TRABAJO FIN DE MÁSTER

Facultad de Matemáticas

GRÖBNER BASES AND

BUCHBERGER'S ALGORITHM

Autor: Raúl Sastriques Guardiola

Director: Dr. Juan Jacabo Simón Pinero

Murcia, June 18, 2024

Contents

Introduction

The aim of this work is to introduce the reader to Gröbner-bases theory, which was developed by Bruno Buchberger's during his doctoral thesis on the direction of Wolfgang Gröbner in 1965. Years after a period of few repercussions, Gröbner bases theory was rediscovered in 1985 by the computer-science and the mathematical community, who needed of algebraic computation. Although applications of the theory may be found in many contexts, we focus our attention on the ring of polynomials and algebraic structures. The aim of the project is to reproduce a classical introduction to the Gröbner theory and its application to ring of polynomials. Chapter 1 has the necessary background for the developing of the theory, whereas Chapter 2 starts developing the theory from its basis, relation theory and term orders. Chapter 3 contains the main theorems and algorithms concerning Gröbner bases; among these results, Gröbner basis existence and Buchberger's Algorithm are the leading ones. Finally, Chapter 4 ends with some application and specializations of the previously developed. Moreover, every algorithm is given with an example. Since Gröbner basis have been in the mathematical community for a while, plenty of literature, and articles, may be found related with this topic, in particular, what has been here presented consists of a compilation of book [1] and article [2], which contains most of the results up to that time. The reader is advised to check the above citations for further learning.

CHAPTER 1

Notation and Preliminaries

We provide a list of notation and word list which will be used all along the text.

For a given set X, the collection of all possible subsets of X is denoted by $\mathcal{P}(X)$, and is called **power set** of X.

Let X be a set. For $A \in \mathcal{P}(X)$, denote by $\overline{A}$ the complement of A in X, that is, $A \cup \overline{A} = X$. We define a binary operation in $\triangle$ on $\mathcal{P}(X)$ by setting$\mathcal{P}(X)$

$$A \triangle B = \left(A \cap \overline{B}\right) \cup \left(B \cap \overline{A}\right)$$

for $A, B \in \mathcal{P}(X)$. The set $A \triangle B$ is called the **symmetric difference** of A and B, or the **union without the intersection** of A and B.

We denote by $\mathcal{P}_{fin}(X)$ **the set of all finite subsets of** X. For a finite set A, $|A|$ denotes the **cardinal** of A, i.e., the number of elements of A.

DEFINITION 1. A method to construct a mathematical object, whose existence is known, in finitely many steps from other objects that it depends upon is called an **algorithm** . When verifying an algorithm, one must prove that it *terminates* after finitely many steps for every input as specified and that it performs that task *correctly*, i.e., it outputs an object that has the desired properties. A **loop invariant** is a mathematical statement or mathematical object that remains unaffected by the execution of the loop in question.

DEFINITION 2. Let M be a non-empty set. Recall that $M \times M$ denotes the set of all ordered pairs (a, b) of elements $a, b \in M$. A (**binary**) **relation** on M is a subset r of $M \times M$. The relation

$$\Delta(M) = \{(a, a) \mid a \in M\},$$

is called the **diagonal** of M. If r, s are relations on M, then

$$r^{-1} = \{(a, b) \mid (b, a) \in r\}$$

is the**inverse relation** of r, and

$$r \circ s = \{(a, c) \mid \text{exists } b \in M : (a, b) \in r, (b, c) \in s\}$$

is the**product, or composition,** of the two relations r and s. If $r \subseteq s$, then s is called an extension of r. We say that a relation r has **strict part** r_s meaning that $r_s = r \setminus r^{-1}$.

REMARK 3. For a relation r on M, given two elements $a, b \in M$, we write $a\, r\, b$ instead of $(a, b) \in r$.

DEFINITION 4. Let r be a relation on M. Then r is called

1) **reflexive** if $\Delta(M) \subseteq r$,

2) **symmetric** if $r \subseteq r^{-1}$,

3) **transitive** if $r \circ r \subseteq r$,

4) **antisymmetric** if $r \cap r^{-1} \subseteq \Delta(M)$,

5) **connex** if $r \cup r^{-1} = M \times M$,

6) **irreflexive** if $\Delta(M) \cap r = \emptyset$,

7) **strictly antisymmetric** if $r \cap r^{-1} = \emptyset$,

8) an **equivalence relation** on M if r is reflexive, symmetric, and transitive,

9) a **quasi-order** on M if r is reflexive and transitive,

10) a **partial order** on M if r is reflexive, transitive, and antisymmetric,

11) a (**linear**) **order** on M if r is a connex partial order on M, and

12) a **linear quasi-order** on M if r is a connex quasi-order on M.

Remark 5. For a symmetric relation, it is also true that $r = r^{-1}$. However, for a transitive relation $r = r \circ r$ is not necessarily true, for instance if $r = \{(a, b)\}$, then $r \circ r = \emptyset$.

Remark 6. We know that the natural ordering $\leq$ on $\mathbb{N}$ satisfies the trichotomy law; that is, if $<$ is the strict part of $\leq$ and $a, b \in \mathbb{N}$, one and only one of the conditions $a < b$, $b < a$ and $a = b$ is satisfied. Hence, if a relation r is connex and antisymmetric, then r satisfies the trichotomy law.

Example 7.

1) Given a set X, inclusion of sets $\subseteq$ is a partial order on $\mathcal{P}(X)$.

2) Divisibility relation is a partial order on $\mathbb{N}$.

3) less-or-equal $\leq$ is a linear order on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Definition 8. If r is a relation on M, we say that (M, r) is a **partially ordered set** (**totally ordered set**) if r is a partial order (a linear order). When we refer to a total ordered subset of a partially ordered set, we use the term **r-chain**.

Definition 9. A **partition** of a set M, is a subset Π of the power set $\mathcal{P}(M)$ of M such that the elements of Π are pairwise disjoint, non-empty subsets of M whose union equals M. A subset S of M is called a **system of unique representatives** for the partition Π of M if $P \cap S$ contains exactly one element for each $P \in \Pi$.

Whenever $\sim$ is an equivalence relation on M, then

$$[a] = \{b \in M \mid b \sim a\}$$

is called the **equivalence class** of a with respect to $\sim$, and the set

$$\{[a] \mid a \in M\}$$

of all equivalence classes is denoted by $M/\sim$.

DEFINITION 10. Let r be a relation on M with strict part r_s and let $N \subseteq M$. Then an element $a \in N$ is called **r-minimal** (**r-maximal**) in N if there is no $b \in N$ with br_sa (with ar_sb).
A **strictly descending** (**strictly ascending**) r-chain in M is an infinite sequence $\{a_n\}_{n\in\mathbb{N}}$ of elements of M such that $a_{n+1}r_sa_n$ (such that $a_nr_sa_{n+1}$) for all $n \in \mathbb{N}$.
The relation r is called **well-founded** (**noetherian**) if every non-empty subset N of M has a r-minimal (a r-maximal) element.
The relation r is a **well-order** on M if r is a well-founded linear order on M.

REMARK 11. An element a is r-minimal (r-maximal) in N iff bra implies arb (iff arb implies bra) for $b \in N$.

PROPOSITION 12. *Let r be a relation. Then r is well-founded (noetherian) iff there are no strictly descending (no strictly ascending) r-chains in M.*

PROOF. If $\{a_n\}_{n\in\mathbb{N}}$ is a strictly descending r-chain in M, then the set

$$N = \{a_n \mid n \in \mathbb{N}\}$$

has no r-minimal element. Conversely, suppose $\emptyset \neq N \subseteq M$ and has no r-minimal element. Then the set

$$A_a = \{b \in N \mid br_sa\}$$

is not empty for each $a \in N$. The axiom of choice, applied to the family $\{A_a\}_{a\in N}$, provides a function

$$f : N \to \cup_{a\in N} A_a \subseteq N,$$

with $f(a)\, r_s a$ for all $a \in N$. Let $a_0 \in N$. Now the sequence $\{a_n\}_{n\in\mathbb{N}}$ defined recursively by $a_{n+1} = f(a_n)$ forms a strictly descending r-chain. The noetherian case is handled analogously. □

DEFINITION 13. Let r be a relation on M. Then $r \cup r^{-1}$ is obviously the smallest relation extending r that is symmetric on M. It is called the **symmetric closure** of r.
We define the **powers** r^n with $n \in \mathbb{N}$ recursively by

$$r^0 = \Delta(M) \text{ and } r^{n+1} = r \circ r^n.$$

Then we call

$$r^+ = \cup_{n=1}^{\infty} r^n,$$

the **transitive closure** of r, and

$$r^* = \cup_{n=0}^{\infty} r^n = r^0 \cup r^+,$$

the **reflexive-transitive closure** of r.

REMARK 14. One can easily prove, by induction, that a pair $(a, c) \in r^n$ with $n \geq 2$ if and only if there exists a sequence $b_1, b_2, ..., b_{n-1}$ so that $arb_1rb_2r...rb_{n-1}rc$.
We now show that r^+ is in fact transitive: If $(a, c) \in r^+ \circ r^+$, then there exist $b \in M$ so that $(a, b), (b, c) \in r^+$; thus there exists $m, n \geq 1$ such that $(a, b) \in r^m, (b, c) \in$

r^n, and so, by the previous observation, there exist sequences $a_1, a_2, ..., a_{m-1}$ and $b_1, b_2, ..., b_{n-1}$ so that

$$ara_1ra_2r...ra_{m-1}brb_1rb_2r...rb_{n-1}rc.$$

By joining the sequence, we have a sequence of $m+n-1$ elements, which shows that $(a,c) \in r^{m+n-1} \subseteq r^+$, as desired.

Note that $r \subseteq r^+$ by definition and if r is transitive, then $r^N \subseteq r$ for all $N \geq 1$, and so $r^+ \subseteq r$, that is, if r is transitive, then $r = r^+$.

We now show that r^* is transitive (note that is reflexive by definition): If r^* is not transitive, then there exist $(a,b), (b,c) \in r^*$ but $(a,c) \notin r^*$. Hence $a \neq b \neq c$, and so $(a,b), (b,c) \in r^+$. Because r^+ is transitive, $(a,c) \in r^+ \subseteq r^*$, a contradiction.

In particular, if r is a symmetric relation, then r^+ and r^* are also symmetric. This is immediate from the fact that if $a, b \in M$ and ar^*b, then either $a = b$ or ar^+b and so there exists a chain

$$ara_1ra_2r...ra_{n-1}rb \ \ (n \geq 2, a_1, a_2, ..., a_{n-1} \in M),$$

and since r is symmetric, we have

$$bra_{n-1}r...ra_2ra_1ra,$$

that is, $(b,a) \in r^n \subseteq r^+ \subseteq r^*$.

Definition 15. Given a quasi-order $\preceq$ on a set M, the relation $\sim$ on M defined as $\preceq \cap (\preceq)^{-1}$ (that is, $a \sim b$ iff $a \preceq b$ and $b \preceq a$) is an equivalence relation which we shall refer to as the **associated equivalence relation** of $\preceq$. Whenever $N \subseteq M$ and $\sim$ is the associated equivalence relation of a quasi-order $\preceq$, we may restrict $\sim$ to N, so that $[a] \cap N$ for $a \in N$ are the equivalent classes in N. In case a is $\preceq$-minimal, we call the restricted equivalent class $[a] \cap N$, **min-class** of N.

Definition 16. A set M together with a **binary operation** $* : M \times M \to M$ is said to be a **monoid** if $*$ verifies the following axioms:

1) $*$ is **associative**, i.e., $(a * b) * c = a * (b * c)$ for all $a, b, c \in M$, and
2) $*$ has **identity element**, i.e., there exists $e \in M$ with $e * a = a$ for all $a \in M$.

We represent a monoid by the pair $(M, *)$ and say that it is an **abelian monoid** if in addition $*$ is **commutative**, i.e., $a * b = b * a$ for all $a, b \in M$.

Instead of symbol $*$, we will use $+$ and $\cdot$, which are called additive and multiplicative notation. When using the additive notation, we write 0 for the identity element, whereas when using the multiplicative notation, we write 1 instead.

Definition 17. Let $(M, +)$ be an abelian monoid and let $\leq$ be a linear order on M with strict part $<$. Then we say $\leq$ is **admissible** if for all $a, b, c \in M$,

1) $0 \leq a$, and

2) $a < b$ implies $a + c < b + c$.

If $\leq$ is an admissible order on M, then we call $(M, \leq)$ an **ordered monoid**.

Definition 18. A **group** is a monoid $(M, *)$ for which all elements are invertible, i.e., for all $a \in M$ there exist $b \in M$ such that $a * b = e = b * a$. In this case b is said to be the inverse of a and also denoted by a^{-1}. An abelian group is an abelian monoid for which all elements are invertible.
A subset N of a group $(M, *)$ is called a subgroup of $(M, *)$ if $(N, *)$ is also a group.

DEFINITION 19. A **ring (with identity)** R is a triple $(R,+,\cdot)$ for which $(R,+)$ is an abelian group, $(R\setminus\{0\},\cdot)$ a monoid and $\cdot$ is distributive with respect to $+$, that is, for all $a,b,c\in R$ we have

$$\begin{aligned} a\cdot(b+c) &= (a\cdot b)+(a\cdot c) \text{ (left distributivity)} \\ (b+c)\cdot a &= (b\cdot a)+(c\cdot a) \text{ (right distributivity)} \end{aligned}$$

An element $0\neq a\in R$ is said to be a divisor of 0 if there exist an element $0\neq b\in R$ so that $a\cdot b=0$. A ring $(R,+,\cdot)$ is said to be

- a **commutative ring** if $(R,\cdot)$ is an abelian monoid.
- an **integral domain** if $(R,\cdot)$ is an abelian monoid and R has no zero divisors.
- a **division ring** if $(R\setminus\{0\},\cdot)$ is a group.
- a **field** if $(R\setminus\{0\},\cdot)$ is an abelian group.

We will say that R is a ring instead of $(R,+,\cdot)$ whenever no possible confusion occur.

DEFINITION 20. A **vector space** over a field K is a triple $(V,+,\cdot)$, where V is a set, $(V,+)$ is an abelian group and $\cdot : K\times V\to V$ is called scalar operation, and verifies

1) $a\cdot(b\cdot v)=(ab)\cdot v$, where the product ab is considered in K
2) $a\cdot(u+v)=a\cdot u+a\cdot v$,
3) $(a+b)\cdot v=a\cdot v+b\cdot v$,
4) $1\cdot v=v$, where 1 denotes the identity of the field,

for all $a,b\in K$, $u,v\in V$.

DEFINITION 21. For a vector space $(V,+,\cdot)$ over a field K, we say that a set $B\subseteq V$ is a **generating set** if for all $v\in V$, there exist $b_1,b_2,...,b_n\in V$, $\lambda_1,\lambda_2,...,\lambda_n\in K$ so that

$$v=\lambda_1 b_1+...+\lambda_n b_n.$$

We say that B is **linearly independent** if the relation

$$\lambda_1 b_1+...+\lambda_m b_m=0,$$

for some $b_1,b_2,...,b_m\in B$, $\lambda_1,\lambda_2,...,\lambda_m\in K$, implies $\lambda_1=\lambda_2=...=\lambda_m=0$. We say that $B\subseteq V$ is a **basis** if it is a linearly independent generating set.

REMARK 22. It is known that every vector space has a basis. The cardinal of such basis is referred as the **dimension** of the vectorial space.

DEFINITION 23. A subset I of R is called an **ideal** of R if $(I,+)$ is a subgroup of $(R,+)$ and for all $x\in I$, $r\in R$ we have $x\cdot r\in I$ and $r\cdot x\in I$. An ideal I is said to be **generated** by the set $F\subseteq R$, and write $I=\mathrm{Id}(F)$, if I is the intersection of all the ideals of R containing F. If $I=\mathrm{Id}(F)$ for a finite set F, we say that I is **finitely generated**; in this case, if $F=\{x_1,x_2,...,x_m\}$, then

$$I=\{a_1x_1b_1+...+a_mx_mb_m \mid r_i,b_i\in R\, i=1,...,m\}.$$

An ideal I generated by a unique element is said a **principal ideal**. A domain R so that every ideal is principal is called **principal ideal domain** (**P.I.D.**).

DEFINITION 24. Given a ring R, the set

$$R[X_1, X_2, ..., X_n] = \{\sum_{i=1}^{k} a_i X_1^{i_1} \cdot ... \cdot X_n^{i_n} \mid a_i \in R, i_j \in \mathbb{N} \text{ for } j = 1, ..., n,\ i = 1, ..., k\}$$

is called the **polynomial ring** over R in the indeterminates $X_1, X_2, ..., X_n$. Elements of $R[X_1, X_2, ..., X_n]$ are called polynomials whereas symbols $X_j^{i_j}$ are called the powers of X_j, and by convention, $X_j^0 = 1$ and $X_j^k \cdot X_j^r = X_k^{k+r}$.

REMARK 25. A basic fact is that if R has no zero divisors, then the polynomial ring $R[X_1, X_2, ..., X_n]$ is a ring (with identity) without zero divisors.

DEFINITION 26. In the ring $R[X]$, every polynomial is of the form $f = \sum_{i=0}^{d} a_i X^i$ for some $d \in \mathbb{N}$. We denote d by $\deg(f)$, and say that d is the **degree** of the polynomial f.

