cap R = \mathfrak{q}_i$ for every i. Then $\mathfrak{q}'_1 = xR'$ by what was proved above, and therefore each $\mathfrak{q}'_i$ is contained in $\mathfrak{m}R'$, whence $v \leq$ height $\mathfrak{m}R' = m+1 < m+r+1 =$ altitude R', which proves (2).

EXAMPLE 3. *A normal local integral domain whose completion is integral over it and a local integral domain of altitude* 1 *whose derived normal ring is not a finite module.*

(E3.1) *Let K be a field characteristic $p \neq 0$ and let $x_1, \ldots, x_n$ be indeterminates. Set $R^+ = K[[x_1, \ldots, x_n]]$ and $R = K^p[[x_1, \ldots, x_n]] \cap K$. Then: (1) an element h of R^+ is in R if and only if the coefficients of h generate a finite extension over K^p, (2) if $[K : K^p] = \infty$ then $R \neq R^+$, and (3) R is a regular local ring and R^+ is the completion of R.*

Proof. (1) is straightforward and (2) is an immediate consequence of (1). As for (3), if we know that R is Noetherian, then we prove the assertion easily. Therefore we shall prove that R is Noetherian. Since R is a local ring which may not be Noetherian whose maximal ideal is generated by the x_i, it is sufficient to show that every ideal $\mathfrak{a}$ of R which has a finite basis is a closed subset of R by virtue of (31.8), hence that $\mathfrak{a}R^* \cap R = \mathfrak{a}$. Let $a_1, \ldots, a_m$ be a basis for $\mathfrak{a}$ and let b be an arbitrary element of $\mathfrak{a}R^* \cap R$. Let K' be the field generated by the coefficients of a_i and b over K^p. Then K' is finite over K^p by (1). Let $\{d_\lambda\}$ $(d_1 = 1)$ be a linear base of K over K'. Since $b \in \mathfrak{a}R^* \cap R$, there are elements $f_1^*, \ldots, f_m^*$ of R^* such that $b = \sum a_i f_i^*$. Each f_i^* is the sum of two elements g_i^* and h_i^* of R^* such that $g_i^* \in K'[[x]]$ and such that the coefficients of h_i^* are linear combinations of the d_λ other than 1. Since $b, a_i \in K'[[x]]$, we see that $b = \sum a_i g_i^*$, which implies that $b \in \sum a_i K'[[x]] \subseteq \mathfrak{a}$ (because $K'[[x]] \subseteq R$ by virtue of (1)), and the assertion is proved.

Thus, if, for instance, K is the field generated by infinitely many algebraically independent elements over a field of characteristic $p \neq 0$, then *R is a regular local ring which is not complete and such that the completion R^* of R is a purely inseparable integral extension of R.*

(E3.2) *Assume that $[K : K^p] = \infty$ and let $b_1, b_2, \ldots, b_i, \ldots$ be p-independent elements of K. Set $c = \sum b_i x_1^i$, and consider the case where $n = 1$. Then $R[c]$ is the required example.*

Proof. Set $d = c^p$. Then $d \in R$ and $X^p - d$ is irreducible over R. $R[c] \cong R[X]/(X^p - d)R[X]$, whence the completion of $R[c]$ is isomorphic to $R^*[X]/(X^p - d)R^*[X]$, in which the residue class of $X - c$ is a non-trivial nilpotent element. Let R' be the derived normal ring of $R[c]$. Then R' is a Noetherian valuation ring by the theorem of Krull-Akizuki and by the fact that $R \leq R[c] \leq R' \leq R^*$. Therefore R' is analytically irreducible. If R' is a finite $R[c]$-module, then $R[c]$ is a subspace of R' and $R[c]$ must be analytically irreducible, which is a contradiction. Thus R' cannot be a finite $R[c]$-module, and the assertion is proved.

We note that we can modify the above example so that:

(E3.3) *There is a Noetherian valuation ring V of a field K such that the field of quotients K^* of the completion V^* of V is a purely inseparable extension of K such that $[K^*:K]$ = the characteristic of K.*

Proof. Let V^* be R^* in the case where $n = 1$ and let c be as above. Let $\{c_\lambda\}$ be a maximal set of p-independent elements of K^* over the field of quotients L of R such that $c \in \{c_\lambda\}$. Let K be the field generated by all the c_λ except c over L. Then $[K^*:K] = p$. Set $V = V^* \cap K$. Then V is a Noetherian valuation ring with maximal ideal x_1V, whence the assertion is proved.

EXAMPLE 4. *A local integral domain T of altitude 2 with derived normal ring T' such that there is a non-Noetherian ring T'' between T and T'.*

Consider the ring R in (E3.1) in the case where $n = 2$. Let us denote x_1 and x_2 by x and y. Let $b_1, \ldots, b_i, \ldots$ be p-independent elements of K and set $c = y \sum b_i x^i$, $c_n = (c - \sum_{i<n} y b_i x^i)/x^n$. We are to show now that:

(E4.1) *$T = R[c]$ and $T'' = R[c_1, \ldots, c_i, \ldots]$ are the required pair of rings.*

Proof. Since c is purely inseparable over R, we see that T is a local ring. Since R^* is integral over R and since $R \subseteq T \subseteq T'' \subseteq R^*$, we see that T'' is integral over T, hence we see that T'' is contained in the derived normal ring of T. Thus it remains only to show that T'' is not Noetherian. Let z be an arbitrary element of $(xR^* + yR^*)^m \cap T''$. Since $z \in T''$, z is a polynomial in $c_1, \ldots, c_n$ (with a suitable n) with coefficients in R. Since $c_i = b_i y + c_{i+1}x$, we can write z as a polynomial in $x^m c_{n+m}$ with coefficients in R, say,

$$z = z_0 + z_1(x^m c_{n+m}) + \cdots + z_t(x^m c_{n+m})^t \quad (z_i \in R).$$

Since $z \in (xR^* + yR^*)^m$, we have

$$z_0 \in (xR^* + yR^*)^m \cap R = (xR + yR)^m.$$

Thus $z \in (xT'' + yT'')^m$. Therefore we see that T'' is a dense subspace of R^*. Therefore, if T'' is Noetherian, then T'' must be regular. But T'' is not normal, because c_1/y is not in T''. Thus T'' is not Noetherian, which completes the proof.

EXAMPLE 5. *A local integral domain of altitude 3 whose derived normal ring is not Noetherian.*

Let R be the ring in (E3.1) in the case where $n = 3$. We denote by x, y, z the variables x_1, x_2, x_3. We change the notation b_i for

p independent elements; we denote them by $b_1, c_1, b_2, c_2, \ldots, \ldots, b_i, c_i, \ldots$. Set $d = y\sum_i b_i x^i + x\sum_i c_i x^i$. For the sake of simplicity, we assume that $p = 2$. Then:

(E5.1) *$R[d]$ is the required example.*

Proof. It is sufficient to show that the derived normal ring T of $R[d]$ is not Noetherian. Since T is normal, $xR^* \cap T = xT$, whence xT is a prime ideal. We consider valuation rings $R' = R_{xR}$ and $R'' = T_{xT}$. Since d is in the completion of R', we see that R' is a dense subspace of R'', whence $R'/xR' = R''/xR''$. Since T/xT is integral over R/xR and since R/xR is normal, it follows that $T/xT = R/xR$. Therefore the maximal ideal of T is generated by x, y, z. Assume for a moment that T is Noetherian. Then T must be regular. Therefore T/zT is regular, which implies that T contains $\sum b_i x^i + zf$ for some $f \in R^*$. Then we can write $\sum b_i x^i + zf = (a_0 + a_1 d)/e_1$, where a_0, a_1, e_1 are elements of R such that they have no common factor. Then we have $e_1 \sum b_i x^i + e_1 zf = a_0 + a_1 y \sum b_i x^i + a_1 z \sum c_i x^i$. Since 1, $\sum b_i x^i$ are linearly independent over $K^p[[x, y]][K]$ $(= R/zR)$, we have $a_0 \in zR$ and $e_1 - a_1 y \in zR$. Therefore we write $a_0 = za_0'$, $e_1 = a_1 y + ez$ $(a_0', e \in R)$. Then $(a_1 y + ez)(\sum b_i x^i + fz) = za_0' + a_1 y \sum b_i x^i + a_1 z \sum c_i x^i$, and therefore $a_1 yzf + ez \sum b_i x^i + efz^2 = za_0' + a_1 z \sum c_i x^i$. We write a_1, a_0', e and f as power series in z with coefficients in $K[[x, y]]$, say, $a_1 = \sum a_{1i} z^i$, $a_0' = \sum a_{0i} z^i$, $e = \sum e_i' z^i$, $f = \sum f_i z^i$. We want to show that e_r', a_{0r}, and a_{1r} are in $yK[[x, y]]$ by induction on r. Comparing the coefficients of z in the above equality, we have $a_{10} yf_0 + e_0' \sum b_i x^i = a_{00} + a_{10} \sum c_i x^i$. Since 1, $\sum b_i x^i$, $\sum c_i x^i$ are linearly independent over $K^p[[x]][K]$, we see that e_0', a_{00}, a_{10} are in $yK[[x, y]]$, which settles the case where $r = 0$. Comparing the coefficients of z^{r+1} in the above equality, we have $y(\sum_0^r a_{1i} f_{r-i}) + e_r' \sum b_i x^i + \sum_0^{r-1} e_i' f_{r-1-i} = a_{0r} + a_{1r} \sum c_i x^i$. Since e_0', $\ldots$, e_{r-1}' are in $yK[[x, y]]$ by induction, we see that e_r', a_{0r} and a_{1r} are in $yK[[x, y]]$. Thus we see that e_1, a_0 and a_1 are in $yR^* \cap R = yR$, which contradicts our choice of them. Thus T cannot be regular, and T is not Noetherian, which proves the assertion.

EXAMPLE 6. *A normal local ring which is analytically ramified.*

We make use again of the ring R in (E3.1) in the case where $n = 2$; we denote x_1 and x_2 by x and y. As in Example 5, let $b_1, c_1, \ldots, \ldots, b_i, c_i, \ldots$ be infinitely many p-independent elements of K. For the sake of simplicity, we assume that $p = 2$. Set $d = \sum(b_i x^i + c_i y^i)$ and $T = R[d]$. Then:

(E6.1) *T is the required example.*

Proof. That T is analytically ramified (i.e., the completion of T has non-trivial nilpotent elements) can be proved similarly as (E3.2). Therefore it remains only to prove that T is a normal ring. Set $e_n = \sum_0^\infty b_{n+i}x^i$, $f_n = \sum_0^\infty c_{n+i}y^i$, and $U = R[e_1, f_1, \ldots, e_n, f_n, \ldots]$, and let U' be the derived normal ring of U. We want to show first that $U = U'$. Let g be an arbitrary element of U'. Then

$$g = (p + qe_n + rf_n + se_nf_n)/t$$

with $p, q, r, s, t \in R$, because $R[e_1, f_1, \ldots, e_n, f_n] = R[e_n, f_n]$. Since p, q, r, s, t are in R, there is an integer N such that the coefficients of these elements are in $K^2(b_1, c_1, \ldots, b_{N-1}, c_{N-1})$. Since $e_n = b_n + b_{n+1}x + \cdots + b_{N-1}x^{N-n-1} + x^{N-n}e_N$ and $f_n = c_n + c_{n+1}y + \cdots + c_{N-1}y^{N-n-1} + y^{N-n}f_N$, we see that g is in the derived normal ring of $V = K^2[[x, y]][b_1, c_1, \ldots, b_{N-1}, c_{N-1}, e_N, f_N]$. $K^2[[x, y]][b_1, c_1, \ldots, \ldots, b_{N-1}, c_{N-1}]]$ is a complete regular local ring. Since the leading forms b_N, c_N of e_N, f_N are p-independent over

$$K^2(b_1, c_1, \ldots, b_{N-1}, c_{N-1}),$$

we see that the ring V is a regular local ring, hence is a normal ring. Thus $g \in V \subseteq U$, and $U = U'$. Since $d = e_1 + f_1$, T is contained in U, and therefore the derived normal ring T' of T is contained in U. This implies that if h is an element of T', then there is an integer N such that $x^Ny^Nh \in R[e_1, f_1]$. Since h is in the field of quotients of $T = R[d]$, have $x^Ny^Nh = a + a'd = a_0 + a_1e_1 + a_2f_1 + a_3e_1f_1$ with $a_i \in R$ and with a, a' in the field of quotients of R. Since $1, e_1, f_1, e_1f_1$ are linearly independent over R and since $d = e_1 + f_1$, we have $a = a = a_0$, $a' = a_1 = a_2$ and $a_3 = 0$. Thus $x^Ny^Nh \in T$. We want to snow that $x^Ny^Nh \in T$ implies that $h \in T$. For that purpose, we may assume that $N = 1$. If $h \notin T$, then we have, by (12.7), one of the following: (1) xyT has an imbedded prime divisor, (2) there is at least one minimal prime divisor $\mathfrak{p}$ of xyT such that $T_\mathfrak{p}$ is not normal. Both are impossible because xT and yT are prime ideals, as can be seen as follows: T/xT is isomorphic to $K^2[[y]][K, f_1]$, which is an integral domain, and xT is prime; similarly, yT is a prime ideal. Thus the proof is complete.

EXAMPLE 7. *A normal local ring which is analytically reducible.*

Let K be a field of characteristic not equal to 2. Let x, y be indeterminates and let $w = \sum a_ix^i$ ($a_0 = 0$, $a_i \in K$) be an element of

$K[[x]]$ which is transcendental over $K(x)$. We put

$$z_1 = x^{-1}(y + w)^n, z_{i+1} = x^{-1}(y + \sum_{j=1}^{n} a_j x^j)^n + x^i$$

and $R = K[x, y, z_1, \ldots, z_n, \ldots]_{\mathfrak{m}}$, where $\mathfrak{m}$ is the ideal generated by $x, y, z_1, \ldots, z_n, \ldots$. Then letting X be an indeterminate, we can assert that:

(37.1) *$R[X]/(X^2 - z)R[X]$ is the required example.*

In order to prove the assertion, we study some properties of R. It is obvious that R is dominated by $K[[x, y]]$. On the other hand, the definition of z implies that there is a polynomial $f_i(x, y) \in K[x, y]$ for each i such that $xz_{i+1} = z_i + f_i(x, y)$ ($f_i(0, 0) = 0$). Therefore every z_i is in $xR + yR$. Thus the maximal ideal of R is generated by x and y. Furthermore, it is easy to see that for any element a of R and for any given natural number n, there is a polynomial $g(x, y) \in K[x, y]$ such that $a - g(x, y) \in (xR + yR)^n$ by virtue of the relation $xz_{i+1} = z_i + f_i(x, y)$. Thus we see that $K[[x, y]]$ is the completion of R in view of the fact that R dominates $K[x, y]_{(xK[x,y]+yK[x,y])}$.