THEOREM 27 (Division Algorithm). *Let R be a ring (with identity) and let $f, g \in R[X]$ with $g \neq 0$ and $\deg(f) \geq \deg(g)$. Suppose that $g = a_d X^d + a_{d-1} X^{d-1} + ... + a_1 X + a_0$ where a_d has inverse in R, then there exist unique polynomials $q, r \in R[X]$ so that $f = qg + r$ with $r = 0$ or $r \neq 0$ and $\deg(r) < \deg(g)$.*

PROOF. See [4], page 39. □

REMARK 28. The polynomials g, q, r of the division algorithm are called divisor, quotient, and remainder of the division, respectively.

DEFINITION 29. Given a ring R, we say that R is **Noetherian** if satisfies **A.C.C.** (the ascending chain condition) on ideals, that is, given a $\subseteq$-chain on the set M of ideals of R,

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$$

there exist $N \in \mathbb{N}$ such that

$$I_N = I_{N+1} = I_{N+2} = ...$$

We say that R is **Artinian** if it satisfies **D.C.C.** (the descending chain condition) on ideals, that is, given a $\supseteq$-chain on the set M of ideals of R,

$$I_1 \supseteq I_2 \supseteq ... \supseteq I_n \supseteq ...$$

there exist $N \in \mathbb{N}$ such that

$$I_N = I_{N+1} = I_{N+2} = ...$$

REMARK 30. Note that by Proposition 12, a ring R is said Noetherian (Artinian) iff the relation $\subseteq$ is noetherian (well-founded).

THEOREM 31 (Hilbert's basis Theorem). *If R in noetherian, then $R[X_1]$ is also noetherian (and so is $R[X_1, X_2, ..., X_n]$).*

PROOF. See [5], page 54. □

DEFINITION 32. Let I be an ideal of $R[X_1, X_2, ..., X_n]$, then the equivalence relation $\equiv_I$ defined by

$$f \equiv_I f \text{ iff } f - g \in I$$

is called **congruence relation** modulo I on $R[X_1, X_2, ..., X_n]$. The set $R[X_1, X_2, ..., X_n] / \equiv_I$ has structure of ring, and it is called **residue class ring** of the ring of polynomials $R[X_1, X_2, ..., X_n]$.

REMARK 33. Whenever we write R or K, we understand that R is a commutative ring with identity and K is a field.

1.1. Simple Explanation of Gröbner Bases

An informal introduction of Gröbner basis is now performed in order to provide a simple idea.

Given an ideal I on $K[X_1, X_2, ..., X_n]$, we are interested in discerning whether a polynomial $f \in I$ or $f \notin I$ (membership problem). By Hilbert's basis Theorem, $K[X_1, X_2, ..., X_n]$ is noetherian, that is, every ideal is finitely generated, and so $I = \mathrm{Id}(F)$ for some finite family $F \subseteq K[X_1, X_2, ..., X_n]$. Best scenario, $f \in F$ and we are done. In other case, if $f \in I$ and $f \notin F$, then $f = a_1 f_1 + ... + a_m f_m$ for some $f_i \in F$ and $a_i \in K$. The idea of subtracting elements of F until the element f is *reduced to* 0, conforms the intuitive idea of the theory. Moreover, if we can't reduce f to 0 by subtracting elements of f we expect $f \notin I$, and so $f \in I$ iff f reduces to 0 modulo F (see Definition 87). However, in opposition to the univariate case, in which the division algorithm provides uniques residues, when subtracting form f elements $f_i \in F$ multiplied by scalars in K, one may reach different results depending on the election of the f_i. For instance, take $f = x^3y \in K[x, y]$ and $F = \{f_1, f_3\}$ where

$$\begin{aligned} f_1 :=& 3x^2y + 2xy + y + 9x^2 + 5x - 3, \\ f_3 :=& x^3y + x^2y + 3x^3 + 2x^2. \end{aligned}$$

By subtracting f_1 to f several times, we achieve the polynomial $g_1 = \frac{1}{9}xy + \frac{2}{9}y - 3x^3 + \frac{1}{3}x^2 + \frac{19}{9}x - \frac{2}{3}$; however, when subtracting f_3 to f, we get $g_3 = \frac{1}{2}xy + \frac{1}{2}y - 3x^2 + x^2 + \frac{3}{2}x - \frac{3}{2}$. We notice that $g_1 \neq g_3$, but also g_1, g_3 are *residues* of $f = x^3y$ with respect to F, that is, they can no longer be reduced by subtracting elements in F.

A Gröbner basis for an ideal I, is a finite family $G \subseteq K[X_1, X_2, ..., X_n]$ such that a polynomial $f \in I$, if and only if, f can be reduced to 0 by subtracting elements of G. An immediate characterization, is that G is a Gröbner basis if and only if the reduction of provides unique residues (on the further theory, unique normal form, see Definition 48). The fundamental theorem of the theory, Gröbner basis existence, claims that every ideal $I \subseteq K[X_1, X_2, ..., X_n]$ has a Gröbner basis. Another important result, Buchberger's algorithm, provides an algorithm to compute such a basis from a finite set F generating the ideal I, i.e., provided a finite set F such that $I = \mathrm{Id}(F)$.

As the reader may guess, Gröbner-bases theory generalizes the Euclidean algorithm from the univariate case to the multivariate, and from a single divisor to a finite family.

Our motivational problem for Gröbner-bases theory, is the problem of effectively computing on $K[X_1, X_2, ..., X_n]/I$ since membership of a polynomial f in a class $[g]$ is equivalent to membership of $f - g$ on the ideal I.

REMARK 34. In order to provide this text with useful examples, we selected from [2] those who are of our interest. In particular, the set $F = \{f_1, f_2, f_3\}$ with

$$\begin{aligned} f_1 &= 3x^2y + 2xy + y + 9x^2 + 5x - 3, \\ f_3 &= x^3y + x^2y + 3x^3 + 2x^2, \\ f_2 &= 2x^3y - xy + 6x^3 - 2x^2 - 3x + 3. \end{aligned}$$

will appear repeatedly in the examples given.

CHAPTER 2

Initials

This chapter is divided into 6 sections, in which the fundamental notions relating Gröbner-bases theory are exposed. Sections 2.1 and 2.2 introduce the reader to two types of relations, Dickson's relations and reduction relation, as well as some properties. Section 2.3 presents some aspects concerning *computer* computability and algorithms. Finally, sections 2.4, 2.5 and 2.6 specializes to relations on the ring of polynomials $K[X_1, X_2, ..., X_n]$, *context* in which Gröbner-bases theory will be developed.

2.1. Dickson's relations

We start the section with a definition.

DEFINITION 35. Let $\preceq$ be a quasi-order on M and let $N \subseteq M$. Then a subset B of N is called a **Dickson basis**, or simply a basis of N w.r.t. (with respect to) $\preceq$ if for every $a \in N$ there exist some $b \in B$ with $b \preceq a$. We say that $\preceq$ has the **Dickson property**, or that is a **Dickson quasi-order**, if every subset N of M has a finite basis w.r.t. $\preceq$.

LEMMA 36. *Every well-founded linear quasi-order has the Dickson property. In particular, every well-order has the Dickson property.*

PROOF. Assume that $\preceq$ is a linear quasi-order on a set M. If N is a subset of M, then N has a minimal element b. Because the relation $\preceq$ is connex, we have $b \preceq a$ or $a \preceq b$ for every $a \in M$. Given that b is minimal, $a \preceq b$ implies $b \preceq a$ and the set $B = \{b\}$ is a basis of $\preceq$. □

Indeed, we will further see that every Dickson quasi-order is well-founded.

PROPOSITION 37. *Let $\preceq$ be a quasi-order on M with associated equivalence relation $\sim$. Then the following are equivalent:*

1) *$\preceq$ is a Dickson quasi-order,*

2) *whenever $\{a_n\}_{n\in\mathbb{N}}$ is a sequence of elements of M, then there exist $i, j \in \mathbb{N}$ with $i < j$ and $a_i \preceq a_j$,*

3) *for every non-empty subset N of M, the number of min-classes in N is finite and non-zero.*

PROOF. (i)⇒(ii): Set $N = \{a_n \mid n \in \mathbb{N}\}$ $j > i$ for all $i \in \mathbb{N}$ with $a_i \in B$. Then $a_i \preceq a_j$ for some $a_i \in B$ with $i < j$.

(ii)⇒(iii): Suppose there exist infinitely many min-classes in some non-empty subset N of M. Using the axiom of choice, we get an infinite sequence $\{a_n\}_{n\in\mathbb{N}}$ of pairwise $\sim$-inequivalent minimal elements of N. By (ii), $a_i \preceq a_j$ for some $i < j$.

From the minimality of a_j, we conclude that $a_j \preceq a_i$ and so $a_i \sim a_j$, a contradiction. On the other hand, if N has no minimal element, then we can produce a strictly descending $\preceq$-chain as in the proof of Proposition 12, contradicting (ii).

(iii)⇒(i): Let N be a non-empty subset of M. Choosing one element of each of the finitely many min-classes, we form a finite subset B of N such that each $b \in B$ is $\preceq$-minimal in N. We claim that B is a basis of N. If $a \in N$ then

$$N' = \{d \in N \mid d \preceq a\}$$

is a non-empty set since $a \in N'$ and so there exists $c \in N'$ that is $\preceq$-minimal in N'. In addition, if $c' \in N$ is such that $c' \preceq c \preceq a$, then $c' \preceq a$ and by minimality of c, $c \preceq c'$, that is, c is $\preceq$-minimal in N too. Hence, $c \sim b$ for some $b \in B$ and $b \preceq c \preceq a$, as required. □

COROLLARY 38. *Let $\leq$ be a Dickson partial order on M. Then every non-empty subset N of M has a unique **minimal finite basis** B, i.e., a finite basis B such that $B \subseteq C$ for all other bases C of N. In particular, B consists of all minimal elements of N.*

PROOF. From the above proposition, the set B of all minimal elements of N forms a basis of N. Let now C be another basis of N. Then for every $b \in B$ there exists some $c \in C$ such that $c \leq b$, and so $c = b$ by the minimality of b. This shows that $B \subseteq C$. □

The following theorem is an immediate consequence of the condition (iii) from the above proposition.

THEOREM 39. *Every Dickson quasi-order is well-founded.*

REMARK 40. If $\preceq$ is a Dickson's quasi-order on a set M, and $N = \{a_n\}_{n\in\mathbb{N}}$ is an infinite subset of M, given $a_i \in N$ we define **the set of superior elements of** a_i as

$$S(a_i) = \{a_n \in N \mid a_i \preceq a_n\}.$$

If $B = \{b_1, b_2, ..., b_k\}$ is a finite basis of N, then $\cup_{j=1}^{k} S(b_j) = N$ is infinite, and so $S(b_j)$ has infinitely many elements for some $1 \leq j \leq k$. As to simplify the proof of the following result, we define $\mathbb{N}_{S(a_i)}$ as the set of indexes of elements in $S(a_i)$, that is, $\mathbb{N}_{S(a_i)} = \{n \in \mathbb{N} \mid a_n \in S(a_i)\}$. For short, we simply write S_i and $\mathbb{N}_i$ for the sets $S(a_i)$ and $\mathbb{N}_{S(a_i)}$. Clearly $\mathbb{N}_i$ and S_i have the same cardinality.

PROPOSITION 41. *Let $\preceq$ be a Dickson quasi-order on M, and let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of elements of M. Then there exist a strictly ascending sequence of natural numbers, $\{n_i\}_{i\in\mathbb{N}}$ such that $a_{n_i} \preceq a_{n_j}$ for all $i < j$.*

PROOF. Along the proof, we will use the notation introduced in the previous Remark. We define the sequence $\{n_i\}_{i\in\mathbb{N}}$ recursively so that in the end it verifies

1) $a_{n_i} \preceq a_{n_{i+1}}$ for all $i \in \mathbb{N}$, and

2) for all $i \in \mathbb{N}$, the set $\mathbb{N}_{n_i}$ is infinite.

For $i = 0$, we set $N = \{a_n \mid n \in \mathbb{N}\}$ and using the previous remark, there exist a finite basis B of N and $b_j \in B$ so that $S(b_j)$ is infinite. Now, because $b_j \in N$, it is of the form $b_j = a_m$. We set $n_0 = m$ and clearly $\mathbb{N}_{n_0} = \mathbb{N}_{S(b_j)}$ is infinite, thus claim (ii) for $i = 0$ follows.

Consider defined the sequence $n_0, n_1, n_2, ..., n_i$ so that $a_{n_j} \preceq a_{n_{j+1}}$ for $0 \leq j < i$ and $\mathbb{N}_{n_j}$ is infinite for $1 \leq j \leq i$. Now we have to define $a_{n_{i+1}}$ so it verifies $a_{n_i} \preceq a_{n_{i+1}}$ and $\mathbb{N}_{n_{i+1}}$ is infinite.

Since $\mathbb{N}_{n_i}$ is infinite, the sequence $N' = S_{n_i}$ is also infinite. Using the previous remark, now applied to N', there exists b'_j in a finite basis of N' so that $S'\left(b'_j\right) = \left\{a_n \in N' \mid b'_j \preceq a_n\right\}$ is infinite. Because $n'_j \in N' = S_{n_i}$, $b'_j = a_{m'}$ for some $m \in \mathbb{N}$ and $a_{n_i} \preceq a_{m'}$. Now we set $n_{i+1} = m$ and trivially $\mathbb{N}_{n_i+1} = \left\{n \in \mathbb{N} \mid a_{n_{i+1}} = b'_j \preceq a_n\right\}$ is infinite since the set $S'\left(b'_j\right)$ is infinite and $N' \subseteq N$.

Note that the sequence of natural numbers is not necessarily an ascending sequence. However, we can easily correct this, it suffices to change the definition of $S(a_i)$ so that $S(a_i) = \{a_n \in N \mid a_i \preceq a_n \textbf{ and } i < n\}$. Then $S(a_i)$ is infinite w.r.t. the new definition, if and only if, it is infinite w.r.t. the previous one. Because $n_{i+i} = m'$ where $a_{m'} \in S(a_{n_i})$ then $n_i < n_{i+1}$ and we are done. □

Definition 42. Let $(M, \preceq)$ and $(N, \preceq)$ be quasi-ordered sets. Then we define $\preceq'$ on $M \times N$ as follows:

$$(a, b) \preceq' (c, d) \text{ iff } a \preceq c \text{ and } b \preceq d$$

for $(a, b), (c, d) \in M \times N$. Note that $\preceq'$ is reflexive and transitive, that is, a quasi-order.

For a finite family of quasi-ordered sets, $\{(M_i, \preceq)\}_{i=1}^n$ the direct product is defined by

$$(a_1, a_2, ..., a_n) \preceq (b_1, b_2, ..., b_n) \text{ iff } a_i \preceq b_i \text{ for all } 1 \leq i \leq n.$$

Now, we are ready to prove the main result of this section, and its corollaries, among which Dickson's Lemma is the most relevant.

Theorem 43. *Let $(M, \preceq)$ and $(N, \preceq)$ be Dickson quasi-ordered sets, and let $(M \times N, \preceq')$ be their direct product. Then $(M \times N, \preceq')$ is a Dickson quasi-ordered set.*

Proof. We verify (ii) of Proposition 37. Let $\{(a_n, b_n)\}_{n \in \mathbb{N}}$ be a sequence of elements of $M \times N$. By Proposition 41, there exists a strictly ascending sequence $\{n_i\}_{i \in \mathbb{N}}$ such that $a_{n_i} \preceq a_{n_j}$ for all $i < j$. By (ii) of Proposition 37 applied to the sequence $\{b_{n_i}\}_{i \in \mathbb{N}}$, there exist $i < j$ with $b_{n_i} \preceq b_{n_j}$, and thus $(a_{n_i}, b_{n_i}) \preceq' \left(a_{n_j}, b_{n_j}\right)$. □

Corollary 44. *Let $(M_i, \preceq)$ be a Dickson quasi-orders sets for $1 \leq i \leq n$, and let $(M, \preceq')$ be the direct product of the $(M_i, \preceq')$. Then $(M, \preceq')$ is a Dickson quasi-ordered set.*

Corollary 45 (Dickson's Lemma). *Let $(\mathbb{N}^n, \preceq')$ be the direct product of n copies of the natural numbers $(\mathbb{N}, \leq)$ with its natural ordering. Then $(\mathbb{N}^n, \preceq')$ is a Dickson partially ordered set. More explicitly, every subset S of $\mathbb{N}^n$ has a finite subset B such that for every $(m_1, m_2, ..., m_n) \in S$, there exists $(k_1, k_2, ..., k_n) \in B$ with $k_i \leq m_i$ for $1 \leq i \leq n$.*

2.2. Reduction relations

The goal of this section is to provide the necessary notions for the formalization of what has been roughly explained in the Prelude about reducing a polynomial f to 0, and subtracting elements form F to f.

DEFINITION 46. Let $\to$ be a relation on a non-empty set M. Then $\to$ is called a **reduction relation** on M if $\to$ is strictly antisymmetric. We say that $a \in M$ is **reducible** with respect to $\to$ if there exist $b \in M$ with $a \to b$ (reads a reduces to b). In connection with a reduction relation $\to$ on M, we will write

1) $\overset{*}{\to}$ for the **reflexive-transitive closure** of $\to$,

2) $\leftrightarrow$ for the **symmetric closure** of $\to$, i.e., $a \leftrightarrow b$ iff $a \to b$ or $b \to a$ for $a, b \in M$,

3) $\overset{*}{\leftrightarrow}$ for the **reflexive-transitive closure** of $\leftrightarrow$, i.e., the smallest equivalence relation on M extending $\to$,

4) $\overset{n}{\to}$ for $(\to)^n$ (where the exponent refers to the definition of powers or a relation given in definition 13)

5) $\overset{n}{\leftrightarrow}$ for $(\leftrightarrow)^n$, and

6) $\downarrow$ for the relation on M defined by $a \downarrow b$ iff there exists $c \in M$ with $a \overset{*}{\to} c \overset{*}{\leftarrow} b$.