Let $\mathfrak{p}$ be a prime ideal of height 1 in R. If $x \in \mathfrak{p}$, then it is obvious that $\mathfrak{p} = xR$. Assume that $x \notin \mathfrak{p}$. Since every z_i is in $K[x, y, z, 1/x]$, the ring $R[1/x]$ is a ring of quotients of $K[x, y, x]$. Since x, y, z are algebraically independent over K, $K[x, y, z]$ is a unique factorization ring, whence $R[1/x]$ is a unique factorization ring, which shows that $\mathfrak{p}R[1/x]$ is principal. Let $p \in \mathfrak{p}$ be a generator of $\mathfrak{p}R[1/x]$. Since xR is a prime ideal of height 1, R_{xR} is a Noetherian valuation ring and $\bigcap_n x^n R = 0$. Therefore we may assume that $p \notin xR$. Let a be an arbitrary element of $\mathfrak{p}$ and let r be an integer such that $ax^r \in pR$, hence $ax^r = pb$ with $b \in R$. If $r > 0$, then $pb \in xR$ which is a prime ideal, and therefore $b \in xR$ because $p \notin xR$. Therefore we prove that $a \in pR$, and $\mathfrak{p} = pR$. Thus every prime ideal of height 1 in R is principal. Let $\mathfrak{q}$ be a prime ideal of R which is not of height 1. We want to show that $\mathfrak{q}$ is maximal. Assume the contrary. Since depth $xR = 1$, as is easily seen, we see that $x \notin \mathfrak{q}$. Therefore $\mathfrak{q}R[1/x] \cap K[x, y, z]$ is a prime ideal of height 2 in $K[x, y, z]$. Therefore the transcendence degree of $R/\mathfrak{q}$ over K is one. Let x', y', z' be the residue classes of x, y, z, respectively, modulo $\mathfrak{q}$. Since the maximal ideal of R is generated by x and y and since $x \notin \mathfrak{q}$ any polynomial ($\neq 0$) in x with coefficients in K cannot be in $\mathfrak{q}$, which implies that x' is transcendental over K. Therefore $R/\mathfrak{q}$ is algebraic over $K[x']$, whence $R/\mathfrak{q}$ is a locality of altitude 1 over K. But, in the completion of $R/\mathfrak{q}$, $z' =$

$(y' + \sum a_i x'^i)^n$. Since $\sum a_i x'^i$ is transcendental over $K(x')$, we see that either x' or y' must be transcendental over $K(x')$, which contradicts the fact that $R/\mathfrak{q}$ is algebraic over $K[x']$. Thus $\mathfrak{q}$ must be maximal. Therefore we have proved that every prime ideal of R has a finite base, which implies that R is Noetherian by the theorem of Cohen. Thus we see that R is a regular local ring. Furthermore we assert that zR is a prime ideal of R. Indeed, since $R[1/x]$ is a ring of quotients of $K[x, y, z]$, z is a prime element of $R[1/x]$. Since zR and xR have no common prime divisor, we see that zR is a prime ideal.

Now we are to prove (E7.1). Since R is Noetherian,

$$R[X]/(X^2 - z)R[X]$$

is Noetherian. Since z is a prime element of the regular local ring R, and since the characteristic of K is different from 2, we see easily that $R[X]/(X^2 - z)R[X]$ is a normal local ring. The completion of the ring is $K[[x, y]][X]/(X^2 - z)K[[x, y]][X]$. Since $z = (y + w)^2$, $X^2 - z = (X - (y + w))(X + (y + w))$, whence the zero ideal of the completion of the local ring has two prime divisors.

EXAMPLE 8. *A Noetherian integral domain T whose derived normal ring is not a finite T-module, such that, if $\mathfrak{p}$ is a prime ideal of T then the derived normal ring of $T_\mathfrak{p}$ is a finite $T_\mathfrak{p}$-module.*

Let K, x, y, $b_1, \ldots, b_n, \ldots, R$ be as in Example 4. Let $p_1, \ldots, \ldots, p_n, \ldots$ be infinitely many prime elements of R ($p_iR \neq p_jR$ if $i \neq j$). For each natural number n, we set $q_n = p_1 \cdots p_n$. Set $c = \sum b_i q_i$. On the other hand, set $I = R[1/x]$. Then:

(E8.1) *$T = I[c]$ is the required example.*

Proof. I is obviously a Dedekind domain, hence T is a Noetherian integral domain of altitude 1. Set $c_n = (c - \sum_1^{n-1} b_i q_i)/q_n$. Then the derived normal ring T' of T contains all the c_n (for $c_n^p \in R$). Since $K^p[[x, y]][b_1, \ldots, b_{n-1}][c_n]$ is a regular local ring, we see easily that $R[c_1, \ldots, c_n, \ldots]$ is a normal ring, hence $T' = I[c_1, \ldots, c_n, \ldots]$. Let $\mathfrak{p}$ be an arbitrary maximal ideal of T. If $p_n \notin \mathfrak{p}$ for any n, then $c_i \in T_\mathfrak{p}$ for every i, whence $T_\mathfrak{p}$ is normal. If $p_n \in \mathfrak{p}$, then $T_\mathfrak{p}$ does not contain c_n, whence $T_\mathfrak{p}$ is not normal. The derived normal ring of $T_\mathfrak{p}$ in this case is $T_\mathfrak{p}[c_1, \ldots, c_n, \ldots] = T_\mathfrak{p}[c_n]$. Thus, in any case, the derived normal ring of $T_\mathfrak{p}$ is a finite $T_\mathfrak{p}$-module. On the other hand, we saw that if $p_i \in \mathfrak{p}$, then $T_\mathfrak{p}$ is not normal, which implies that there are infinitely many prime ideals $\mathfrak{p}$ of height 1 such that $T_\mathfrak{p}$ is not

normal. Therefore the proof is to be completed by the following lemma:

(38.2) *If the derived normal ring R' of a Noetherian integral domain R is a finite module, then there is only a finite number of prime ideals $\mathfrak{p}$ of height 1 in R such that $R_{\mathfrak{p}}$ is not normal.*

Proof. Such a $\mathfrak{p}$ must contain the conductor of R in R', which proves the assertion.

A2. Historical Note

We shall look at the history of the important results in our book. But we shall not concern ourselves with those historical facts which can be seen in Krull's book [4].

Chapter 1:

§1. The topics in this section are rather classical except for the principle of idealization and the exactness of tensor products. The former was first noticed by Nagata [16] and then by Nagata-Akizuki [1]. The exactness of a tensor product is a special case of exactness of functors which was discussed in Cartan-Eilenberg [1].

§2. The topics in this section are all classical.

§3. (3.3) and the theorem of Cohen (3.4) were given by Oka [1] and Cohen [2], respectively. We note by the way that the original form of the Hilbert basis theorem (3.6) is in Hilbert [1]. The lemma of Artin-Rees (3.7) was orally communicated to us by E. Artin in his lecture at Kyoto University in 1955. On the other hand, a special case of the lemma (the case where $N = R$ and N' is an ideal of R) was published by D. Rees [2]. The intersection theorem of Krull (3.11) is a generalization by Chevalley [1] of a theorem (our (4.2)) given by Krull [9]. (3.12) is a generalization of a result of Rees [2] which asserts only the case where x is not a zero divisor and $M = R$ (the case where x may be a zero divisor was noted by Lech [1]), hence (3.13) and (3.14) are new. (3.16) was given by Y. Mori and was orally communicated to the writer by him in 1952. Exercises 2 and 3 were remarked by H. Matsumura.

§4. The history of the lemma of Krull-Azumaya (4.1) is somewhat complicated. Namely, the case where $N = 0$ and where M is an ideal was given and used effectively by Krull. But the one who effectively used the module case is really Azumaya (cf. Azumaya [1]), hence the writer once named this lemma "Azumaya's lemma" in Nagata

[10]. But, since (4.4) is an easy generalization of the case given by Krull, the writer changed his mind when he wrote Nagata [23]. (The first literature which contains the lemma in the present form is Nagata [1], but the writer learned its formulation from T. Nakayama and G. Azumaya orally at Nagoya University when the writer was an undergraduate student.) Meanwhile, the writer saw that some mathematicians call this lemma "Nakayama's lemma" and therefore the writer asked Nakayama, who had this formulation first, and what would be the best name for this lemma? Then, Nakayama kindly answered the writer that he did not remember whether Nakayama or Azumaya was the first person and that the name of Krull-Azumaya for the commutative case and the name of Jacobson-Azumaya for the non-commutative case would be the best names for the lemma. Thus the writer employs the name of Krull-Azumaya in this book. (4.2) was substantially given by Krull [9] (cf. the history of (3.11)). (4.3) was given by Nagata [14].

§5. The results in this section are contained substantially in Krull [9].

§6. The notion of rings of quotients was first studied by Grell [1], who treated only the case where S consists merely of non-zero-divisors. The case was clarified by Chevalley [1]. Chevalley [2] defined the ring of quotients with respect to a prime ideal, then Uzkov [1] generalized completely. The method of Chevalley [1] can be applied to the generalized case and we obtain (6.4)–(6.9). The writer does not know any existing literature which contains (6.13). The notation $R(x)$ was introduced (in a more general case) by Nagata [13].

§7. Prime divisors (or associated prime ideals) of an ideal in a Noetherian ring had been defined by virtue of primary decomposition, which is not applicable to the general case; Nagata [10] generalized the notion and obtained the results in this section, except for (7.8) which we owe to Krull [1].

§8. The results in this section for non-graded Noetherian rings are proved by Noether [1] and expounded by Van der Waerden [1]. The notion of graded rings and graded modules are immediate generalizations of the notions of homogeneous rings and homogeneous ideals, hence one may say that these notions are classical. By virtue of our (8.3), the known method (cf. Van der Waerden [1]) can be adapted to the graded case and we obtain the results. Primary decomposition in Noetherian modules has been treated as an adaption of the case of ideals, and the idea in the exercises is new.

§9. (9.1) was given by Akizuki [2]. (9.2) and the altitude theorem of Krull (9.3) were given by Krull [1], and (9.4), (9.5), and (9.6) are immediate consequences of (9.3). The notion of a system of parameters of a local ring was introduced and used effectively by Chevalley [1]. (9.10) has been regarded as an obvious fact by many people.

§10. The notion of integral dependence is classical, but the object has been generalized; the case of algebraic integers at first, then the integral dependence over a ring (cf. Noether [3]), and then the one over an ideal (cf. Krull [5]). (10.5), (10.7), the lying-over theorem (10.8), the going-up theorem (10.9), (10.11), (10.12), the going-down theorem (10.13), and (10.14) were given by Krull [7] and generalized a little by Cohen-Seidenberg [1]. Grell [1] is the first person who studied the notion of a conductor in the general case. (10.1), (10.2), (10.3), (10.4), (10.15), and (10.16) are either classical or immediate generalizations of classical results and should be referred to Noether [3] (the validity of (10.15) in this form (i.e., the case where f may be reducible) was noted by Zariski [6]). (10.18) is also classical and has been known to algebraic geometers. Exercises 1–3 are adaptions of the case of integral dependence over a ring. Exercise 4 was given partly by Northcott-Rees [1], then by Nagata [18] in this form. Exercise 5 is new.

§11. We owe the theory of valuation rings mostly to Krull [2]; (11.1)–(11.9), and (11.12) are either Krull's results or immediate generalizations of Krull's results. (11.10) and the theorem of independence of valuations (11.11) were given by Nagata [4]. Exercise 1 was given by Nagata [4] and is an adaption of the classical approximation theorem (cf. Krull [2]). Exercises 2 and 4 were given by Krull [2].

§12. (12.1) and (12.4) are classical. (12.2) was given by Sato [2]. (12.3), (12.5), (12.6), and (12.7) were given by Nagata [10], [11]. (12.9) was given by Krull [3]. (12.10) is classical. The Exercises 1–5 are classical.

§13. All the results in this section (except for Exercises) are classical.

§14. The classical normalization theorem (for finitely generated integral domain) is the case where the ground field contains infinitely many elements and was given by Noether [2]. A normalization theorem for polynomial rings over a field (containing infinitely many elements) was given by Chevalley [4]. A generalization of Noether's

normalization theorem to the case of an integral domain over a field which may contain only a finite number of elements was given by Zariski [2]. Our generalizations (14.1) (14.4) and proofs of them were given by Nagata [6] and [13]. (14.5) and (14.6) are classical. (14.7) was given by Zariski [4]. (14.8) is an immediate consequence of the case where I is a field and the case was proved by Zariski [4] (cf. Nagata [13]). The Hilbert zero-points theorem was given by Hilbert [2] in a slightly different form, and, as is well known, there are many proofs of it by many authors. (14.10) was partly given by Artin-Tate [1] (in the Noetherian case) and then by Nagata [13] in the general case.

Chapter II

§15. (15.3) was given by Chevalley [1].

§16. (16.2)–(16.4) are special cases of some elementary results in the general theory of topological groups. (16.5) was given by Serre [3]. As for (16.7) we should give a reference to Krull [9]. (16.8) was given by Chevalley [1]. Zariski rings were treated first by Zariski [3].

§17. (17.7) was given by Chevalley [1]. (17.8) was partly given by Chevalley [1] and then given by Serre [3]. (17.9) was given by Krull [9] and by Chevalley [1]. (17.11) was given by Serre [3]. (17.12) was substantially given by Krull [9].

§18. (18.1) was noted by J-P. Serre as was communicated to the writer by P. Samuel in a letter (in 1955—the writer believes). (18.3)–(18.12) are new. On the other hand, the special case of the results in this section where R is a semi-local ring or a Zariski ring and R^* is the completion of R were given by the following authors: (18.1), (1) by Nagata [6], (18.1), (3) Zariski [5], (18.1), (4)–(5) by Chevalley [1]. (18.4) by Y. Mori (orally; in 1952). (18.11), partly by Nagata [16], then by Sato [1]. Exercise 5 was given at first in the case of a local ring by Y. Mori (orally; in 1949), then by Yoshida [1] in the general case. Exercise 6 was given at first in the case of a local ring by Y. Mori (orally; in 1949), and Sato [1] remarked this fact. Exercise 7 is new.