REMARK 47. The relations $\overset{*}{\to}, \leftrightarrow, \overset{*}{\leftrightarrow}$ are no longer strictly antisymmetric. In particular, $\overset{*}{\to}$ is an antisymmetric quasi-order, and $\overset{*}{\leftrightarrow}$ is a partial order.

DEFINITION 48. An element $a \in M$ is said to be in **normal form**, or a **normal form**, with respect to $\to$ if a is $\to$-maximal in M. We say that $b \in M$ is a **normal form of** $a \in M$ with respect to $\to$ if $a \overset{*}{\to} b$ and b is in $\to$-normal form. Often we just say that an element is in normal form when it is clear the reduction relation we are dealing with.

As we will see in Section 4.2 and pointed out before in Section 1.1, normal forms are the generalization of the residue in Euclid's algorithm.

Our first result is a sufficient condition for the existence of such *residues*.

LEMMA 49. *If $\to$ is a noetherian reduction relation on M, then each $a \in M$ has at least one normal form $a' \in M$ with respect to $\to$.*

PROOF. The set $N = \left\{ b \in M \mid a \overset{*}{\to} b \right\}$ is a non-empty set because $a \in N$, and so N contains a $\to$-maximal element. □

What is worth noticing of the above result is that the element a and the set M play no role in the existence of the normal form of a w.r.t. M. This shows the importance of the reduction that we choose, in particular, the noetherian property will always be desired for a reduction relation.

We give now a sufficient condition for a relation to be noetherian.

LEMMA 50. *Let r be a well-founded relation on M with strict part r_s, and assume that $a \to b$ implies br_sa. Then $\to$ is a noetherian reduction relation on M.*

PROOF. We use the characterization shown in Proposition 12. Assume M has a strictly ascending $\to$-chain $\{a_n\}_{n\in\mathbb{N}}$. Then $\{a_n\}_{n\in\mathbb{N}}$ is a strictly descending chain r-chain, and has and r-minimal element a_n, since r is a well-founded relation. Then, $a_n r_s a_{n+1}$ and $a_{n+1} r_s a_n$, a contradiction. □

DEFINITION 51. Let $\to$ be a reduction relation on M. Then $\to$ is said

1) to be **locally confluent** if $b \leftarrow a \to c$ implies $b \downarrow c$ for all $a, b, c \in M$,

2) to be **confluent** if $b \overset{*}{\leftarrow} a \overset{*}{\to} c$ implies $b \downarrow c$ for all $a, b, c \in M$,

3) to have the **Church-Rosser property** if $b \overset{*}{\leftrightarrow} c$ implies $b \downarrow c$ for all $b, c \in M$,

4) to have **unique normal form** if $b \overset{*}{\leftarrow} a \overset{*}{\to} c$ with b and c in $\to$-normal form implies $b = c$ for all $a, b, c \in M$.

The following result establishes the equivalence of the above numbered sentences. Remark that (iv) is the desired property for a set G to be Gröbner basis (given an adequate reduction by elements of G), and so the result is crucial for the Gröbner-bases theory.

THEOREM 52 (Newman's Lemma). *Let $\to$ be a noetherian reduction relation on M. Then the following are equivalent:*

1) $\to$ is locally confluent,

2) $\to$ is confluent,

3) $\to$ has unique normal form,

4) $\to$ has the Church-Rosser property.

PROOF. (i)⇒(ii): Assume for a contradiction that $\to$ is locally confluent, but the set

$$N = \left\{ a \in M \mid \text{there exist } b, c \in M \text{ with } b \overset{*}{\leftarrow} a \overset{*}{\to} c, \text{ but not } b \downarrow c \right\}$$

is non-empty. Since $\to$ is noetherian, N has a $\to$-maximal element, say a, and let $b, c \in M$ with $b \overset{*}{\leftarrow} a \overset{*}{\to} c$ but not $b \downarrow c$. Thus, $a \neq b$ and $a \neq b$ since otherwise $b \downarrow c$, and there exist $b', c' \in M$ with

$$b \overset{*}{\leftarrow} b' \leftarrow a \to c' \overset{*}{\to} c.$$

Because $\to$ is locally confluence there exist $d \in M$ with $b' \overset{*}{\to} d \overset{*}{\leftarrow} c'$. Hence, we have $b \overset{*}{\leftarrow} b' \overset{*}{\to} d$ with $a \to b'$; by the maximality of a in N, $b \downarrow d$ and so there exist $e \in M$ with

$$b \overset{*}{\to} e \overset{*}{\leftarrow} d.$$

In addition, we have $e \overset{*}{\leftarrow} c' \overset{*}{\to} c$ with $a \to c'$, and so by minimality of a in N a $e \downarrow c$ and there exists $f \in M$ with

$$e \overset{*}{\to} f \overset{*}{\leftarrow} c.$$

In summary, we have proved $b \overset{*}{\to} e \overset{*}{\to} f \overset{*}{\leftarrow} c$, a contradiction.

(ii)⇒(iii): If $b \overset{*}{\leftarrow} a \overset{*}{\to} c$, by(ii) there exists $d \in M$ with $b \overset{*}{\to} d \overset{*}{\leftarrow} c$. If b and c are in $\to$-normal form, then $b = d = c$.

(iii)⇒(iv): We show by induction on $k \in \mathbb{N}$ that for all $a, b \in M$ with $a \overset{k}{\leftrightarrow} b$ it follows that $a \downarrow b$. The case $k = 0$ is trivial. Let now $a \overset{k+1}{\leftrightarrow} b$, say

$$a \overset{k}{\leftrightarrow} c \leftrightarrow b.$$

then by induction hypothesis there exists $d \in M$ with $a \xrightarrow{*} d \xleftarrow{*} c$. If $c \leftarrow b$ we are done. Consider the case $c \rightarrow b$ and let d', b' be $\rightarrow$-normal forms of d and b respectively. Then

$$d' \xleftarrow{*} d \xleftarrow{*} c \xrightarrow{*} b \xrightarrow{*} b',$$

and so d' and b' are normal forms of c. Hence, by (iii), $d' = b'$ and $a \xrightarrow{*} d \xrightarrow{*} d' \xleftarrow{*} b$, that is $a \downarrow b$.

(iv)⇒(i): Let $b \leftarrow a \rightarrow c$. Then $b \overset{*}{\leftrightarrow} c$, and so $b \downarrow c$ by (iv). □

COROLLARY 53. *Let $\rightarrow$ be a locally confluent, noetherian reduction relation on M and let $a, b \in M$. Then the following are equivalent:*

1) $a \overset{*}{\leftrightarrow} b$,
2) *whenever a' and b' are normal forms of a and b w.r.t. $\rightarrow$, then $a' = b'$.*

PROOF. The converse implication is obvious. For the direct implication, we trivially have that $a' \overset{*}{\leftrightarrow} b'$ and by the Church-Rosser property, $a' \rightarrow c \leftarrow b'$ for some $c \in M$. Because a', b' are in $\rightarrow$-normal form, $a' = c = b'$ as required. □

REMARK 54. As we show early, noetherian condition is desired for a reduction relation. From the previous results we see that a relation being locally confluent is also important for our purpose since it provides unique normal form. Moreover, the reflexive-symmetric-transitive closure of the relation will be an important object of our study.

2.3. Computations and Algorithms

Since the goal of Gröbner bases and Buchberger's algorithm is to offer a method for computing on the residue class ring $K[\mathbf{X}]/I$, typically using a computer, this chapter focuses on concepts related to algorithms and the computability of operations.

DEFINITION 55. A set M is **decidable** if its elements are given in such a way that there is an algorithm which, upon input of $a, b \in M$, decides whether $a = b$, or not.

DEFINITION 56. Let $\rightarrow$ be a reduction relation on M and let $\sim$ be an equivalence relation on M. Then we call $\rightarrow$ **adequate** for $\sim$ if $\sim$ coincides with the reflexive-symmetric-transitive closure $\overset{*}{\leftrightarrow}$ of $\rightarrow$. We say $\rightarrow$ is **decidable** if there is an algorithm which, on the input of $a \in M$, decides whether a is reducible with respect to $\rightarrow$, and if so selects some $b \in M$ with $a \rightarrow b$.

THEOREM 57. *Let $\sim$ be an equivalence relation on a non-empty set M. Let $\rightarrow$ be a locally confluent noetherian reduction relation on M that is adequate for $\sim$, and suppose M and $\rightarrow$ are decidable. Then there exists an algorithm which, on input of $a, b \in M$, decides whether $a \sim b$ or not.*

PROOF.

Algorithm 1 EQUIV

Specification: $v \leftarrow \text{EQUIV}\,(a, b)$
Test whether $a \sim b$
Given: $a, b \in M$
Find: $v \in \{\textbf{true}, \textbf{false}\}$ such that $v = \textbf{true}$ iff $a \sim b$
begin EQUIV
$A \leftarrow a$; $B \leftarrow b$;
while A is reducible w.r.t. $\rightarrow$ **do**
select $C \in M$ with $A \rightarrow C$
$A \leftarrow C$
end
while B is reducible w.r.t. $\rightarrow$ **do**
select $D \in M$ with $B \rightarrow D$
$B \leftarrow D$
end
if $A = B$
return(true)
else
return(false)
end
end EQUIV

Termination: An infinite loop would provide an infinite ascending $\rightarrow$-chain, contradicting the fact that $\rightarrow$ is noetherian.

Correctness: By definition, $a \sim b$ iff $a \overset{*}{\leftrightarrow} b$. Moreover, if a', b' are normal forms of a, b, by Corollary 53, $a \sim b$ iff $a' = b'$ and the algorithm is correct. □

REMARK 58. Provided a relation $\sim$ and a reduction relation $\rightarrow$ as in the theorem above, the set $\{h \in M \mid h \text{ is in } \rightarrow\text{-normal form}\}$ is a system of unique representatives for the partition $M/\sim$ of M.

Because we are not at the point to define a noetherian reduction relation, we will later see an example of the above algorithm (Example 141).

DEFINITION 59. A monoid M (a ring R) is called **computable** if the elements of M (of R) are given in such a way that M (R) is decidable as a set, and there is an algorithm (there are algorithms) which, upon input of $a, b \in M$ (if $a, b \in R$) computes $ab \in M$(computes $ab, a + b$ and $-a \in R$). A field K is called a **computable field** if it is computable as a ring and there is an algorithm which, upon input of $0 \neq a \in K$, computes $a^{-1} \in K$. An order $\leq$ is called **decidable** if there is an algorithm that decides, for $a, b \in M$, whether $a \leq b$.

The following example constitutes an apéritif for the computation on the polynomial residue ring $K[X_1, X_2, ..., X_n]/I$.

EXAMPLE 60. Let R be a computable ring, $\{0\} \neq I$ an ideal of R such that there is an algorithm which, upon input $a \in R$, decides whether $a \in I$, or not. We claim that the residue class R/I is a computable ring. The elements $a + I$ of R/I, are obviously given as elements of R, viewed as residue class modulo I. Two elements a and b of R, represent the same residue class iff $a - b \in I$, a condition

which we can effectively test by our assumption on I. Addition, subtraction, and multiplication in R/I are performed by doing the respective in R on representatives, which is possible by the assumption on R.

2.4. Term Orders

On Euclid's algorithm, the notion of degree of a polynomial is as essential as clear. However, on the multivariate case, no notion of degree of a polynomial seems obvious since the many possibilities one can think. This section is devoted to term orders, that is, (linear) orders on the variables and to introduce the notion of degree in the multivariate case.

DEFINITION 61. A **term** t in the indeterminates, or variables, $X_1, X_2, ..., X_n$ is a power product of the form $t = X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}$ with $e_i \in \mathbb{N}$ for $i = 1, ..., n$; in particular $1 = X_1^0 \cdot ... \cdot X_n^0$ is a term. We denote by $T(X_1, X_2, ..., X_n)$, or simply by T, the set of all terms in these variables. The set T forms an abelian (multiplicative) monoid with identity element 1 w.r.t. the natural multiplication.

REMARK 62. Note that two terms are different, if and only if, their exponent tuples are different. This means that the abelian monoids $(T, 1, \cdot)$ and $(\mathbb{N}^n, (0, ..., 0), +)$ are isomorphic via the **exponent map** $\eta : T \to \mathbb{N}^n$ given by $\eta(X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}) = (e_1, e_2, ..., e_n)$.

DEFINITION 63. The partial order $\leq'$ on $\mathbb{N}^n$ defined by

$$(k_1, k_2, ..., k_n) \leq' (m_1, m_2, ..., m_n) \text{ iff } k_i \leq m_i \text{ for } i = 1, ..., n$$

is called **natural partial order** on $\mathbb{N}^n$. The **divisibility relation** $|$ on T is defined by $s|t$ iff there exists $s' \in T$ with $s \cdot s' = t$. Clearly, $s|t$ iff $\eta(s) \leq' \eta(t)$ where $\leq'$ is the natural partial order on $\mathbb{N}^n$.

Although the divisibility relation in T could have been defined as in $R[X_1, X_2, ..., X_n]$, that is, $s \mid t$ if there is a $r \in R[X_1, X_2, ..., X_n]$ such that $t = rs$, the previous definition allows us to extend previous results about Dickson's quasi-orders to the division relation, in particular we have the following result.

THEOREM 64. *The divisibility relation $|$ on T is a Dickson partial order on T. More explicitly, every non-empty subset S of T has a finite subset B such that for all $s \in S$, there exists $t \in B$ with $t|s$.*

PROOF. This result is an immediate consequence Dickson's Lemma (Corollary 45). □

From the above theorem, we see that Dickson partial orders are indeed part of our study, and Section 2.1 represents no deviation from our goal.

DEFINITION 65. A **term order** is an admissible linear order for the monoid $(T, \cdot)$, i.e., is a linear order on T that satisfies the following conditions.

1) $1 \leq t$ for all $t \in T$.

2) $t_1 < t_2$ implies $t_1 \cdot s < t_2 \cdot s$ for all $s, t_1, t_2 \in T$.

REMARK 66. A term t is in correspondence with a tuple in $\mathbb{N}^n$ (of exponents of the variables $X_1, X_2, ..., X_n$). Therefore, any commutation of the variables is not allowed in a term. Given a polynomial f on $R[X_1, X_2, ..., X_n]$, we may reorder

the power products appearing in f as to form a term, and so we need the variables $X_1, X_2, ..., X_n$ to commute. For this reason, we set every ring R to be a commutative ring.

From the definition of term order, we see that the divisibility relation is a term order. But we can say more, every term order on T is paired with an admissible order in $\mathbb{N}^n$ and vice versa.

LEMMA 67. *Let $\leq$ be and admissible order on $(\mathbb{N}^n, (0, ..., 0), +)$, and define $\leq'$ on T by setting $s \leq' t$ iff $\eta(s) \leq \eta(t)$. Then $\leq'$ is a term order on T. Moreover, every term order on T is obtained in this way, and the resulting correspondence between term orders on T and admissible orders in $(\mathbb{N}^n, (0), +)$ is one-to-one.*

PROOF. Let $\leq$ be an admissible order on $(\mathbb{N}^n, (0), +)$. Then $\leq'$ is a term order on T, since $\eta(1) = \eta(0)$ and $\eta(s \cdot t) = \eta(s) + \eta(t)$. Using the fact that $\eta^{-1} : (\mathbb{N}^n, (0), +) \to (T, 1, \cdot)$ is an isomorphism, one easily proves that every order on T is obtained in this way, and that the correspondence is one to one. □

The following theorem is an immediate consequence of the theorem and lemma above. Property (ii) is also a consequence of Dickson's Lemma (Corollary 45).

THEOREM 68.

1) If $\leq$ is a term order on T, then $s \mid t$ implies $s \leq t$ for all $s, t \in T$.

2) Every term order is a well-order on T.

Some of the most common terms orders are given in the following definition.

DEFINITION 69. We define now some common term orders on T.

1) $X_1^{d_1} \cdot X_2^{d_2} \cdot \ldots \cdot X_n^{d_n} \leq X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}$ iff the following holds: $(d_1, d_2, ..., d_n) = (e_1, e_2, ..., e_n)$, or there exists $1 \leq i \leq n$ with $d_j = e_j$ for $j = 1, ..., i-1$ and $d_i < e_i$. This term order is called the **lexicographical**, or **lexical order** on T.

2) $X_1^{d_1} \cdot X_2^{d_2} \cdot \ldots \cdot X_n^{d_n} \leq X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}$ iff the following holds: $(d_1, d_2, ..., d_n) = (e_1, e_2, ..., e_n)$, or there exists $1 \leq i \leq n$ with $d_j = e_j$ for $j = i+1, ..., n$ and $d_i < e_i$. This term order is called the **inverse lexicographical**, or **inverse lexical order** on T.

3) Let $\leq$ be an order on T that satisfies condition: $t_1 \leq t_2$ implies $t_1 \cdot s \leq t_2 \cdot s$ for all $s, t_1, t_2 \in T$ (see Definition 65). Set
$$X_1^{d_1} \cdot X_2^{d_2} \cdot \ldots \cdot X_n^{d_n} \leq' X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}$$
iff the following condition holds:
$$\sum_{i=1}^{n} d_i < \sum_{i=1}^{n} e_i, \text{ or}$$
$$\sum_{i=1}^{n} d_i = \sum_{i=1}^{n} e_i, \text{ and } X_1^{d_1} \cdot X_2^{d_2} \cdot \ldots \cdot X_n^{d_n} \leq X_1^{e_1} \cdot X_2^{e_2} \cdot \ldots \cdot X_n^{e_n}.$$
This class of term orders is called the class of **total degree orders**. If $\leq$ is the lexicographical order, then the resulting term order is called the **total degree-lexicographical order**.

EXAMPLE 70. The polynomials f_1, f_2 and f_3 defined in Remark 34 are ordered w.r.t. the inverse lexicographical order.

Now, consider the polynomial in $K[x, y]$

$$f = x^2y^2 + x^2y + xy^2 + x^2 + y^2 + xy + x + y.$$

Then the polynomials

$$\begin{aligned} f_1 &= x^2y^2 + xy^2 + y^2 + x^2y + xy + y + x^2 + x, \\ f_2 &= x^2y^2 + x^2y + x^2 + xy^2 + xy + x + y^2 + y, \\ f_3 &= x^2y^2 + xy^2 + x^2y + y^2 + xy + x^2 + x + +y, \end{aligned}$$

are the representation of f w.r.t. the inverse lexicographical order, the lexicographical order and the total degree-inverse lexicographical order respectively. Note that by swapping the terms xy and y^2 if f, it would be ordered w.r.t. the total degree-inverse-inverse lexicographical order.

Previous to define an "ordering" on the polynomials, we present a polynomial as sum of terms, or tuple of terms, and make sure that representation is computable.

PROPOSITION 71. *Let M be the set of all monomials in $R[X_1, X_2, ..., X_n]$.*

1) *Let $\leq$ be a term order on T. Then every polynomial $f \in R[X_1, X_2, ..., X_n]$ has a unique representation as sum of monomials $\sum_{i=1}^{k} m_i$ with $m_i \in M$ and $m_1 > m_2 > ... > m_k$.*

2) *If, in addition, R is a computable ring and $\leq$ is a decidable order on T, there is an algorithm that computes the representation of (i) from any arbitrary representation of f as a sum of monomials.*

PROOF. Given the unique representation of f as sum of pairwise inequivalent monomials, $\sum_{i=1}^{k} m_i$, we can subtract the coefficient of each m_i to obtain a term t_i. By ordering the sequence $(t_i)_{i=1}^{k}$, say $t_{i_1} > t_{i_2} > ... > t_{i_k}$, where the strict part is possible since monomials m_i are pairwise inequivalent. We set $f = \sum_{j=1}^{k} m_{i_j}$, and the claims follows. Condition (ii) is now immediate from (i). □

REMARK 72. Note that m_i are monomials and not terms, so the relation $m_i > m_j$ must be understood as relation on the terms appearing in m_i, m_j. However, as in the proposition, we will write $m_1 > m_2 > ... > m_k$ since less notation is needed.

The previous result allows us to define the following.

DEFINITION 73. Given a polynomial $f \in R[X_1, X_2, ..., X_n]$, let $f = \sum_{i=1}^{k} m_i$ be the unique representation of f with m_i monomials of $R[X_1, X_2, ..., X_n]$ such that $m_1 > m_2 > ... > m_k$. Then we write $M(f) = \{m_i\}_{i=1}^{k}$ for **the set of all monomials of** f; $T(f)$ for **the set of all terms of** f, i.e., the set of all terms of monomials $m \in M(f)$; and $C(f)$ for **the set of all coefficients of** f.

When we omit the polynomial f, M (T) denotes **the set of all monomials** (**of all terms**) of $R[X_1, X_2, ..., X_n]$. We will also write $\mathrm{C}(t, f)$ for **the coefficient of the term** t **in** f.

2.5. Induced quasi-order of a term order

The aim of this section is to define a quasi-order on the polynomial ring $R[X_1, X_2, ..., X_n]$. As an anticipation, the resulting quasi-order is a consequence of the chosen ordering on T extended recursively on a polynomial using its representation as sums of monomials.

The following technical result will be later needed.

LEMMA 74. *Let $\preceq$ be a quasi-order on M with associated equivalence relation $\sim$, let $\leq$ be a well-founded partial order on N, and let $\varphi : M \to N$ be a map such that for all $a, b \in M$, the following hold:*

1) $a \preceq b$ implies $\varphi(a) \leq \varphi(b)$, and

2) $\varphi(a) = \varphi(b)$ implies $a \sim b$.

Then $\preceq$ is well-founded.

PROOF. Assume for a contradiction that $\{a_n\}_{n\in\mathbb{N}}$ is a strictly descending $\preceq$-chain. Then $\varphi(a_j) \leq \varphi(a_i)$ for $i < j$, and $\varphi(a_i) \neq \varphi(a_j)$ since otherwise $a_i \sim a_j$. Then $\{\varphi(a_n)\}_{n\in\mathbb{N}}$ form a strictly descending $\leq$-chain, a contradiction. □

DEFINITION 75. Let $(M, \leq)$ be an ordered set, and let $\mathcal{P}_{fin}(M)$ be the set of all finite subsets of M. Every $\emptyset \neq A \in \mathcal{P}_{fin}(M)$ obviously has a maximal and minimal element w.r.t. the order $\leq$. We denote these by $\max(A)$, and $\min(A)$, respectively. With $A' = A \setminus \{\max A\}$, we define a binary relation $\leq'$ on $\mathcal{P}_{fin}(M)$ as follows. Let $A, B \in \mathcal{P}_{fin}(M)$; then $A \leq' B$ is defined by recursion on the number $|A|$: if $A = \emptyset$, then $A \leq' B$. If $A \neq \emptyset$, then $A \leq' B$ iff $B \neq \emptyset$ and the following conditions holds:

$$\begin{aligned} \max(A) &< \max(B), \text{ or} \\ \max(A) &= \max(B) \text{ and } A' \leq' B'. \end{aligned}$$

The next result follows easily by induction, whereas the posterior one uses the Cantor's second diagonal argument.

LEMMA 76. *Let $(M, \leq)$, $\mathcal{P}_{fin}(M)$ and $\leq'$ be as in the definition above. Then $(\mathcal{P}_{fin}(M), \leq')$ is an ordered set.*

PROOF. $\leq'$ is reflexive: we argue by induction on $n = |A|$ for $A \in \mathcal{P}_{fin}(M)$ that $A \leq A$. It is clear from definition for $n = 0$. If $n > 0$, it follows by induction hypothesis that $A' \leq' A'$ since $|A'| < n$ and so $A \leq' A$ from definition.

$\leq'$ is transitive: assume that $A, B, C \in \mathcal{P}_{fin}(M)$ with $A \leq' B$ and $B \leq' C$. We use induction on $n = |A|$ to prove that $A \leq' C$. This is trivial if $n = 0$. If $n > 0$, then $A \neq \emptyset$, and so $B, C \neq \emptyset$. We thus have

$$\max(A) \leq \max(B) \text{ and } \max(B) \leq \max(C).$$

If at least one of the inequalities is strict, then it follows immediately that $A \leq' C$. If we have equality in both cases, then

$$A' \leq' B' \leq' C',$$

and so $A' \leq' C'$ by hypothesis induction. This together with $\max(A) = \max(C)$ implies that $A \leq' C$.

$\leq'$ is antisymmetric: suppose $A, B \in \mathcal{P}_{fin}(M)$ with $A \leq' B$ and $B \leq' A$. To prove that $A = B$, we proceed by induction on $n = |A|$. If $n = 0$, then $A = B = \emptyset$.

If $n > 0$, then both A, B must be non-empty, and we must have $\max(A) = \max(B)$ and both $A' \leq' B'$ and $B' \leq' A'$. The induction hypothesis now implies that $A = B$.

$\leq'$ is connex: let $A, B \in \mathcal{P}_{fin}(M)$. If $B = \emptyset$ then $B \leq' A$. For the remaining case, $B \neq \emptyset$ and we use induction on $n = |A|$ to prove that $A \leq' B$ or $B \leq' A$. This is trivial if $n = 0$. Finally, if $n > 0$, then either the maximal of A and B are different, in which case we are done, or they agree, in which case we apply induction hypothesis to A' and B'. □

THEOREM 77. *If $(M, \leq)$ is a well-ordered set, then so is $(\mathcal{P}_{fin}(M), \leq')$.*

PROOF. Assume for contradiction that there is a strictly descending $\leq'$-chain $\{A_n\}_{n\in\mathbb{N}}$ in $\mathcal{P}_{fin}(M)$. We will show there exist a strictly descending $\leq$-chain in M. We first note that $A_n \neq \emptyset$ for all $n \in \mathbb{N}$ by the definition of $\leq'$. We construct by recursion on $k \in \mathbb{N}$ a sequence

$$\left\{\left(a_k, \{B_{kn}\}_{n\in\mathbb{N}}\right)\right\}_{k\in\mathbb{N}},$$

formed by ordered pairs which the first component is an element of M, while the second component is a sequence of elements on $\mathcal{P}_{fin}(M)$. Moreover, we define the sequence in such a way so it verifies:

1) $\{B_{kn}\}_{n\in\mathbb{N}}$ is a strictly descending $\leq'$-chain in $\mathcal{P}_{fin}(M)$ for each $k \in \mathbb{N}$.

2) $a_k > \max(B_{kn})$ for all $n \in \mathbb{N}$.

For $k = 0$, let

$$C = \{\max(A_n) \mid n \in \mathbb{N}\},$$

and set $a_0 = \min(C)$. Now let j be the least index such that $a_0 \in A_j$. Then $a_0 = \max(A_n)$ for all $n \geq j$, since $\{A_n\}_{n\in\mathbb{N}}$ is a strictly descending $\leq'$-chain. If we now set $B_{0n} = A'_{j+n}$ for all $n \in \mathbb{N}$, then $a_0 = \max(A_{j+n}) > \max\left(A'_{j+n}\right)$ by definition of $\leq'$ and because $\max(A_{j+n}) = a_0 = \max\left(A_{j+(n+1)}\right)$, the fact $\{A_n\}_{n\in\mathbb{N}}$ is a strictly descending $\leq'$-chain implies $B_{0n} = A'_{j+n} > A'_{j+(n+1)} = B_{0n+1}$. Suppose we have defined the sequence up to the index k, let's now define the pair $\left(a_{k+1}, \left\{B_{(k+1)n}\right\}\right)$. Consider the set

$$D = \{\max(B_{kn}) \mid n \in \mathbb{N}\},$$

and define $a_{k+1} = \min(D)$. Let j be the least index such that $a_{k+1} \in B_{kj}$. Then $a_{k+1} = \max(B_{kj})$ for all $n \geq j$, and we set $B_{(k+1)n} = B'_{k(n+j)}$. As before, the fact that $\{B_{kn}\}_{n\in\mathbb{N}}$ is a strictly descending $\leq'$-chain and $\max\left(B_{k(j+n)}\right) = a_{k+1} = \max\left(B_{k(j+n+1)}\right)$, by definition of $\leq'$ we have $B_{(k+1)n} = B'_{k(j+n)} > B'_{k(j+n+1)} = B_{(k+1)(n+1)}$ and so $\left\{B_{(k+1)n}\right\}_{n\in\mathbb{N}}$ is a strictly descending $\leq'$-chain. Because $a_{k+1} = \max(B_{kj})$ for all $n \geq j$, the claim $a_{k+1} > \max\left(B'_{k(j+n)}\right) = \max\left(B_{(k+1)n}\right)$ is clear.

Finally, remark that $a_{k+1} \in B_{kn}$ for all $k \in \mathbb{N}$ by definition, and so $a_k > a_{k+1}$ for all $k \in \mathbb{N}$ by (ii). Hence, $\{a_k\}_{k\in\mathbb{N}}$ is a strictly descending $\leq$-chain in M, a contradiction since $\leq$ is well-founded. □

Specializing the above to our interest, the ring of polynomials, we can enunciate the following.

DEFINITION 78. Let $\leq$ be a term order on T and let $\leq'$ be the induced well-order on $\mathcal{P}_{fin}(T)$ of theorem above. We define a relation $\preceq$ on $R[X_1, X_2, ..., X_n]$ by setting

$$f \preceq g \text{ iff } T(f) \leq' T(g).$$

THEOREM 79. *Let $\leq$ be a term order on T. Then $\leq$ can be extended to a linear well-founded quasi-order $\preceq$ on $R[X_1, X_2, ..., X_n]$.*

PROOF. Consider the relation $\preceq$ defined above. The order $\leq'$ on $\mathcal{P}_{fin}$ upon which the definition of $\preceq$ is based is a linear order by Lemma 76, i.e., it is reflexive, transitive and connex. Trivially $\preceq$ inherits these properties. Moreover, we can apply Lemma 74 to $\preceq$ with $M = R[X_1, X_2, ..., X_n]$, $N = \mathcal{P}_{fin}(T)$ and $\varphi : R[X_1, X_2, ..., X_n] \to \mathcal{P}_{fin}(T)$ defined by $\varphi(f) = T(f)$, and so $\preceq$ is well-founded. □

REMARK 80. Theorem and definition above is of utmost importance for the Gröbner bases theory; whenever a term order $\leq$ has been fixed and $f \leq g$ occurs for some polynomials f, g, then it is the **induced (well-founded linear) quasi-order** $\preceq$ on $R[X_1, X_2, ..., X_n]$ that is being referred to.

EXAMPLE 81. Consider the polynomials $f = x^2y + y^2 + x$ and $g = x^2y + x^2 + y$ and $h = x^3 + y^2$.

If $\leq$ is both the inverse lexicographical order on T, and the induced quasi-order on $R[X_1, X_2, ..., X_n]$, then $\mathrm{HT}(f) = y^2$, $\mathrm{HT}(g) = x^2y$ and $\mathrm{HT}(h) = y^2$. Hence $f > g$ and $h > g$. Because $\mathrm{HT}(f) = \mathrm{HT}(h)$ we consider the polynomials $f' = f - \mathrm{HT}(f) = x^2y + x$ and $h' = h - \mathrm{HT}(h) = x^3$. Now, $\mathrm{HT}(f') = x^2y$ and $\mathrm{HT}(h') = x^3$ which implies $f' > h'$, and so $f > h$.

If we now consider the total degree-inverse lexicographical order. Then $\mathrm{HT}(f) = x^2y$,$\mathrm{HT}(g) = x^2y$ and $\mathrm{HT}(h) = x^3$. Hence $f > h$ and $g > h$. Now consider $f' = f - \mathrm{HT}(f) = y^2 + x$ and $g' = g - \mathrm{HT}(g) = x^2 + y$. Because $\mathrm{HT}(f') = y^2 > x^2 = \mathrm{HT}(g')$ we conclude that $f' > g'$, and so $f > g$.

2.6. Polynomial reductions

In this section we introduce reduction relations to the ring of polynomials over a field $K[X_1, X_2, ..., X_n]$.

Before to proceed with reduction relations, we give some definition that are useful in order to describe polynomials in a more precise way.

DEFINITION 82. Let $\leq$ be a term order on T. For any finite, non-empty subset A of M consisting of pairwise inequivalent monomials, we let $\max(A)$ be the unique maximal element of A w.r.t. $\leq$. For any non-zero polynomial $f \in R[X_1, X_2, ..., X_n]$ we define the **head term** $\mathrm{HT}(f)$, the **head monomial** $\mathrm{HM}(f)$, and the **head coefficient** $\mathrm{HC}(f)$ of f w.r.t. $\leq$ as follows:

$$\begin{aligned} \mathrm{HT}(f) &= \max(T(f)), \\ \mathrm{HM}(f) &= \max(M(f)), \text{ and} \\ \mathrm{HC}(f) &= \text{the coefficient of } \mathrm{HM}(f). \end{aligned}$$

Given an ideal I, we may also write

$$\begin{aligned} \mathrm{HT}(I) &= \{\mathrm{HT}(f) \mid f \in I\}, \text{ and} \\ \mathrm{HM}(I) &= \{\mathrm{HM}(I) \mid f \in I\}. \end{aligned}$$

The **reductum** $\mathrm{red}(f)$ of f w.r.t. $\leq$ is defined as $f - \mathrm{HM}(f)$, i.e., $f = \mathrm{HM}(f) + red(f)$. A polynomial $f \in R[X_1, X_2, ..., X_n]$ is called **monic** w.r.t. $\leq$ if $f \neq 0$ and $\mathrm{HC}(f) = 1$.

REMARK 83. If $f = \sum_{i=1}^{k} m_i$ is the unique representation of f with $m_1 > m_2 > ... > m_k$, $m_i \in M$, then $m_1 = \mathrm{HM}(f)$. In addition, $\mathrm{red}(f) = m_2 + ... + m_k < m_1$ follows from the definition of the relation and so $\mathrm{red}(f) < \mathrm{HM}(f) \leq f$ (note that $\leq$ denotes the relation $\preceq$ of Theorem 79).