§19. All results in this section are new, though (3) in (19.2) was substantially proved by Nagata [16]. The origin of the "theorem of transition" is a theorem of transition of a multiplicity for geometric local rings given by Chevalley [4], which asserts that if R is a geometric local ring (in Chevalley's sense), if R^* is the completion of

R, if $\mathfrak{p}$ is a prime ideal of R and if $\mathfrak{p}^*$ is a (minimal) prime divisor of $\mathfrak{p}R^*$, then $\mu(\mathfrak{q}R_{\mathfrak{p}}) = \mu(\mathfrak{q}R^*_{\mathfrak{p}^*})$ for a primary ideal $\mathfrak{q}$ generated by a system of parameters of $R_{\mathfrak{p}}$. This, Chevalley's result, was generalized at first a little by Samuel [1], whose result says in our terms that the theorem of transition holds for $R_{\mathfrak{p}}$ and $R^*_{\mathfrak{p}^*}$ (in the above case). This, Samuel's generalization, was generalized to an arbitrary local ring by Nagata [16], which is a special case of our (19.2), (2).

Chapter III

The multiplicity of a system of parameters in a local ring which contains a field was introduced by Chevalley [1] and studied by Chevalley [4] in the case of geometric local rings (in Chevalley's sense). A nice idea to make use of Hilbert characteristic functions was employed by Samuel [1], whose theory was developed by Nagata [16].

§20. The results are adaptions of classical ones.

§21. (21.1) and (21.2) are easy generalizations of the first step of Samuel's theory (cf. Nagata [16]). (21.5) was first remarked in this book.

§22. (22.1)–(22.5) are easy generalizations of results by Samuel [1] (cf. Nagata [16]). (22.6) is a non-trivial generalization of a result by Samuel [1] and of a result by Serre [2]. (22.7) and (22.8) are easy generalizations of results by Samuel [1].

§23. Our definition of a multiplicity is a generalization of a relative multiplicity defined by Nagata [16]. (Cf. Auslander-Buchsbaum [2]) (23.1) was substantially noted by Nagata [16]. (23.3) was first noted substantially by Serre [2], (23.4) by Samuel [1], (23.5) by Nagata [16] and Serre [2] independently, and (23.7) by Serre [2].

§24. (24.1) and (24.2) are generalizations of results by Samuel [1], Nagata [16], Serre [2]. (24.4), (24.5), and (24.6) are generalizations of results by Lech [1] (cf. Sakuma [1]). The associativity formula (24.7) was first proved by Chevalley [4] in geometric local rings and was generalized to the case of an arbitrary local ring by Nagata [16], Serre [2], and Lech [1] independently.

§25. Though the notion of a distinct system of parameters was introduced by Samuel [1], the theory of Macaulay rings was given by Nagata [16]; (25.1)–(25.13) were substantially given by Nagata [16]. The normality of a regular local ring was given by Krull [9] whose proof was adapted by us for (25.15). That a regular local ring

in a Macaulay ring was proved by Cohen [1]. (25.16) was given by H. Hironaka in his Master's degree thesis at Kyoto University (unpublished). (25.18) was given by Chevalley [1].

Chapter IV

§*26*. The results are elementary.

§*27*. (27.6) and (27.8) were given by Serre [1] making use of homological algebra; other results except for Exercises can be regarded as new.

§*28*. (28.2) was given by Auslander, Buchsbaum, and Serre; at first the converse part was given by Auslander-Buchsbaum (published later in [1]) then completed by Serre [1]; they used, of course, homological algebra. (28.3) was given by Serre [1], but some special cases had been proved by Cohen [1] and Nagata [16]. (28.4) was given by Serre [1] and Nagata [16] independently (partly by Cohen [1]). (28.5) was given by Auslander-Buchsbaum [3]. (28.6) was given by Nagata [14]. (28.7) has rather long history. The case of power series over an infinite field is seemingly classical. Krull [8] proved the theorem for power series rings over a complete Noetherian valuation ring which is not a field, and the result was generalized by Cohen [1] to complete unramified regular local rings. The algebraic-geometrical case was proved by Zariski [4]. Then Y. Mori proved the theorem for the case of altitude not greater than 2 and also for unramified regular local rings (announced at the spring meeting of the Mathematical Society of Japan in 1949) and the same was given independently by the writer in March of 1950 (unpublished); later in 1954, the same was published by Krull [10] (written in 1952). As for the general case, the reduction to the case of altitude 3 was made by O. Zariski (unpublished) and Nagata [14] independently and the case of altitude 3 was proved by Auslander-Buchsbaum [3].

§*29*. The classical result by Hilbert [1] is the one for the case of homogeneous polynomial rings over a field.

Chapter V

§*30*. (30.1) was given by Chevalley [1]. (30.2) was given by Cohen [1]. (30.4) is an easy adaption of the well known Hensel lemma in complete valuation rings and was noted by Cohen [1] (in the Noetherian case, and the general case was noted by Nagata [1]). (30.5) is rather classical and we should refer to Azumaya [1]. (30.6) was

substantially given by Chevalley [1]. Exercise 1 was given by Cohen [1].

§31. (31.1) was given by Cohen [1], whose proof was simplified by Narita [1] and Geddes [1], [2]. (Nagata [1] simplified the proof in some special cases and his proof in the general case contained some serious errors. Geddes [1] simplified the proof for a local ring which contains a field. Narita [1] gave a proof which we expounded in this book, and then Geddes [2] gave another, but similar proof.) (31.2) and (31.3) were given by Teichmüller [1]. (31.5) was given by Nagata [2]. (31.6) and (31.7) were given by Cohen [1]. (31.8) was given by Nagata [1]. The notion of multiplicative representatives was given by Teichmüller [1]. (31.9), (31.10), and (31.12) were given by Cohen [1]. Exercise 2 was noted by Cohen [1] and also by Chevalley [1]. Exercise 3 was noted by Nagata [22].

§32. (32.1) was given by Nagata [7] and Mori [2]. (32.2) was given by Mori [1].

§33. (33.1) was given by Nagata [11]. As for (33.2): it was proved by Krull (Math. Ann. 103 (1930); cf. [6]) that the derived normal ring of a local integral domain of altitude 1 is Noetherian (and also Exercise 1), then Akizuki [1] generalized the result of Krull in our form, but assuming that R' is integral over R. The present form is a slight generalization of Akizuki's result and was given by Cohen [2]. The theory of Krull rings was originated by Krull [3] ((33.3), (33.4), (33.5), (33.6); cf. Nagata [11]). (33.9) is easy and is well known; (33.8) is its generalization and was noted by Nagata [11]. (33.10) was given by Mori [1] for local rings and then by Nagata [11] in the general case; (2) in (33.10) was first explicitly stated by Chevalley [5], though it had been proved by Y. Mori (unpublished). (33.11) was given by Nagata [11]; the present proof was given by H. Matsumura and was published by Akizuki-Nagata [1]. (33.12) was given by Mori [2] for local rings and was generalized by Nagata [11].

§34. (34.2) and (34.3) were given by Nagata [17] (in which our (34.3) was misstated). (34.4) was substantially given by Cohen [1]. (34.5) and (34.6) were given by Nagata [17]. (34.7) and (34.8) may be said to be new. (34.9) and (34.10) were given by Nagata [17].

Chapter VI

§35. (35.2) was given by Nagata [13] and is a slight generalization of a classical result. (35.3) was substantially given by Nagata [13].