REMARK 84. The induced quasi-order on $R[X_1, X_2, ..., X_n]$ can be defined recursively by $f \leq g$ if $f = 0$, and for $f, g \neq 0$ the relation $f \leq g$ holds iff

$$\begin{aligned} \mathrm{HM}(f) &< \mathrm{HM}(g), \text{ or} \\ \mathrm{HM}(f) &= \mathrm{HM}(g) \text{ and } \mathrm{red}(f) \leq \mathrm{red}(g). \end{aligned}$$

LEMMA 85. *Let R be an integral domain and let $f, g \in R[X_1, X_2, ..., X_n]$ with f, g non-zero. Then*

1) $\mathrm{HT}(fg) = \mathrm{HT}(f) \cdot \mathrm{HT}(g)$,

2) $\mathrm{HM}(fg) = \mathrm{HM}(f) \cdot \mathrm{HM}(g)$,

3) $\mathrm{HC}(fg) = \mathrm{HC}(f) \cdot \mathrm{HC}(g)$, *and*

4) $\mathrm{HT}(f + g) \leq \max\{\mathrm{HT}(f), \mathrm{HT}(g)\}$.

PROOF. (i) By definition $T(fg) = \{t \cdot s \mid t \in T(f), s \in T(g)\}$, because term orders are admissible, if $t < \mathrm{HT}(f)$ or $s < \mathrm{HT}(g)$, then $t \cdot s < \mathrm{HT}(f) \cdot \mathrm{HT}(g)$.

(ii) Because the only product of monomials of f and g that has $\mathrm{HT}(f) \cdot \mathrm{HT}(g)$ as term is $\mathrm{HM}(f) \cdot \mathrm{HM}(g)$, the claim follows.

(iii) Is immediate form (i) and (ii).

(iv) It follows form the fact $T(f + g) \subseteq T(f) \cup T(g)$. □

REMARK 86. We now define the notion of reduction of a polynomial. As said before, we now restrict to polynomials over a field; the reason why is simple, we need the inverse of the head coefficient of every polynomial on the ring.

DEFINITION 87. Let f, g, p be polynomials in $K[X_1, X_2, ..., X_n]$ with $f, p \neq 0$, and let P be a subset of $K[X_1, X_2, ..., X_n]$ .Then we say

1) f **reduces to** g **modulo** p **by eliminating** t (notation $f \underset{p}{\to} g[t]$), if $t \in T(f)$, there exists $s \in T$ with $s \cdot \mathrm{HT}(p) = t$, and

$$g = f - \frac{\mathrm{C}(t, f)}{\mathrm{HC}(p)} \cdot s \cdot p,$$

2) f **reduces to** g **modulo** p (notation $f \underset{p}{\to} g$), if $f \underset{p}{\to} g[t]$ for some $t \in T(f)$,

3) f **reduces to** g **modulo** P (notation $f \underset{P}{\to} g$), if $f \underset{p}{\to} g$ for some $p \in P$,

4) f is **reducible modulo** p if there exists $g \in K[X_1, X_2, ..., X_n]$ such that $f \underset{p}{\to} g$, and

5) f is **reducible modulo** P if there exists $g \in K[X_1, X_2, ..., X_n]$ such that $f \underset{P}{\to} g$.

If f is not reducible modulo p (modulo P), then we say f is **in normal form modulo** p (**modulo** P). A **normal form** of f **modulo** P is a polynomial g that is in normal form modulo P and satisfies

$$f \underset{P}{\overset{*}{\to}} g,$$

where $\underset{P}{\overset{*}{\to}}$ is the reflexive-transitive closure of $\underset{P}{\to}$ (see Definition 13). We call

$$f \underset{p}{\to} g\ [t],$$

a **top-reduction** of f if $t = \mathrm{HT}(f)$; whenever a top-reduction of f exists (with $p \in P$), we say that f is **top-reducible modulo** p (**modulo** P).

As expected, reduction of polynomials can be computed.

LEMMA 88. *If $\leq$ is a decidable term order and $K[X_1, X_2, ..., X_n]$ is a polynomial ring over a computable field, then $\underset{P}{\to}$ is decidable for every finite $P \subseteq K[X_1, X_2, ..., X_n]$.*

PROOF. Using the unique representation of a polynomial f shown in Proposition 71, we can clearly decide whether or not f is reducible modulo P (note that P is finite and claim (ii) of the proposition asserts there is an algorithm to find that representation). In addition, if we can reduce f modulo P, then the computability of K and $K[X_1, X_2, ..., X_n]$ allows us to compute $f - \frac{\mathrm{C}(t,f)}{\mathrm{HC}(p)} \cdot s \cdot p$, i.e., to compute $f \underset{P}{\to} g$. □

Some simple properties about reductions on $K[X_1, X_2, ..., X_n]$ are compiled in the following lemma.

LEMMA 89. *Let f, g, p be polynomials in $K[X_1, X_2, ..., X_n]$ and P a subset of $K[X_1, X_2, ..., X_n]$. The the following hold:*

1) f is reducible modulo p iff there exists $t \in T(f)$ such that $\mathrm{HT}(p) \mid t$.

2) If $f \underset{p}{\to} f - mp$ for some monomial m, then $\mathrm{HT}(mp) \in T(f)$.

3) Suppose $f \underset{p}{\to} g\ [t]$. Then $t \notin T(g)$, while for all $t' \in T$ with $t' > t$, we have $t' \in T(f)$ iff $t' \in T(g)$. In fact, $m \in M(f)$ iff $m \in M(g)$ for every monomial $m > t$.

4) If $f \underset{p}{\to} g$, then $g < f$.

5) If $f \underset{P}{\overset{*}{\to}} g$, then $g \leq f$, and $g = 0$ or $\mathrm{HT}(g) \leq \mathrm{HT}(f)$.

PROOF. (i) and (ii) are immediate from the definitions.
[start=3]

1) By Proposition 71 (i), we can write $f = \sum_{i=1}^{k} m_i$ with $m_1 > m_2 > ... > m_k$. Because f reduces to g modulo p by eliminating t, there exists $q \in T$

such that $q \cdot \mathrm{HT}(p) = t$, and so

$$m_j = \frac{\mathrm{C}(t,f)}{\mathrm{HC}(p)} \cdot q \cdot \mathrm{HM}(p)$$

for some $1 \leq j \leq k$. If we now write $\frac{\mathrm{C}(t,f)}{\mathrm{HC}(p)} \cdot q \cdot p = \sum_{i=1}^{s} r_i$ with $m_j = r_1 > r_2 > ... > r_s$, then

$$g = f - \frac{\mathrm{C}(t,f)}{\mathrm{HC}(p)} \cdot q \cdot p = \sum_{i=1}^{k} m_i - m_j - \sum_{i=2}^{s} r_i,$$

and the claim follows since $m_i > r_d$ for all $1 \leq d \leq s$ if $i < j$.

2) From (iii) above, we see that $T(g) < T(f)$ in the well-order of $\mathcal{P}_{fin}(T)$ induced by $\leq$, and so $g < f$.

3) The first statement follows easily from (iv) by induction on the length of the reduction chain $f \xrightarrow[P]{*} g$. The second one is now obvious form the definition of the induced quasi-order.

□

REMARK 90. Inequality $g \leq f$ of (v) is not strict. Because when doing several reductions to a polynomial f we still consider the terms in f, and not only the terms of the reduced polynomials, we may recover an eliminated term, which may provide the equality. With some care this can be avoided in practice and the inequality may be considered strict.

In Section 2.2 we saw the importance of choosing a noetherian reduction relation. Therefore, wee may check noetherian condition out of the list given the following result.

THEOREM 91. *The relation $\xrightarrow[P]{}$ is a noetherian reduction relation on $K[X_1, X_2, ..., X_n]$ for every $P \subseteq K[X_1, X_2, ..., X_n]$.*

PROOF. We have already seen that $\leq$ is a well-founded relation on $K[X_1, X_2, ..., X_n]$ (see Theorem 79) and that if $f, g \in K[X_1, X_2, ..., X_n]$ with $f \xrightarrow[P]{} g$, then $g < f$ (see (iv) of Lemma above). Now we apply Lemma 50 to finish the proof. □

Now Lemma 49 applied to the relation $\xrightarrow[P]{}$ produces the desired result.

COROLLARY 92. *Every polynomial $f \in K[X_1, X_2, ..., X_n]$ has at least one normal form modulo P.*

Actually, given a polynomial f and a finite set of polynomials P, there is an algorithm, Algorithm 2, that on input of f, P produces a normal form of f modulo P as output. Note that this algorithm, generalizes the division of polynomials in one variable to the multivariate case, and from one divisor to a (finite) family.

PROPOSITION 93. *Let P be a subset of $K[X_1, X_2, ..., X_n]$ and $f \in K[X_1, X_2, ..., X_n]$. Then there is a normal form $g \in K[X_1, X_2, ..., X_n]$ of f modulo P and a family*

$\mathscr{F} = \{q_p\}_{p\in P}$ of elements of $K[X_1, X_2, ..., X_n]$ with

$$f = \left(\sum_{p\in P} q_p p\right) + g \text{ and } \max\{\mathrm{HT}(q_p p) \mid p \in P, q_p p \neq 0\} \leq \mathrm{HT}(f).$$

If P is finite, the ground field is computable, and the term order on T is decidable, then g and $\{q_p\}_{p\in P}$ can be computed form f and P.

PROOF. We give an algorithm, (Algorithm 2) for the computation of g and q_p.

Algorithm 2 REDPOL

Specification: $(\mathscr{F}, g) \leftarrow \mathrm{REDPOL}(f, P)$
Complete reduction of f modulo P.
Given: a finite subset P of $K[X_1, X_2, ..., X_n]$ and $f \in K[X_1, X_2, ..., X_n]$.
Find: a normal form g of f modulo P, and a family of polynomials $\mathscr{F} = \{q_p\}_{p\in P}$ with $f = f = \left(\sum_{p\in P} q_p p\right) + g$ and $\max\{\mathrm{HT}(q_p p) \mid p \in P, q_p p \neq 0\} \leq \mathrm{HT}(f)$.
begin
$q_p \leftarrow 0$ (**for all** $p \in P$)
$g \leftarrow f$
while g is reducible modulo P **do**
select $p \in P$ such that g is reducible modulo p,
determine a monomial m with $g \underset{p}{\rightarrow} g - mp$
$g \leftarrow g - mp$
$q_p \leftarrow q_p + m$
end
$\mathscr{F} \leftarrow \{q_p\}_{p\in P}$
return$(\mathscr{F}, g)$
end REDPOL

For general, possibly non-computable field, non-decidable term order and infinite subset P, the steps of the algorithm can be interpreted as mathematical constructions that prove the existence of the q_p.

Le us denote by g_i the value of g after the i-th run trough the **while**-loop, with $g_0 = f$.

Termination: An infinite run of the **while-**loop would rise to an infinite ascending chain $g_0 \underset{P}{\rightarrow} g_1 \underset{P}{\rightarrow} ...$, a contradiction with $\underset{P}{\rightarrow}$ being a noetherian relation.

Correctness: Suppose there are N runs through the **while**-loop. From $g_i \underset{P}{\rightarrow} g_{i+1}$ for all $0 \leq i < N$, we conclude that $f \overset{*}{\underset{P}{\rightarrow}} g$ is an invariant of the loop. It is easy to see that the equation

$$f = \left(\sum_{p\in P} q_p p\right) + g$$

is also a loop invariant. Finally, we claim that

$$\max\{\mathrm{HT}(q_p p) \mid p \in P, q_p p \neq 0\} \leq \mathrm{HT}(f),$$

is an invariant of the loop. It is trivial true upon initialization. Now suppose it is true after the ith run for $1 \leq i < N$, then $f \xrightarrow[P]{*} g_i$ and $\mathrm{HT}(g_i) \leq \mathrm{HT}(f)$. Let mp be the polynomial that is being subtracted form g during the next run. Then $\mathrm{HT}(mp) \in T(g)$ and so $\mathrm{HT}(mp) \leq \mathrm{HT}(g_i) \leq \mathrm{HT}(f)$; because $T(g_i - mp) \subseteq T(g_i) \cup T(mp)$, we have

$$\mathrm{HT}(g_i - mp) \leq \max\{\mathrm{HT}(g_i), \mathrm{HT}(mp)\} \leq \mathrm{HT}(f),$$

and the claim follows since $g_{i+1} = g_i - mp$. □

Remark 94. Algorithm above is often referred as the division algorithm in several variables. Following this terminology, the polynomial g is called residue and despite the univariate case, this residue is not necessarily unique as shown on the introduction.

Example 95. Consider the polynomial $f = 2x^2y + \frac{5}{2}xy + \frac{3}{2}y + 8x^2 + \frac{3}{2}x - \frac{9}{2}$ and let $F = \{f_1, f_2, f_3\}$ as in Remark 34. We see that $\mathrm{HT}(f_1) = x^2y$ divides $\mathrm{HT}(f)$, and so f is reducible modulo F. In particular we have the reduction $f \xrightarrow[F]{} h$ where $h = f_1 - \frac{2}{3}f_1 = \frac{7}{6}xy + \frac{5}{6}y + 2x^2 - \frac{11}{6}x - \frac{5}{2}$. Because $\mathrm{HT}(h)$ is not divisible by $\mathrm{HT}(f_i)$ for any $1 \leq i \leq 3$, the algorithm terminates with $f = \left(\frac{2}{3}f_1\right) + h$.

CHAPTER 3

Gröbner Basis

The Chapter is divided into 5 sections and is committed to proof Gröbner basis existence and its construction via Buchberger's Algorithm. Section 3.1 introduces the last and necessary results for the proof of Gröbner bases existence, which is achieved in Section 3.2. In Section 3.4 Buchberger algorithm for constructing such bases is given, and then improved in Section 3.5.

3.1. Congruence relation

In this section, necessary and sufficient conditions for $f \xrightarrow[P]{*} 0$ are studied. The name of the section is referred to the membership problem, which is now connected with reduction relation and constitutes the main result of the section together with the more technical result called Translation Lemma (Lemma 97).

LEMMA 96. *Let $P \subseteq K[X_1, X_2, ..., X_n]$ and $f, g, h \in K[X_1, X_2, ..., X_n]$, and let $m \in M$.*

1) If $f \in P$, then $hf \xrightarrow[P]{*} 0$.

2) If $f \xrightarrow[P]{} g$, then $mf \xrightarrow[P]{} mg$.

3) If $f \xrightarrow[P]{*} g$, then $mf \xrightarrow[P]{*} mg$. In particular, $f \xrightarrow[P]{*} 0$ implies $mf \xrightarrow[P]{*} 0$.

PROOF.

1) Assume for a contradiction that the set
$$H = \left\{ h \in K[X_1, X_2, ..., X_n] \mid \text{not } hf \xrightarrow[P]{*} 0 \right\}$$
is non-empty. Then H contains a $\leq$-minimal element $h \neq 0$. With $m = \mathrm{HM}(h)$, we obtain $\mathrm{HM}(hf) = m \cdot \mathrm{HM}(f)$, and so
$$hf \xrightarrow[f]{} hf - mf \text{ and } hf - mf = \mathrm{red}(h) \cdot f.$$
We have $\mathrm{red}(h) \notin H$ since $\mathrm{red}(h) < h$, and so $\mathrm{red}(h) \cdot f \xrightarrow[P]{*} 0$; thus $hf \xrightarrow[P]{*} 0$, a contradiction.

2) Suppose $f \xrightarrow[p]{} g$, say $g = f - m'p$ for some $p \in P$, then $\mathrm{HT}(m'mp) \in T(f)$ and so $\mathrm{HT}(m'mp) \in T(fm)$. Finally we see that
$$mf \xrightarrow[p]{} mf - m'mp \text{ and } mf - mm'p = mg.$$

3) This follows from (ii) by induction on the length k of the reduction chain $f \xrightarrow[P]{k} g$.

□

LEMMA 97 (Translation Lemma). *Let* $f, g, h, h_1 \in K[X_1, X_2, ..., X_n]$, *and let* $P \subseteq K[X_1, X_2, ..., X_n]$.

1) *If* $f - g = h$ *and* $h \underset{P}{\overset{*}{\to}} h_1$ *then there exists* $f_1, g_1 \in K[X_1, X_2, ..., X_n]$ *such that* $f_1 - g_1 = h_1$, $f \underset{P}{\overset{*}{\to}} f_1$, *and* $g \underset{P}{\overset{*}{\to}} g_1$.

2) *If* $f - g \underset{P}{\overset{*}{\to}} 0$, *then* $f \downarrow g$, *and so in particular* $f \underset{P}{\overset{*}{\leftrightarrow}} g$.

PROOF. Note that (ii) is the special case of (i) where $h = 0$. We now proof (i) by induction on k, where $f - g = h$, and $h \underset{P}{\overset{k}{\to}} h_1$. For $k = 0$, $f_1 = f$ and $g_1 = g$ satisfy the claim. For $k + 1$, $f - g = h$ and $h \underset{P}{\overset{k+1}{\to}} h_1$; we split the reduction as

$$h \underset{P}{\overset{k}{\to}} h_2 \underset{P}{\to} h_1,$$

for some polynomial h_2. By induction hypothesis, there exist f_2, h_2 such that

$$f_2 - g_2 = h_2, \quad f \underset{P}{\overset{*}{\to}} h_2 \quad \text{and} \quad g \underset{P}{\overset{*}{\to}} g_2.$$

We now proof there exist polynomials f_1, g_1 such that

$$f \underset{P}{\overset{*}{\to}} f_1, \quad g_2 \underset{P}{\overset{*}{\to}} g_1 \quad \text{and} \quad f_1 - g_1 = h_1,$$

and so, by transitivity of $\underset{P}{\overset{*}{\to}}$, the result follows. Because $h_2 \underset{P}{\to} h_1$ there exist $p \in P$, $u \in T$ such that

$$h_1 = h_2 - \frac{\mathrm{C}(t, h_2)}{\mathrm{HC}(p)} \cdot u \cdot p.$$

If the above reduction eliminates the term $t \in T(h_2)$, because $f_2 - g_2 = h_2$, we have $t \in T(f_2) \cup T(g_2)$. Now set

$$f_1 = f_2 - \frac{\mathrm{C}(t, f_2)}{\mathrm{HT}(p)} \cdot u \cdot p \quad \text{and} \quad g_1 = g_2 - \frac{\mathrm{C}(t, g_2)}{\mathrm{HT}(p)} \cdot u \cdot p,$$

where $C(t, f_2) = 0$ if $t \notin T(f_2)$ and $C(t, g_2) = 0$ is $t \notin T(g_2)$. In both cases we have $f_2 \underset{P}{\to} f_1$ and $g_2 \underset{P}{\to} g_1$. In addition, if $h_2 = f_2 - g_2$ the relation among coefficients $\mathrm{C}(t, h_2) = \mathrm{C}(t, f_2) - \mathrm{C}(t, g_2)$ holds. Finally,

$$f_1 - g_1 = (f_2 - g_2) - \frac{\mathrm{C}(t, f_2) - \mathrm{C}(t, g_2)}{\mathrm{HC}(p)} \cdot u \cdot p = h_2 - \frac{\mathrm{C}(t, h_2)}{\mathrm{HC}(p)} \cdot u \cdot p = h_1,$$

as required. □

LEMMA 98. *Let* $P \subseteq K[X_1, X_2, ..., X_n]$, *and let* $f, g \in K[X_1, X_2, ..., X_n]$. *Then* $f \equiv_{\mathrm{Id}(P)} g$ *iff* $f \underset{P}{\overset{*}{\leftrightarrow}} g$. *In particular,* $f \underset{P}{\overset{*}{\leftrightarrow}} g$ *implies* $f - g \in \mathrm{Id}(P)$, *and* $f \underset{P}{\overset{*}{\to}} 0$ *implies* $f \in \mathrm{Id}(P)$.

PROOF. " $\Longleftarrow$ ": We show by induction on $k \in \mathbb{N}$ that $f \underset{P}{\overset{k}{\leftrightarrow}} g$ implies $g - f \in \mathrm{Id}(P)$. If $k = 0$, then $f = g$, and so $g - f = 0 \in \mathrm{Id}(P)$.

Suppose the claim is true for every two polynomials related by $\overset{k}{\underset{P}{\leftrightarrow}}$, and consider $f \overset{k+1}{\underset{P}{\leftrightarrow}} g$. Say

$$f \overset{k}{\underset{P}{\leftrightarrow}} h \underset{P}{\leftrightarrow} g,$$

then $h - f \in \mathrm{Id}(P)$ by the induction hypothesis, and $g - h = mp$ for some $m \in M$, $p \in P$ by the definition of $\underset{P}{\rightarrow}$. Consequently, $g - f = (g - h) + (h - f) \in \mathrm{Id}(P)$.

"$\Longrightarrow$": Let $g - f \in \mathrm{Id}(P)$. Then there exists $p_i \in P$ and $h_i \in K[X_1, X_2, ..., X_n]$ with $1 \leq i \leq k$ such that

$$g = f + \sum_{i=1}^{k} h_i p_i.$$

We show by induction on k that $f \overset{*}{\underset{P}{\leftrightarrow}} g$. If $k = 0$, then $f = g$. If

$$g = f + \sum_{i=1}^{k} h_i p_i + k_{k+1} p_{k+1},$$

we apply induction hypothesis to $g' = f + \sum_{i=1}^{k} h_i p_i$ and so $g' \overset{*}{\underset{P}{\leftrightarrow}} f$. Because $g = g' + h_{k+1} p_{k+1}$, we have $g \overset{*}{\underset{P}{\leftrightarrow}} f + h_{k+1} p_{k+1}$ and it suffices to show that

$$(f + h_{k+1} p_{k+1}) \overset{*}{\underset{P}{\leftrightarrow}} f.$$

If we set $F = f + h_{k+1} p_{k+1}$ and $G = f$, then $F - G = h_{k+1} p_{k+1}$ which reduces to zero modulo P by Lemma 96 (i). Now, case (ii) of Translation Lemma (Lemma 97) applied to $F - G$ finishes the proof. □

Corollary 99. *Let $P \subseteq K[X_1, X_2, ..., X_n]$. Then the reduction relation $\underset{P}{\rightarrow}$ on $K[X_1, X_2, ..., X_n]$ is adequate for $\equiv_{\mathrm{Id}(P)}$.*

Definition 100. Let $P \subseteq K[X_1, X_2, ..., X_n]$. Then P is called **monic** if every $p \in P$ is monic. P is called **reduced** (or **autoreduced**) if every $p \in P$ is monic and in normal form modulo $P \setminus \{p\}$.

Proposition 101. *Let P be a finite subset of $K[X_1, X_2, ..., X_n]$. Suppose the ground field is computable and the term order on T is decidable. Then the algorithm REDUCTION (Algorithm 3) computes a finite reduced subset Q of $K[X_1, X_2, ..., X_n]$ such that $\mathrm{Id}(Q) = \mathrm{Id}(P)$.*

Proof.

Algorithm 3 REDUCTION

Specification: $Q \leftarrow \text{REDUCTION}(P)$
Construction of a finite reduced set Q such that $\text{Id}(Q) = \text{Id}(P)$
Given: a finite subset P of $K[X_1, X_2, ..., X_n]$
Find: a finite reduced set in $K[X_1, X_2, ..., X_n]$ with $\text{Id}(Q) = \text{Id}(P)$
begin
$Q \leftarrow P$
while there is $p \in Q$ which is reducible modulo $Q \setminus \{p\}$ **do**
select $p \in Q$ which is reducible modulo $Q \setminus \{p\}$
$Q \leftarrow Q \setminus \{p\}$
$h \leftarrow$some normal form of p modulo Q
if $h \neq 0$ **then** $Q \leftarrow Q \cup \{h\}$ **end**
end
$Q \leftarrow \left\{\text{HC}(q)^{-1} \cdot q \mid q \in Q\right\}$
end REDUCTION

It is easy to see that $\text{Id}(Q) = \text{Id}(P)$ is an invariant of the **while**-loop. *Correctness* is obvious from the **while**-clause. To prove *Termination,* let $P = \{p_1, p_2, ..., p_m\}$ be the input set. We may regard P as an ordered m-tuple $(p_1, p_2, ..., p_m)$ rather than a set. After a run on the loop, the algorithm replaces an element $p_j \in P$ with some normal form h of p_j (no matter if $h = 0$). Let Q_i denote the m-tuple obtained after the ith run through the loop. If the algorithm does not terminate, it produces an infinite sequence of m-tuples $\{Q_i\}_{i \in \mathbb{N}}$ where Q_i is never the zero-tuple for any $i \in \mathbb{N}$, since otherwise the loop terminates. Moreover, since an entry that becomes zero after k runs of the loop never becomes nonzero, there must be an entry that is replaced infinitely many times with nonzero elements. Because we replace an element p with some normal form h modulo Q of p, we have $h < p$ and the sequence of normals forms modulo Q form a strictly descending chain w.r.t. the induced well-founded quasi-order on $K[X_1, X_2, ..., X_n]$, a contradiction. □

EXAMPLE 102. Consider the set $P = \{p_1, p_2\}$ in $K[x, y]$ with the inverse lexicographical order given by

$$\begin{aligned} p_1 &= y - \frac{14}{3}x^3 + \frac{38}{3}x^2 + \frac{61}{6}x - 3, \\ p_2 &= x^3 - \frac{5}{2}x^2 - \frac{5}{2}x. \end{aligned}$$

By initialization, $Q = P$, and the while-clause is satisfied since $\text{HT}(p_2) = x^3 \in T(p_1)$, that is, we can reduce $p_2 \in Q$ modulo $Q \setminus \{p_2\} = p_1$ by eliminating the term x^3. Computation of $p_1 \underset{p_2}{\to} p_1 - \left(\frac{-14}{3}\right) p_2 = p_1'$ leads to the new polynomial $p_1' = y + x^2 - \frac{3}{2}x - 3$, which is in normal form modulo Q, once removed p_1, and so the if-condition is also satisfied. Thus, we have $Q = \{p_1', p_2\}$ and the while-clause is no longer satisfied; because both p_1' and p_2 are monic, the last actualization of Q does not modify it, and so $Q = \{p_1', p_2\}$ is a reduced set with $\text{Id}(Q) = \text{Id}(P)$.

REMARK 103. Algorithm 3 when applied to $P = \{f, g\}$ with $f, g \in K[X]$ produces as result $Q = \{\gcd(f, g)\}$, just like the Euclidean algorithm does.

3.2. Gröbner basis existence

Given an finitely generated ideal I, we want a finite set P such that $\mathrm{Id}(P) = I$ and $f \xrightarrow[P]{*} 0$ iff $f \in I$. The direct implication is clear and the converse constitutes the object of this section.

If h is a normal form of f modulo P, then $f \xrightarrow[P]{*} h$ and $f = \sum_{i=1}^{k} s_i p_i + h$ for some monomials $s_i \in M$ and polynomials $p_i \in P$. In case $\underset{P}{\rightarrow}$ is locally confluent, as application of Newman's Lemma $\underset{P}{\rightarrow}$ has a unique normal form and the Church-Rosser property. Then if $f \in I$, then $h = f - \sum_{i=1}^{k} s_i p_i \in I$, and $h \equiv_I 0$, that is, $f \xleftrightarrow[P]{*} 0$; by the Church-Rosser property, $h \rightarrow r \leftarrow 0$ for some r, and so $h = 0$, that is, $f \xrightarrow[P]{*} 0$. Conversely, if $f \xrightarrow[P]{*} 0$, since $\underset{P}{\rightarrow}$ has a unique normal form, $h = 0$ and $f \in I$.

In general $\underset{P}{\rightarrow}$ is not locally confluent but fortunately, we prove that we can always find a finite set G such that $\mathrm{Id}(G) = \mathrm{Id}(P)$ and $\underset{G}{\rightarrow}$ locally confluent, i.e., every ideal finitely generated has a Gröbner-basis.

Definition 104. If $P \subseteq K[X_1, X_2, ..., X_n]$, then we set $\mathrm{HT}(P) = \{\mathrm{HT}(p) \mid 0 \neq p \in P\}$; for $S \subseteq T$,

$$\mathrm{mult}(S) = \{t \in T \mid \text{there is } s \in S \text{ with } s \mid t\}$$

denotes **the set of all multiples of elements of** S.

Theorem 105 (Theorem-Definition). *A subset G of $K[X_1, X_2, ..., X_n]$ is called a **Gröbner basis** (w.r.t. the term order $\leq$) if it is finite, $0 \notin G$, and G satisfies one of the following equivalent conditions:*

1) $\underset{G}{\rightarrow}$ *is locally confluent,*
2) $\underset{G}{\rightarrow}$ *is confluent,*
3) $\underset{G}{\rightarrow}$ *has unique normal form,*
4) $\underset{G}{\rightarrow}$ *has the Church-Rosser property,*
5) $f \xrightarrow[G]{*} 0$ *for all* $f \in \mathrm{Id}(G)$,
6) *every* $0 \neq f \in \mathrm{Id}(G)$ *is reducible modulo* G,
7) *every* $0 \neq f \in \mathrm{Id}(G)$ *is top-reducible modulo* G,
8) *for every* $t \in \mathrm{HT}(\mathrm{Id}(G))$ *there exists* $s \in \mathrm{HT}(G)$ *with* $s \mid t$,
9) $\mathrm{HT}(\mathrm{Id}(G)) \subseteq mult(\mathrm{HT}(G))$,
10) *the polynomials* $h \in K[X_1, X_2, ..., X_n]$ *that are in normal form w.r.t.* $\underset{G}{\rightarrow}$ *form a system of unique representatives for the partition*

$$\{f + \mathrm{Id}(G) \mid f \in K[X_1, X_2, ..., X_n]\}$$

of $K[X_1, X_2, ..., X_n]$.

PROOF. We now proof that (i)-(x) are equivalent. We have already seen equivalence (i)-(iv) or an arbitrary noetherian reduction relation (see Newman's Lemma, Theorem 52).

(iv)⇒(v): Let $f \in \mathrm{Id}(G)$. Then $f - 0 \in \mathrm{Id}(G)$ and thus $f \overset{*}{\underset{G}{\leftrightarrow}} 0$ by Lemma 98. Since $\underset{G}{\rightarrow}$ has the Church-Rosser property, there exists $h \in K[X_1, X_2, ..., X_n]$ with $f \overset{*}{\underset{G}{\rightarrow}} h$ and $0 \overset{*}{\underset{G}{\rightarrow}} h$. Since 0 is always in normal form, $h = 0$.

(v)⇒(vii): Let $0 \neq f \in \mathrm{Id}(G)$. By (v), there exists $h \in K[X_1, X_2, ..., X_n]$ with $f \underset{G}{\rightarrow} h \overset{*}{\underset{G}{\rightarrow}} 0$.

(vi)⇒(vii): Assume for contradiction that $0 \neq f \in \mathrm{Id}(G)$ is minimal (w.r.t. the induced quasi-order on $K[X_1, X_2, ..., X_n]$) such that it is not top-reducible w.r.t. $\underset{G}{\rightarrow}$. Then by (vi), there exists $h \in K[X_1, X_2, ..., X_n]$ with $f \underset{G}{\rightarrow} h$. It follows that $h \in \mathrm{Id}(G)$ and $h < f$. Moreover, $\mathrm{HM}(h) = \mathrm{HM}(f)$ since f was not top-reducible. By the minimal choice of f, h is top-reducible w.r.t. $\underset{G}{\rightarrow}$, say $h \underset{g}{\rightarrow} h_1$ for some $g \in G$. Then, $\mathrm{HT}(g) \mid \mathrm{HT}(h)$, and so f is top-reducible w.r.t. $\underset{g}{\rightarrow}$, a contradiction.

(vii), (viii) and (ix) are simple reformulations of each other.

(ix)⇒(x): Assume for contradiction that there exist $f_1, f_2 \in K[X_1, X_2, ..., X_n]$ both in normal form w.r.t. $\underset{G}{\rightarrow}$ with $f_1 \neq f_2$ and

$$f_1 + \mathrm{Id}(G) = f_2 + \mathrm{Id}(G).$$

Then, $f_1 - f_2 \in \mathrm{Id}(G)$ and so there exist $g \in G$ with $\mathrm{HT}(g) \mid \mathrm{HT}(f_1 - f_2)$, but

$$\mathrm{HT}(f_1 - f_2) \in T(f_1) \cup T(f_2),$$

hence f_1 or f_2 is reducible modulo G, a contradiction.

(x)⇒(iv): Let $f_1, f_2 \in K[X_1, X_2, ..., X_n]$ with $f_1 \overset{*}{\underset{G}{\leftrightarrow}} f_2$. Then $f_1 - f_2 \in \mathrm{Id}(G)$ by Lemma 98, and so

$$f_1 + \mathrm{Id}(G) = f_2 + \mathrm{Id}(G).$$

Let h_1 and h_2 be normal forms of f_1 and f_2, respectively. Then $h_1, h_2 \in f_1 + \mathrm{Id}(G)$ again by Lemma 98, and so $h_1 = h_2$ by (x). □

REMARK 106. Among all previous equivalent conditions, (iii) and (v) are conceptually the most clarifying. It is also worth noting that the definition of Gröbner-basis, which is usually referred as a set G generating an ideal, is also a property (or properties) of the reduction relation $\underset{G}{\rightarrow}$ upon which the definition is based, and so G being a Gröbner basis is also dependent on the induced quasi-order on $K[X_1, X_2, ..., X_n]$, and term order on T.

DEFINITION 107. If I is an ideal of $K[X_1, X_2, ..., X_n]$, then a **Gröbner basis of** I (w.r.t. $\leq$) is a Gröbner basis G (w.r.t. $\leq$) such that $\mathrm{Id}(G) = I$.

Next result, although simple, constitutes a characterization of Gröbner basis G, being the unique subset of an ideal I, generating the whole ideal I with the property $f \overset{*}{\underset{G}{\rightarrow}} 0$ for all $f \in I$ (together with other equivalent properties).

PROPOSITION 108. *Let I be an ideal of $K[X_1, X_2, ..., X_n]$ and G a finite subset of I with $0 \notin G$. Then each of the following is equivalent to G being a Gröbner basis of I.*

1) $f \xrightarrow[G]{*} 0$ *for all* $f \in I$,

2) every $0 \neq f \in I$ *is reducible modulo* G,

3) every $0 \neq f \in I$ *is top-reducible modulo* G,

4) for every $s \in \mathrm{HT}(I)$ *there exists* $t \in \mathrm{HT}(G)$ *with* $t \mid s$,

5) $\mathrm{HT}(I) \subseteq mult(\mathrm{HT}(G))$,

6) the polynomials $h \in K[X_1, X_2, ..., X_n]$ *that are in normal form w.r.t.* $\xrightarrow[G]{}$ *form a system of representatives for the partition*

$$\{f + I \mid f \in K[X_1, X_2, ..., X_n]\}$$

of $K[X_1, X_2, ..., X_n]$.