(35.5) was given in a more general form by Nagata [21] (whose proof must be modified a little because our (34.3) was misstated in [17] and the misstated lemma was used in [21]). (35.6) was given by Nagata [21].

§36. (36.2) and (36.3) were substantially given by Zariski [5] (who treated the case where R is normal). (36.4) was given by Nagata [6] adapting Zariski's proof (Zariski [5]) of the analytical unramifiedness of algebraic-geometrical local rings. The analytical unramifiedness of algebraic-geometrical local rings was first given by Chevalley [4]. (36.5), (36.6), and (36.8) are new ((36.8) was partly given by Nagata [16]). (36.9) was substantially given by Hironaka [1]. (36.10) was also given by Hironaka.

§37. (37.1) was formulated in this form by Nagata [24] but was substantially given by Zariski [5]. (37.2) was given by Zariski [6]. (37.3) was substantially given by Zariski [6]. (37.4) is a ring-theoretic formulation of the so-called Zariski's main theorem on birational transformations and the present proof was given by Chevalley in his lecture at Kyoto University in 1953. (37.5) was partly given by Zariski [6] (the case where I is a field and R is separably generated over I), then by Nagata [6] (the case where I is a field), then by Nagata [7] (nearly the present case) and then by Nagata [13] (the present form). (37.6) is an immediate consequence of (37.5). (37.7) was noted by Nagata [13]. (37.8), (37.9), (37.10), and the exercise appear for the first time in this book.

§38. (38.1) and (38.2) are adaptions of the algebraic-geometrical case (cf. Zariski [2]). (38.3), (38.4) and (38.5) were given by Nagata [14]. (38.6) was partly given by Zariski [1] (the case where R is a normal locality over a field), whose proof can be applied to the case where R and R' are normal, then by Chevalley [6] (though Chevalley assumed that R is a locality over a field, he proved substantially the general case; he proved a little bit less than we have) and then by Nagata [24]. We make here a remark on the literature "Chevalley [6]." Exposé 5 in the seminar was given by A. Grothendieck and no name was given in its Appendix I. But the writer was told by A. Grothendieck that the appendix was written by Chevalley. (38.9) is rather classical. (38.10) was noted by Nagata [23]. The exercise is an adaption of the algebraic-geometrical case (cf. Zariski [2]).

§39. MacLane [1] proved that a function field L over a field K is separably generated over K if and only if L has a separating tran-

neendence base. Our results in this section are mostly reformulations given by Nagata [14] of Weil's treatment (Weil [1]). (39.11) was given by Nagata [14]. Exercise 1 was also given by Nagata [14]. Exercise 3 was first given in this book.

§40. (40.1) and (40.2) were given by Nagata [16]. (40.3) was partly given by Nagata [3] and [25]. (40.4) is a ring-theoretic formulation of a theorem (Proposition 6) in Nagata [13]. (40.5) was substantially given by Nagata [3]. It is not yet known to the writer's knowledge whether or not (40.1) is true without assuming that $\mathfrak{p}$ is analytically unramified. If it is true, then (40.3) (hence, its special case (40.5), too) is true without assuming that I or R is pseudo-geometric. (40.6) was partly given by Samuel [1] (the case where R contains a field) and then by Nagata [16] (the present form).

§41. The algebraic-geometrical case of (41.1) was proved by Zariski [7], the special case where altitude $R = 2$ was proved by Serre (unpublished) and Auslander-Buchsbaum [4] independently, and then the present general result was given by Nagata [24]. (41.2) is an adaptation of a classical result in number theory. The notion of discriminant is also an adaptation of the one in algebraic number theory. A special case of (41.5) (the case where R is a Noetherian normal ring and R' is also normal) was given by Auslander [4]. (41.7) was given by Chow [1]. (41.8) was noted by Nagata [5].

§42. The notion of a local tensor product was introduced by Nagata [14]. The notion of a complete tensor product was introduced by Chevalley [4] who treated only complete tensor products of complete semi-local rings over fields. Our treatment until (42.4) was given by Nagata [14]. (42.6) was partly given by Chevalley [4] and then, still partly, by Samuel [1] and then in this form by Nagata [16]. (42.8) was substantially given by Chevalley [4]. (42.9) and (42.10) were given by Y. Nakai in or before 1953 (unpublished) and published by some other authors. (42.11) and (42.12) were noted by Nagata [14]. The order of inseparability of a function field over a ground field was introduced by Weil [1] and Chevalley [4] (Chevalley called it the level of inseparability). The notion was generalized by Nagata [15] and our treatment of the notion is a simplification of what was given by Nagata [15]. The fundamental results, (42.15), (42.16), and (42.17), were given by Nagata [15] (published also by Nakai-Nagata [1]). (42.19) and (42.20) were given by Weil [1]. The

first equality in Exercise 3 was given by Weil [1], then a more general formula was given by Nagata [15].

Chapter VII

§43. The notion of Henselian rings was introduced by Azumaya [1] and the notion of Henselization was introduced by Nagata [4], [5], [23]. (43.1) and (43.2) were given by Nagata [4]. (43.5) was given by Nagata [23]. (43.8) was newly given in this book. (43.9) was substantially given by Nagata [5]. (43.10) was given by Nagata [5], [23]. (43.12) was noted by Nagata [5] (cf. (43.15)). (43.14) was pointed out by T. Nakayama and was published by Azumaya [1]. (43.15) was given by Azumaya [1]. (43.17) was first given in this book. (43.18) was given by Nagata [23]. (43.19), (43.20), and Exercises 1 and 2 were given by Nagata [5]. Exercise 3 was first given in this book. Exercises 4 and 5 were given by Nagata [4].

§44. (44.1) was substantially given by Nagata [7]. (44.2) is new. (44.4) was partly given by Nagata [4] (the case where R is a valuation ring), and this general case is new. The exercise was given by Nagata [4].

§45. Our notion of a Weierstrass ring was modified from that which was given by Nagata [7]. (45.1) was substantially given by Nagata [7]. (45.3) is classical. (Note that the original form of the theorem given by Weierstrass is Exercise 1, and the present form was noted by H. Späth in 1929 (*J. Reine Angew. Math.* Vol. 162), but the present form is substantially equivalent to that of Weierstrass as is easily seen.) (45.4) and (45.5) are also classical. (45.6) was given by Nagata [7]. Exercises 2 and 3 were newly given in this book. Exercise 4 was substantially given by Nagata [7].

§46. The notion of a mixed Jacobian matrix was introduced by Zariski [4], who proved (46.3) in the case where A is a polynomial ring. The generalized (46.3) was given by Nagata [19]. (46.4) was also given by Nagata [19]. (46.7) was noted by Nagata [25]. Exercise 2 was noted by Nagata [14]. Exercise 3 was given by Nagata [19].

§47. (47.2) and (47.3) were given by Nagata [9], and (47.4) and (47.5) are immediate consequences of (47.3). Note that (47.5) says, in the case where K is the complex number field, that the product of two irreducible analytic varieties is again irreducible. (47.6) and Exercise 5 were published in Sûgaku, Vol. 9 No. 1 (1957), p. 61

(Solution of Problem 8.1.15); the proof is not complete and a supplement is expected to appear soon. (17.7), (17.8), and (17.9) are seemingly new. Though some people know (17.10) in the case where K is the complex number field (Mr. Iwahashi of Nagoya University told the writer that he knew the result but his proof was difficult), the writer could not find any literature containing the result. Exercises 1, 3, and 4 were given by Nagata [9].