Proof. We prove (i) implies G is a Gröbner basis of I and then, we prove that (i)-(vi) are equivalent.

If (i) holds, $f \xrightarrow[G]{*} 0$ for all $f \in I$, and because $\mathrm{Id}(G) \subseteq I$, G is a Gröbner basis. Now we apply Lemma 96 and $f \xrightarrow[G]{*} 0$ implies $f \in \mathrm{Id}(G)$, that is, $I = \mathrm{Id}(G)$.

Equivalence of (i)-(vi) is consequence of (v)-(x) of the Gröbner basis Theorem-Definition (Theorem 105). □

We can now give a proof of the Gröbner bases existence.

Theorem 109. *Let* I *be an ideal of* $K[X_1, X_2, ..., X_n]$. *Then there exists a Gröbner basis* G *of* I *w.r.t.* $\leq$.

Proof. By Theorem 64, the divisibility relation is a Dickson partial order on T. So the set $\mathrm{HT}(I)$ has a finite basis S w.r.t. divisibility relation. For each $t \in S$, there exists $f_t \in I$ such that $\mathrm{HT}(f_t) = t$. Let now $G = \{f_t \mid t \in S\}$. Then G satisfies condition (iv) of the previous proposition, and so G is Gröbner basis of I. □

Although the previous result is positive, it presents two difficulties in order to compute the relation $\equiv_I$ for an ideal I of $K[X_1, X_2, ..., X_n]$. The first one is that we don't have a way to construct a Gröbner basis, the second one, Gröbner basis are not uniquely determined by the ideal and so we may consider different basis for an ideal. Fortunately, both problems can be solved; first problem will be dealt in the next chapter, and the second one can be easily solved with the concept of ***reduced Gröbner basis*** (see Definition 100).

In the following we give a proof of the existence and uniqueness of reduced Gröbner bases. However, in the next section we provide a new formulation of Gröbner basis that is useful for both comprehension of the concept and for simplification of the reduced Gröbner basis proof.

Lemma 110. *Suppose* I *is an ideal of* $K[X_1, X_2, ..., X_n]$, m *is a monomial, and* f, g *are minimal polynomials in* I *such that* $\mathrm{HM}(f) = \mathrm{HM}(g) = m$. *Then* $f = g$.

Proof. We must have $T(f) = T(g)$ since otherwise $f < g$ or $g < f$. Note that $f - g \in I$, and $f - g = 0$ or $s = \mathrm{HT}(f - g) < m$. In the latter case

$s \in T(f) = T(g)$, we can reduce f modulo $f - g$ so that $f \underset{f-g}{\to} h$ and $h < f$ contradicting the minimality of f. □

THEOREM 111. *Let I be an ideal of $K[X_1, X_2, ..., X_n]$. Then there exists a unique reduced Gröbner basis G of I w.r.t. $\leq$.*

PROOF. As in Theorem 109 let S be the unique minimal basis of $\mathrm{HT}(I)$. For each $t \in S$, there exits $f_t \in T$ with , and because I is an ideal,w.o.l.g. we may consider $\mathrm{HM}(f_t) = t$. Indeed, by the above lemma we may consider f_t is the unique minimal polynomial with $\mathrm{HM}(f_t) = t$. We now set

$$G = \{f_t \mid t \in S\},$$

and claim that G is the unique reduced Gröbner basis of I. By definition, G is monic and if G is not reduced, there exist $g_1 \neq g_2 \in G$ and $f \in K[X_1, X_2, ..., X_n]$ with $g_1 \underset{g_2}{\to} f$. We may assume that the reduction is a top reduction since otherwise $\mathrm{HM}(f) = \mathrm{HM}(g_1)$ with $f < g$, again the minimality of $g_1 \in G$. Therefore, $\mathrm{HT}(g_2) \mid \mathrm{HT}(g_1)$ and so $S' = S \setminus \{\mathrm{HT}(g_1)\}$ is also a basis of $\mathrm{HT}(I)$ with $S' \subseteq S$, a contradiction with the minimality of S.

We now proof uniqueness. Assume for a contradiction that H is another reduced Gröbner basis of I, and let g be an element of the symmetric set difference $G \triangle H$ (see Chapter 1) such that $\mathrm{HT}(g)$ is minimal in $\mathrm{HT}(G \triangle H)$. W.l.o.g. let $g \in G \setminus H$; given that H is a Gröbner basis, there exists $h \in H$ so that $\mathrm{HT}(h) \mid \mathrm{HT}(g)$ and by the minimality of g, $\mathrm{HT}(g) = \mathrm{HT}(h)$. Consider now $f = g - h$ then we clearly see that $f \in I$, $f < g$ and $\mathrm{HT}(f) \in T(g) \cup T(h)$. If $\mathrm{HT}(f) \in T(g)$, because $f \in I$, there exist polynomial $p \in T(g)$ so that $\mathrm{HT}(p) \mid \mathrm{HT}(f) \in T(g)$ contradicting the fact that G was reduced. In case $\mathrm{HT}(f) \in T(g)$ we reason analogously to reach the contradiction. □

3.3. Reduced Gröbner bases

We now discuss some definitions relating Gröbner basis which are frequently used. We show the equivalence between this new definitions and those given early and use them as to simplify the proof of reduced Gröbner basis existence. In particular, what is been here exposed can be found in [4].

DEFINITION 112 (Alternative Definition). For a fixed term ordering in $K[X_1, X_2, ..., X_n]$, a finite subset $G = \{g_1, g_2, ..., g_t\}$ of an ideal I is said to be a **Gröbner basis** if

$$\mathrm{Id}(\mathrm{HT}(G)) = \mathrm{Id}(\mathrm{HT}(I)).$$

REMARK 113. Using (iv) of Gröbner basis Theorem-Definition (Theorem 105) we can easily see the equivalence between both definitions.

DEFINITION 114. A **minimal Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

1) $\mathrm{HC}(g) = 1$ for all $g \in G$, and

2) for all $g \in G$, $\mathrm{HT}(g) \notin \mathrm{Id}(\mathrm{HT}(G'))$ where $G' = G \setminus \{g\}$.

THEOREM 115. *Let G be a Gröbner basis for the ideal I, and let $g \in G$ be a polynomial such that $\mathrm{HT}(g) \in \mathrm{Id}(G')$. Then $G \setminus \{g\}$ is also a Gröbner basis.*

PROOF. If $\mathrm{HT}(g) \in \mathrm{Id}(\mathrm{HT}(G \setminus \{g\}))$, then $\mathrm{Id}(\mathrm{HT}(G \setminus \{g\})) = \mathrm{Id}(\mathrm{HT}(G)) = \mathrm{Id}(\mathrm{HT}(I))$ since G is a Gröbner basis and the claim follows. □

REMARK 116. Clearly converting a Gröbner basis G to a monic set doesn't change the fact that G is a Gröbner basis. Now, theorem above shows that reducing G to G' by eliminating those polynomials $g \in G$ with $\mathrm{HT}(g) \in \mathrm{Id}(G')$ does implies that G' is also a Gröbner basis. Then, since Gröbner bases exist for any ideal I, so do minimal Gröbner bases.

DEFINITION 117. A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis I such that:

1) $\mathrm{HC}(g) = 1$ for all $g \in G$, and

2) for all $g \in G$, no monomial of g lies in $\mathrm{Id}(\mathrm{HT}(G'))$ where $G' = G \setminus \{g\}$.

REMARK 118. Definition above and our first definition are equivalent. Condition (i) stands that G is monic and we claim condition (ii) is equivalent to g is not reducible modulo G'. If g is reducible modulo G', there exists $g_2 \in G'$ so that $\mathrm{HT}(g_2) \mid t$ for some $t \in T(g)$, and if m is the monomial in g so that $t \in T(m)$, then $m \in \mathrm{Id}(\mathrm{HT}(G'))$. Conversely, if some monomial m of g lies in $\mathrm{Id}(\mathrm{HT}(G'))$, in particular $m = a\prod_{i=1}^{k} \mathrm{HT}(g_i)$ for some $a \in K$, $g_i \in G$, and so $\mathrm{HT}(g_i) \mid t$ where $t \in T(m)$, that is, g is reducible modulo G'.

PROPOSITION 119. *Let $\{0\} \neq I \subseteq K[X_1, X_2, ..., X_n]$. Then, for a given monomial ordering, I has unique reduced Gröbner basis.*

PROOF. Let G be a minimal Gröbner basis for I. Our goal is to modify G until all its elements are reduced.

A first observation is that if g is reduced for G, then g is also reduced for any other minimal Gröbner basis of I that contains g and has the same set of leading terms. This follows because the definition only involves the leading terms.

Given $g \in G$, take g' a normal form of g modulo $G' = G \setminus \{g\}$ and set $G^* = (G \setminus \{g\}) \cup \{g'\}$. Then we have $\mathrm{HT}(g') = \mathrm{HT}(g)$ since $\mathrm{HT}(g)$ is not divisible by any element of $\mathrm{HT}(G')$ and so when dividing g by G', $\mathrm{HT}(g)$ goes to the remainder. This shows that $\mathrm{Id}(\mathrm{HT}(G^*)) = \mathrm{Id}(\mathrm{HT}(G))$ and because $G^* \subseteq I$ we conclude that G^* is a minimal Gröbner basis of I and g' is reduced for G^* by construction.

Now take the elements of G and apply the above process until they are all reduced. The Gröbner basis may change each time we do the process, but our earlier observation shows that once element is reduced, it stays reduced since we never change the leading terms. Thus, we end up with a reduced Gröbner basis.

In remains to prove uniqueness. Suppose G and $\widetilde{G}$ are reduced Gröbner bases for I. Then in particular, G and $\widetilde{G}$ are minimal Gröbner bases. We now prove that $\mathrm{HT}(G) = \mathrm{HT}\left(\widetilde{G}\right)$. Take $t_1 \in \mathrm{HT}(G)$, because $t_1 \in \mathrm{Id}(\mathrm{HT}(G)) = \mathrm{Id}\left(\mathrm{HT}\left(\widetilde{G}\right)\right)$ there exist some $\widetilde{t} \in \mathrm{HT}\left(\widetilde{G}\right)$ so that $\widetilde{t} \mid t_1$. Repeating the argument for $\widetilde{t}$, there exists $t_2 \in \mathrm{HT}(G)$ so that $t_2 \mid \widetilde{t}$. If the relation $t_2 \mid \widetilde{t} \mid t_1$ holds for $t_1 \neq t_2$, then there exist $g_1 \in G$ with $\mathrm{HT}(g_1) = t_1$ so that $t_1 \in \mathrm{Id}(\mathrm{HT}(G \setminus \{g_1\}))$ since $t_2 \mid t_1$ and $t_2 \in \mathrm{HT}(G \setminus \{g\})$, a contradiction. Hence $t_1 = t_2 = \widetilde{t}$ and the claim is proved. (Notice that this also implies that G and $\widetilde{G}$ have the cardinal).

Given $g \in G$, take $\widetilde{g} \in \widetilde{G}$ such that $\mathrm{HT}(g) = \mathrm{HT}(\widetilde{g})$. Because $g - \widetilde{g} \in I$, we have $g - \widetilde{g} \xrightarrow[G]{*} 0$, and $\mathrm{HT}(g) = \mathrm{HT}(\widetilde{g})$, this term cancels in $g - \widetilde{g}$, and the remaining terms are divisible by none of the $\mathrm{HT}(G) = \mathrm{HT}\left(\widetilde{G}\right)$ since G, $\widetilde{G}$ are reduced Gröbner basis. Hence $g - \widetilde{g}$ is in normal for modulo G, by uniqueness of normal forms $g - \widetilde{g} = 0$ and $G = \widetilde{G}$. □

REMARK 120. Form what has been argued on the proof we see that application of Algorithm 3 to a Gröbner basis produces a reduced Gröbner basis.

3.4. Buchberger's Algorithm

For the construction of Gröbner basis, a special class of polynomials, called S-polynomials are introduced. This polynomials play a decisive roll in Buchberger's algorithm. Before that, a sufficient condition for G being a Gröbner basis is given.

LEMMA 121. *Let G be a finite subset of $K[X_1, X_2, ..., X_n]$ with $0 \notin G$. Assume that whenever $g_1, g_2 \in G$ with $g_1 \neq g_2$ and monomials m_1, m_2 such that*

$$\mathrm{HM}(m_1 g_1) = \mathrm{HM}(m_2 g_2),$$

it follows that $m_1 g_1 - m_2 g_2 \xrightarrow[G]{*} 0$. Then G is a Gröbner basis.

PROOF. We show that $\underset{G}{\to}$ is locally confluent. Let $f, f_1, f_2 \in K[X_1, X_2, ..., X_n]$ with $f \underset{G}{\to} f_i$ where $f_i = f - m_i g_i$ for some $m_i \in M$, $g_i \in G$ for $i = 1, 2$. It suffices to show that $f_1 - f_2 = m_1 g_1 - m_2 g_2 \xrightarrow[G]{*} 0$ so by application of Translation Lemma (Lemma 97), claim (ii), $f_1 \downarrow_G f_2$.

If $\mathrm{HT}(m_1 g_1) = \mathrm{HT}(m_2 g_2) = t$, because f reduces to $f_i = f - m_i g_i$, the equality $\mathrm{HM}(m_1 g_1) = \mathrm{HM}(m_2 g_2)$ holds, and by hypothesis $m_1 g_1 - m_2 g_2 \xrightarrow[G]{*} 0$ if $g_1 \neq g_2$. In case $g_1 = g_2$, then $f_1 - f_2 = (m_1 - m_2) g_1 \underset{G}{\to} 0$ by statement (i) Lemma 96. Now consider the case $\mathrm{HT}(m_1 g_1) \neq \mathrm{HT}(m_2 g_2)$, say $\mathrm{HT}(m_1 g_1) > \mathrm{HT}(m_2 g_2)$. Then we can perform the top reductions $m_1 g_1 - m_2 g_2 \underset{g_1}{\to} -m_2 g_2$ by means of $g_1 \in G$ and then $-m_2 g_2 \underset{g_2}{\to} 0$ by means of $g_2 \in G$. Hence $m_1 g_1 - m_2 g_2 \xrightarrow[G]{*} 0$ and the claim follows. □

DEFINITION 122. For $i = 1, 2$, let $0 \neq g_i \in K[X_1, X_2, ..., X_n]$, and $s_i \in T$ such that $s_i \cdot \mathrm{HT}(g_i) = \mathrm{lcm}(\mathrm{HT}(g_2), \mathrm{HT}(g_2))$. Then the **S-polynomial** of g_1 and g_2 is defined as

$$\mathrm{spol}(g_1, g_2) = \mathrm{HC}(g_2)\, s_1 g_1 - \mathrm{HC}(g_1)\, s_2 g_2.$$

EXAMPLE 123. [2] Given $f_1 := 3x^2y + 2xy + y + 9x^2 + 5x - 3$ and $f_2 := 2x^3y - x - y + 6x^3 - 2x^2 - 3x + 3$ we have

$$\begin{aligned} \mathrm{spol}(f_1, f_2) &= 3 \cdot x \cdot f_1 - 2 \cdot 1 \cdot f_2, \\ &= 2x^2y + \frac{5}{2}xy + \frac{3}{2}y + 8x^2 + \frac{3}{2}x - \frac{9}{2}. \end{aligned}$$

The concept of S-polynomials besides its practical utility for constructing a Gröbner basis, also provide a new characterization for such basis. The following result will be needed when construction Buchberger's algorithm.

THEOREM 124 (Characterization of Gröbner bases by S-polynomials). *Let G be a finite subset of $K[X_1, X_2, ..., X_n]$ with $0 \notin G$. Then the following are equivalent:*

1) *G is a Gröbner basis,*

2) *whenever $g_1, g_2 \in G$ and $h \in K[X_1, X_2, ..., X_n]$ is a normal form of $spol(g_1, g_2)$ modulo G, then $h = 0$,*

3) *$spol(g_1, g_2) \xrightarrow[G]{*} 0$ for all $g_1, g_2 \in G$.*

PROOF. (i)⇒(ii): $\operatorname{spol}(g_1, g_2)$ is obviously in $\operatorname{Id}(G)$ for all $g_1, g_2 \in G$. So by Gröbner basis Theorem-Definition (Theorem 105), $\operatorname{spol}(g_1, g_2)$ reduces to 0 modulo G, and uniqueness of normal forms implies $h = 0$.

(ii)⇒(iii): It is trivial.