Appendix A1

(E1.1) was noted by Nagata [25]. (E1.2), Example 2, and (E2.1) were given by Nagata [4]. An example of a local integral domain of altitude 1 whose derived normal ring is not finite was first given by Akizuki [1] in the case of characteristic zero. Examples 4 and 5 were given by Nagata [8]. Example 6 was given by Nagata [12] and Example 7 was given by Nagata [20]. Example 8 was given by Nagata [25].

References

Akizuki, Y.

[1] Einige Bemerkungen über primäre Integritätsbereiche mit Teilerkettensatz, Proc. Phys.-Math. Soc. Japan, 17 (1935), pp. 327–336.

[2] Teilerkettensatz und Vielfachenkettensatz, Proc. Phys.-Math. Soc. Japan 17 (1935), pp. 337–345.

Akizuki, Y., and Nagata, M.

[1] Modern algebra (in Japanese). Kyôritsu, Tokyo, 1957.

Auslander, M., and Buchsbaum, D. A.

[1] Homological dimension in local rings, Trans. Am. Math. Soc. 85 (1957), pp. 390–405.

[2] Codimension and multiplicity, Ann. Math., 68 (1958), pp. 625–657; Errata Ann. Math. 70 (1959), pp. 395–397.

[3] Unique factorization in regular local rings, Proc. Nat. Acad. Sci. U. S. 45 (1959), pp. 733–734.

[4] On ramification theory in Noetherian rings, Am. J. Math. 81 (1959), pp. 749–765.

Artin, E., and Tate, J. T.

[1] A note on finite ring extensions, J. Math. Soc. Japan 3 (1951), pp. 74–77.

Azumaya, G.

[1] On maximally central algebras, Nagoya Math. J. 2 (1950), pp. 119–150.

Bourbaki, N.

[1] Algèbre multilinéaire (Algèbre, Chapitre 3), Hermann, Paris, 1948.

Cartan, H., and Eilenberg S.

[1] Homological algebra, Princeton University Press, Princeton, 1956.

Chevalley, C.

[1] On the theory of local rings, Ann. Math. 44 (1943), pp. 690–708.

[2] On the notion of the ring of quotients of a prime ideal, Bull. Am. Math. Soc. 50 (1944), pp. 93–97.

[3] Some properties of ideals in rings of power series, Trans. Am. Math. Soc. 55 (1944), pp. 68–84.

[4] Intersections of algebraic and algebroid varieties, Trans. Am. Math. Soc. 57 (1945), pp. 1–85.

[5] La notion d'anneau de décomposition, Nagoya Math. J. 7 (1954), pp. 21–33.

[6] Séminaire C. Chevalley 1956–1958; Appendix I to Exposé 5. École Normal Supérieure, Paris, 1958.

COHEN, I. S.

[1] On the structure and ideal theory of complete local rings, Trans. Am. Math. Soc. 59 (1946), pp. 54–106.

[2] Commutative rings with restricted minimum condition, Duke Math. J. 17 (1950), pp. 27–42.

COHEN, I. S., AND SEIDENBERG, A.

[1] Prime ideals and integral dependence, Bull. Am. Math. Soc. 52 (1946), pp. 252–261.

CHOW, W. L.

[1] On the theorem of Bertini for local domains, Proc. Nat. Acad. Sci. U. S. 44 (1958), pp. 580–584.

GEDDES, A.

[1] A short proof of the existence of coefficient fields for complete equicharacteristic local rings, J. London Math. Soc. 29 (1954), pp. 334–341.

[2] On the embedding theorem for complete local rings, Proc. London Math. Soc. 6 (1956), pp. 343–354.

GRELL, H.

[1] Beziehungen zwischen der Idealen verschiedener Ringe, Math. Ann. 97 (1927), pp. 490–523.

HILBERT, D.

[1] Über die theorie der algebraischen Formen, Math. Ann. 36 (1890), pp. 471–534.

[2] Über die vollen Invariantensysteme, Math. Ann. 42 (1893), pp. 313–373.

HIRONAKA, H.

[1] A note on algebraic geometry over ground rings—The invariance of Hilbert characteristic function under the specialization process, Illinois J. Math. 2 (1958), pp. 355–366.

KRULL, W.

[1] Primidealketten in allgemeinen Ringbereichen, S.-B. Heiderberg Akad. Wiss. 7 (1928).

[2] Allgemeine Bewertungstheorie, J. Reine Angew. Math. 167 (1931), pp. 160–196.

[3] Über die Zerlegung der Hauptideale in algemeinen Ringen, Math. Ann. 105 (1931), pp. 1–14.

[4] Idealtheorie, Ergeb. der Math. 4, No. 3, Julius Springer, Berlin, 1935.

[5] Beiträge zur Arithmetik kommutativer Integritätsbereiche, Math. Z. 41 (1936), pp. 545–577.

[6] Beiträge zur Arithmetik kommutativer Integritätsbereiche, II, Math. Z. 41 (1936), pp. 665–679.

[7] Beiträge zur Arithmetik kommutativer Integritätsbereiche, III, Math. Z. 42 (1937), pp. 745–766.

[8] Beiträge zur Arithmetik kommutativer Integritätsbereiche V, Math. Z. 43 (1938), pp. 768–782.

[9] Die Idealtheorie in Stellenringen, J. Reine Angew. Math. 179 (1938), pp. 204–220.

[10] Zur Theorie der kommutativen Integritätsbereiche, J. Reine Angew. Math. 192 (1954), pp. 230–252.

Lech, C.

[1] On the associativity formula for multiplicities, Arkiv. Math. 3 (1956), pp. 301–314.

Macaulay, F. S.

[1] Algebraic theory of modular systems, Cambridge Tracts Math., 19 Cambridge University Press, Cambridge, 1916.

MacLane, S.

[1] Modular fields. I, Duke Math. J. 5 (1939), pp. 372–393.

Mori, Y.

[1] On the integral closure of an integral domain, Mem. Coll. Sci., Univ. Kyoto 27 (1952–53), pp. 249–256; Errata, Mem. Coll. Sci., Univ. Kyoto 28 (1953–1954), pp. 327–328.

[2] On the integral closure of an integral domain, II, Bull. Kyoto Gakugei Univ. B7 (1955), pp. 19–30.

Nagata, M.

[1] On the structure of complete local rings, Nagoya Math. J. 1 (1950), pp. 63–70; Errata, Nagoya Math. J. 5 (1953), pp. 145–147.

[2] On the theory of semi-local rings, Proc. Japan Acad. 26 (1950) pp. 131–140.

[3] Local rings (in Japanese), Sugaku 5 (1953–54) pp. 104–114 and pp. 229–238.

[4] On the theory of Henselian rings, Nagoya Math. J. 5 (1953), pp. 45–57.

[5] On the theory of Henselian rings, II, Nagoya Math. J. 7 (1954), pp. 1–19.

[6] Some remarks on local rings, Nagoya Math. J. 6 (1953), pp. 53–58.

[7] Some remarks on local rings, II, Mem. Coll. Sci., Univ. Kyoto 28 (1953–54), pp. 109–120.

[8] Note on integral closures of Noetherian domains, Mem. Coll. Sci., Univ. Kyoto 28 (1953–54), pp. 121–124.

[9] Note on complete local integrity domains, Mem. Coll. Sci., Univ. Kyoto 28 (1953–54), pp. 271–278.

[10] Basic theorems on general commutative rings, Mem. Coll. Sci., Univ. Kyoto 29 (1955), pp. 59–77.

[11] On the derived normal rings of Noetherian integral domains, Mem. Coll Sci., Univ. Kyoto 29 (1955), pp. 293–303.

[12] An example of normal ring which is analytically ramified, Nagoya Math. J. 9 (1955), pp. 111–113.

[13] A general theory of algebraic geometry over Dedekind domains, I, Am. J. Math. 78 (1956), pp. 78–116.

[14] A general theory of algebraic geometry over Dedekind domains, II, Am. J. Math. 80 (1958), pp. 382–420.

[15] A general theory of algebraic geometry over Dedekind domains, III, Am. J. Math., 81 (1959), pp. 401–435.

[16] The theory of multiplicity in general local rings, Proceedings of the International Symposium, Tokyo-Nikko 1955, Scientific Council of Japan, Tokyo, 1956, pp. 191–226.
[17] On the chain problem of prime ideals, Nagoya Math. J. 10 (1956), pp. 51–61.
[18] Note on a paper of Samuel concerning asymptotic properties of ideals, Mem. Coll. Sci., Univ. Kyoto 30 (1956–57), pp. 165–176.
[19] A Jacobian criterion of simple points, Illinois J. Math. 1 (1957), pp. 427–432.
[20] An example of a normal local ring which is analytically reducible, Mem. Coll. Sci., Univ. Kyoto 31 (1958), pp. 83–85.
[21] Note on a chain condition for prime ideals, Mem. Coll. Sci., Univ. Kyoto 32 (1959–1960), pp. 85–90.
[22] Note on coefficient fields of complete local rings, Mem. Coll. Sci., Univ. Kyoto 32 (1959–1960), pp. 91–92.
[23] On the theory of Henselian rings, III, Mem. Coll. Sci., Univ. Kyoto 32 (1959–1960), pp. 93–101.
[24] On the purity of branch loci in regular local rings, Illinois J. Math. 3 (1959), pp. 328–333.
[25] On the closedness of singular loci, Publs. Math. Inst. Haut. Étud. Sci. 2 (1959), pp. 29–36.

NAKAI, Y. and NAGATA, M.

[1] Algebraic geometry (in Japanese). Kyôritsu, Tokyo, 1957.

NARITA, M.

[1] On the structure of complete local rings, J. Math. Soc. Japan 7 (1955), pp. 435–443.
[2] On the unique factorization theorem in regular local rings, Proc. Japan Acad. 35 (1959), pp. 329–331.

NISHI, M.

[1] On the dimension of local rings, Mem. Coll. Sci., Univ. Kyoto 29 (1955), pp. 7–9.

NOETHER, E.

[1] Idealtheorie in Ringbereichen, Math. Ann. 83 (1921), pp. 24–66.
[2] Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p, Nachr. Ges. Wiss. Göttingen, 1926, pp. 28–35.
[3] Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. Math. Ann. 96 (1926) pp. 26–61.

NORTHCOTT, D. G.

[1] Hilbert function in a local ring, Quart. J. Math. Oxford 4 (1953), pp. 67–80.

NORTHCOTT, D. G. and REES, D.

[1] Reduction of ideals in local rings, Proc. Cambridge Phil. Soc. 50 (1954), pp. 145–158.
[2] A note on reductions of ideals with an application to the generalized Hilbert function, Proc. Cambridge Phil. Soc. 50 (1954), pp. 353–359.

OKA, K.

[1] Sur les fonctions analytiques de plusieurs variables, VIII, J. Math. Soc. Japan 3 (1951), pp. 204–214.

REES, D.

[1] A note on valuations associated with a local domain, Proc. Cambridge Phil. Soc. 51 (1955), pp. 252–253.

[2] Two classical theorems of ideal theory, Proc. Cambridge Phil. Soc. 52 (1956), pp. 155–157.

SAKUMA, M.

[1] On the theory of multiplicities in finite modules over semi-local rings, J. Sci. Hiroshima Univ. 23 (1959), pp. 1–17.

SAMUEL, P.

[1] La notion de multiplicité en algèbre et en géométrie algébrique, J. math. pures appl. 30 (1951), pp. 159–274; Thèse, Paris, 1951.

[2] Algèbre locale, Mémorial Sci. Math. 123. Gauthier-Villars, Paris, 1953.

SATO, H.

[1] Some remarks on Zariski rings, J. Sci. Hiroshima Univ. 20 (1956–1957), pp. 93–99.

[2] A note on principal ideals, J. Sci. Hiroshima Univ. 21 (1957–1958), pp. 77–78.

SEIDENBERG, A.

[1] A note on dimension theory of rings, Pacific J. Math. 3 (1953) pp. 505–512.

SERRE, J.-P.

[1] Sur la dimension homologique des anneaux et des modules noethérian, Proceedings of the International Symposium, Tokyo-Nikko 1955, Scientific Council of Japan, Tokyo, 1956, pp. 175–189.

[2] Multiplicités d'intersection, mimeographed notes, 1955.

[3] Géométrie algébrique et géométrie analytique, Ann. inst. Fourier 6 (1955–1956), pp. 1–42.

TEICHMÜLLER, O.

[1] Diskret bewertete perfekte Körper mit unvollkommenen Restklassenkörper, J. Reine Angew. Math. 176 (1937), pp. 141–152.

UZKOV, A. I.

[1] On the rings of quotients of commutative rings, Mat. Sbornik N. S. 22 (64) (1948), pp. 439–441 (in Russian); cf. Math. Rev. 10 (1949), p. 97.

WAERDEN, B. L. VAN DER

[1] Moderne Algebra, I, Grundl. Math. Wiss. 33. Julius Springer, Berlin, 1930 (1st edition); 1937 (2nd edition); etc.

[2] Moderne Algebra, II, Grundl. Math. Wiss. 34. Julius Springer, Berlin, 1931 (1st edition); 1940 (2nd edition); etc.

WEIL, A.

[1] Foundations of algebraic geometry, Am. Math. Soc. Coll. Publ., 29. Am. Math. Soc., New York, 1946.

YOSHIDA, M

[1] A theorem on Zariski rings, Can. J. Math. 8 (1956), pp. 3–4.

ZARISKI, O.

[1] Algebraic varieties over ground field of characteristic zero, Am. J. Math. 62 (1940), pp. 187–221.

[2] Foundations of a general theory of birational correspondences, Trans. Am. Math. Soc. 53 (1943), pp. 490–542.

[3] Generalized semi local rings, Summa Brasil. Math. 1 (1946), pp. 169–185.

[4] The concept of a simple point of an abstract algebraic variety, Trans. Am. Math. Soc. 62 (1947), pp. 1–52.

[5] Analytical irreducibility of normal varieties, Ann. Math. 49 (1948), pp. 352–361.

[6] Sur la normalité analytique des variété normales, Ann. inst. Fourier 2 (1950), pp. 161–164.

[7] On the purity of the branch locus of algebraic functions, Proc. Nat. Acad. U. S. 44 (1958), pp. 791–796.

ZARISKI, O. AND SAMUEL, P.

[1] Commutative algebra, 1, van Nostrand, New York, 1958.

TABLE OF NOTATION

INDEX

G

H

I

J

K, κ

L, λ

M

N

O

P

Q

R

S, σ