(iii)⇒(i): We show that whenever $g_1, g_2 \in G$ with $g_1 \neq g_2$ and m_1 and m_2 are monomials such that

$$\operatorname{HM}(m_1 g_1) = \operatorname{HM}(m_2 g_2), \tag{3.4.1}$$

it follows that $m_1 g_1 - m_2 g_2 \xrightarrow[G]{*} 0$ and then apply Lemma 121. For $i = 1, 2$, let $t_i = \operatorname{HT}(g_i)$, $a_i = \operatorname{HC}(g_i)$ and $m_i = b_i u_i$ with $b_i \in K$ and $u_i \in T$. Then Equation (3.4.1) becomes

$$b_1 a_1 u_1 t_1 = b_2 a_2 u_2 t_2. \tag{3.4.2}$$

Now let $s_1, s_2 \in T$ such that $s_i t_i = \operatorname{lcm}(t_1, t_2)$ for $i = 1, 2$. From Equation (3.4.2) we see that $u_1 t_1 = u_2 t_2$ is a common multiple of t_1 and t_2. Hence there exists $v \in T$ such that for $i = 1, 2$,

$$u_i t_i = v \cdot \operatorname{lcm}(t_1, t_2) = v s_i t_i.$$

We see that $u_i = v s_i$. Furthermore, Equation (3.4.2) implies that $(b_1/a_2) = (b_2/a_1)$, and we obtain

$$\begin{aligned} m_1 g_1 - m_2 g_2 &= b_1 u_1 g_1 - b_2 u_2 g_2 \\ &= b_1 v s_1 g_1 - b_2 v s_2 g_2 \\ &= \frac{b_1}{a_2} \cdot v \cdot (a_2 s_1 g_1 - a_1 s_2 g_2) \\ &= \frac{b_1}{a_2} \cdot v \cdot \operatorname{spol}(g_1, g_2). \end{aligned}$$

Using Lemma 96 (i) and the fact that $\operatorname{spol}(g_1, g_2) \xrightarrow[G]{*} 0$, we conclude that

$$\frac{b_1}{a_2} \cdot v \cdot \operatorname{spol}(g_1, g_2) \xrightarrow[G]{*} 0.$$

□

COROLLARY 125. *Let G be a finite subset of $K[X_1, X_2, ..., X_n]$. Suppose the ground field is computable, and the term order on T is decidable. Then the algorithm 4 decides whether G is a Gröbner basis or not.*

Algorithm 4 GRÖBNERTEST

Specification: $v \leftarrow$GRÖBNERTEST(G)
Test whether G is a Gröbner basis
Given: $G =$ a finite subset of $K[X_1, X_2, ..., X_n]$
Find: $v \in \{\textbf{true}, \textbf{false}\}$ such that $v = \textbf{true}$ iff G is a Gröbner basis
begin
$B \leftarrow \{(g_1, g_2) \mid g_1, g_2 \in G \textbf{ with } g_1 \neq g_2\}$
while $B \neq \emptyset$ **do**
select $\{g_1, g_1\}$ form B
$h \leftarrow$ some normal form of spol (g_1, g_2) modulo G
if $h = 0$ **then**
$B \leftarrow B \setminus \{\{g_1, g_2\}\}$
else
return(false)
end
end
return(true)
end GRÖBNERTEST

EXAMPLE 126. Let $F = \{f_1, f_2, f_3\}$ as in Remark 34. We now form Example 123 that spol $(f_1, f_2) = 2x^2y + \frac{5}{2}xy + \frac{3}{2}y + 8x^2 + \frac{3}{2}x - \frac{9}{2}$, and form Example 95, a normal form for spol (f_1, f_2) is $h = \frac{7}{6}xy + \frac{5}{6}y + 2x^2 - \frac{11}{6}x - \frac{5}{2}$. Because $h \neq 0$, the algorithm return **false**, that is, F is not a Gröbner basis w.r.t. the inverse lexicographical order.

The main result of this section, and also of the chapter, is now given.

THEOREM 127 (Buchberger's Algorithm). *Let F be a finite subset of $K[X_1, X_2, ..., X_n]$. Suppose the ground field is computable, and the term order on T is decidable. Then Algorithm 5 computes G in $K[X_1, X_2, ..., X_n]$ such that $F \subseteq G$ and* Id $(G) =$ Id (F).

Algorithm 5 BUCHBERGER

PROOF. **Specification:** $G \leftarrow$BUCHBERGER(F)
Construction of a Gröbner basis G of $\mathrm{Id}(F)$
Given: $F =$ a finite subset of $K[X_1, X_2, ..., X_n]$
Find: $G =$ a finite subset of $K[X_1, X_2, ..., X_n]$ such that G is a Gröbner basis in $K[X_1, X_2, ..., X_n]$with $F \subseteq G$ and $\mathrm{Id}(G) = \mathrm{Id}(F)$.
begin
$G \leftarrow F$
$B \leftarrow \{\{g_1, g_2\} \mid g_1, g_2 \in G$ **with** $g_1 \neq g_2\}$
while $B \neq \emptyset$ **do**
select $\{g_1, g_2\}$ from B
$B \leftarrow B \setminus \{\{g_1, g_2\}\}$
$h \leftarrow \mathrm{spol}(g_1, g_2)$
$h_0 \leftarrow$ some normal form of h modulo G
if $h_0 \neq 0$ **then**
$B \leftarrow B \cup \{\{g, h_0\} \mid g \in G\}$
$G \leftarrow G \cup \{h_0\}$
end
end
end BUCHBERGER

Termination: Assume for contradiction that the **while**-loop does not terminate. Let $F = G_0 \subset G_1 \subset G_2 \subset ...$ be the successive value of G. Considering those runs through the **while**-loop that actually enlarge G, we see that there exists an ascending sequence $\{n_i\}_{i \in \mathbb{N}}$ of natural numbers such that for all $1 \leq i \in \mathbb{N}$, there exists $h_i \in G_{n_i} \setminus G_{n_{i-1}}$ which is in normal form modulo $G_{n_{i-1}}$. Let $t_k = \mathrm{HT}(h_k)$ for all $k \in \mathbb{N}$; then $i < j$ implies that t_i does not divide t_j, since otherwise h_j would be top-reducible modulo $\{h_i\}$ and hence modulo $\{G_{n_{j-1}}\}$. Since divisibility of terms is a Dickson partial order, this contradicts Proposition 37 (ii).

Correctness: It is clear that $F \subseteq G \subseteq \mathrm{Id}(F)$ with G a finite subset of $K[X_1, X_2, ..., X_n]$ is a loop invariant. We show that

$$\mathrm{spol}(g_1, g_2) \xrightarrow[G]{*} 0,$$

for all $g_1, g_2 \in G$ and so by Theorem 124 G is Gröbner basis.

Take $g_1, g_2 \in G$ with $g_1 \neq g_2$, that is, $(g_1, g_2) \in B$ and say that the pair has been considered at the ith run of the **while**-loop. Because $\mathrm{spol}(g_1, g_2) \xrightarrow[G_i]{*} h_0$, if $h_0 = 0$ we are done, otherwise, $h_0 \neq 0$ and $G_{i+1} = G_i \cup \{h_0\}$. Since $G_i \subseteq G$ for all i, $\mathrm{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ as required. □

Note that this algorithm is non-deterministic; the resulting Gröbner basis is not uniquely determined by the input F since different pairs may be choose form the set B. We will refer to this pairs as **critical pairs**.

It is also clear that the algorithm is potentially rather complex. In the next section, we will see how the growth of the set B can be controlled by elimination unnecessary pairs.

EXAMPLE 128. [2] We now perform the Buchberger's algorithm to the set $F = \{f_1, f_2, f_3\}$ defined in Remark 34. Recall that if instead of adding h_0 to G in

Buchberger's algorithm, we add h_0 multiplied by a scalar, we still have a Gröbner basis G as output. Hence we can add h_0 once normalized, that is, after multiplying by the inverse of the head coefficient as to make h_0 monic.

We know from the previous example that $\operatorname{spol}(f_1, f_2) = 2x^2y + \frac{5}{2}xy + \frac{3}{2}y + 8x^2 + \frac{3}{2}x - \frac{9}{2}$. Now, a $\underset{G}{\to}$-normal form h_0 of $\operatorname{spol}(f_1, f_2)$ is $\frac{7}{6}xy + \frac{5}{6}y + 2x^2 - \frac{11}{6}x - \frac{5}{2}$ by Example 95; instead of adding the previous normal form to the set G, we normalize it by multiplying by $\frac{6}{7}$ and so we add $f_4 = xy + \frac{5}{7}y + \frac{12}{7}x^2 - \frac{11}{7}x - \frac{15}{7}$ to G. Now, a (normalized) normal form of $\operatorname{spol}(f_1, f_4)$ is $f_5 = y - \frac{14}{3}x^3 + \frac{38}{3}x^2 + \frac{61}{6}x - 3$, which we add to G.

If we now calculate the S-polynomial of f_4 and f_5 (both polynomials in G), and then some normal form, which we normalize, we reach the polynomial $f_6 = x^4 - 2x^3 - \frac{15}{4}x^2 - \frac{5}{4}x$, and again, we add it to G.

Finally, we reach the last new polynomial $f_7 = x^3 - \frac{5}{2}x^2 - \frac{5}{2}x$ after normalizing the normal form of $\operatorname{spol}(f_1, f_3)$.

Now, the S-polynomial of any two pairs f_i, f_j in G has 0 as normal form, and so no polynomial is added to $G = \{f_1, f_2, ..., f_7\}$ during any future execution of the while-loop. Hence the, Buchberger's algorithm produces G as output, and so, G is a Gröbner basis for $\operatorname{Id}(F)$.

In the following we give an algorithm to compute a reduced Gröbner basis given a Gröbner basis. As commented in Remark 120, application of Algorithm 3 (REDUCTION) to the output of Algorithm 5 (BUCHBERGER) may produce the desired reduced Gröbner basis. However this procedure may be more costly than the necessary and the following procedure may be taken in account.

PROPOSITION 129. *Let G be a Gröbner basis in $K[X_1, X_2, ..., X_n]$. Suppose K is computable and the term order on T is decidable. Then the following algorithm computes the reduced Gröbner basis of* $\operatorname{Id}(G)$.

PROOF.

Algorithm 6 REDGRÖBNER

Specification: $H \leftarrow$GRÖBNER(G)
Construction of a Gröbner basis of $\operatorname{Id}(G)$
Given: G a Gröbner basis in $K[X_1, X_2, ..., X_n]$
Find: H the reduced Gröbner basis of $\operatorname{Id}(G)$
begin
$H \leftarrow \emptyset$;$F \leftarrow G$
while $F \neq \emptyset$ **do**
select h from F
$F \leftarrow F \setminus \{h\}$
if $\operatorname{HT}(f) \nmid \operatorname{HT}(h)$ for all $f \in F \cup H$ **then**
$H \leftarrow H \cup \{h\}$
end
end
$H \leftarrow$**REDUCTION**(H)
end REDGRÖBNER

Termination of the algorithm is clear. Now we proof *Correctness.* We see that the if condition looks for a polynomial in $f \in F \cup H$ so that $\mathrm{HT}(f_0)$ is multiple of $\mathrm{HT}(f)$ and in case such polynomial does not exist, it adds f_0 to H. Hence $\mathrm{mult}(\mathrm{HT}(F \cup H))$ is a loop-invariant. Since upon initialization $F = G$ and $H = \emptyset$, $\mathrm{mult}(\mathrm{HT}(F \cup H)) = \mathrm{mult}(G)$ and since at the end of the loop $F = \emptyset$, $\mathrm{mult}(\mathrm{HT}(H)) = \mathrm{mult}(G)$ given that $\mathrm{mult}(\mathrm{HT}(F \cup H))$ is a loop-invariant. By Proposition 108 (v), H is a Gröbner basis of $\mathrm{Id}(G)$.

To see that H is reduced at the end of the loop, notice that $\mathrm{HT}(f) \nmid \mathrm{HT}(h)$ for all $h \in H$ and for all $f \in F \cup (H \setminus \{h\})$ is a loop-invariant (provided that $\mathrm{mult}(\mathrm{HT}(F \cup H))$ is a loop-invariant). At the end, $F = \emptyset$ and the loop-invariant implies $\mathrm{HT}(h_1) \nmid \mathrm{HT}(h_2)$ for all $h_1, h_2 \in H$, i.e., $\mathrm{HT}(H)$ is a reduced set. Now, execution of Algorithm Congruence relation (REDUCTION) does not change the set $\mathrm{mult}(\mathrm{HT}(H))$ since the reductions carried out by the algorithm are not top reductions, otherwise $\mathrm{HT}(H)$ would not be reduced. Hence, after application of Algorithm 3 (REDUCTION), H is a reduced Gröbner basis of $\mathrm{Id}(G)$. □

EXAMPLE 130. Consider the Gröbner basis $G = \{f_1, f_2, ..., f_7\}$ provided by Example 128, that is,

$$\begin{aligned}
f_1 &= 3x^2y + 2xy + y + 9x^2 + 5x - 3,\\
f_2 &= 2x^3y - x - y + 6x^3 - 2x^2 - 3x + 3,\\
f_3 &= x^3y + x^2y + 3x^3 + 2x^2,\\
f_4 &= xy + \frac{5}{7}y + \frac{12}{7}x^2 - \frac{11}{7}x - \frac{15}{7},\\
f_5 &= y - \frac{14}{3}x^3 + \frac{38}{3}x^2 + \frac{61}{6}x - 3,\\
f_6 &= x^4 - 2x^3 - \frac{15}{4}x^2 - \frac{5}{4}x,\\
f_7 &= x^3 - \frac{5}{2}x^2 - \frac{5}{2}x.
\end{aligned}$$

We see that $\mathrm{HT}(f_5)$ divides the head term of f_1, f_2, f_3 and f_4 and no term in $\mathrm{HT}(G)$ divides $\mathrm{HT}(f_5)$, thus $f_5 \in H$ while $f_1, f_2, f_3, f_4 \notin H$. Now, $\mathrm{HT}(f_7)$ divides $\mathrm{HT}(f_6)$ and so $f_6 \notin H$ while $f_7 \in H$ since no term in $\mathrm{HT}(G)$ divides $\mathrm{HT}(f_7)$. As shown in Example 102, application of REDUCTION to $H = \{f_5, f_7\}$ leads to the reduced Gröbner basis $\left\{y + x^2 - \frac{3}{2}x - 3,\ x^3 - \frac{5}{2}x^2 - \frac{5}{2}x\right\}$ for $\mathrm{Id}(F)$ where $F = \{f_1, f_2, f_3\}$ w.r.t. the inverse lexicographical order.

3.5. Improved Buchberger's Algorithm

For the improvement of Buchberger's Algorithm, two results known as Buchberger's criterion's, and first given by Buchberger itself in [3], are needed. This results together with its applications to the Buchberger's Algorithm constitute the object of this section.

DEFINITION 131. Let $0 \neq f \in K[X_1, X_2, ..., X_n]$, P a finite subset of $K[X_1, X_2, ..., X_n]$. A representation

$$f = \sum_{i=1}^{k} m_i p_i,$$

with monomials $0 \neq m_i \in K[X_1, X_2, ..., X_n]$ and $p_i \in P$ not necessarily pairwise different $(1 \leq i \leq k)$ is called a **standard representation** of f w.r.t. P (and $\leq$) if

$$\max\{\mathrm{HT}(m_i p_i) \mid 1 \leq i \leq k\} \leq \mathrm{HT}(f).$$

In case that

$$\max\{\mathrm{HT}(m_i p_i) \mid 1 \leq i \leq k\} \leq t,$$

for some $t \in T$, we also say that f has a t**-representation** w.r.t. to P.

The following result is immediate from the definition and Proposition 93.

THEOREM 132. *A finite subset G of $K[X_1, X_2, ..., X_n]$ with $0 \notin G$ is a Gröbner basis w.r.t. the term order $\leq$ iff $0 \neq f \in \mathrm{Id}(G)$ has a standard representation w.r.t. G and $\leq$.*

With the previous definition, we have a new sufficient condition for a a Gröbner basis.

THEOREM 133. *Let G be a finite subset of $K[X_1, X_2, ..., X_n]$ with $0 \neq G$. Assume that for all $g_1, g_2 \in G$, spol(g_1, g_2) either equals zero or it has a t-representation w.r.t. G for some $t < lcm(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$. Then G is a Gröbner basis.*

PROOF. We show that any polynomial $0 \neq f \in \mathrm{Id}(G)$ has a standard representation w.r.t. G and $\leq$. Because $f \in \mathrm{Id}(G)$ we can write

$$f = \sum_{g \in G} p_i g,$$

with $p_i \in K[X_1, X_2, ..., X_n]$ by Proposition 93. Reordering the above summands, we have

$$f = \sum_{i=1}^{k} m_i g_i,$$

where the m_i are monomials and the g_i are not necessarily distinct. In this case, we denote $s = \max\{\mathrm{HT}(m_i g_i) \mid 1 \leq i \leq k\}$, and say s is the head term of the representation. Because the above representation is not unique the term s depends on the representation and we may consider we picked one so the head term s is minimal among all possible head terms of all representations. Clearly, $\mathrm{HT}(f) \leq s$ and we claim that $\mathrm{HT}(f) = s$.

Assume for contradiction that $\mathrm{HT}(f) < s$, we proof there exists a representation of f with head term of the representation s' with $s' < s$. In order to do so, we use induction on the number n_s of summands in $\sum_{i=1}^{k} m_i g_i$ with $s = \mathrm{HT}(m_i g_i)$. Because $s \notin T(f)$, then s cancels out of the sum and so $n_s > 1$.

Suppose $n_s = 2$, say $\mathrm{HT}(m_1 g_1) = \mathrm{HT}(m_2 g_2) = s$. Now we argue as in Theorem 124 (iii)⇒(i), in order to show that $m_1 g_1 + m_2 g_2$ is multiple of spol(g_1, g_2). Because $\mathrm{HT}(m_i g_i) = s$, we have $m_i = a_i t_i$ with $a_i \in K$ and $t_i \in T$ for $i = 1, 2$. Moreover, $s = t_i \mathrm{HT}(g_i)$ and $s = u \cdot \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$ for some term $u \in T$. Now write

$$\mathrm{spol}(g_1, g_2) = \mathrm{HC}(g_2) \cdot u_1 \cdot g_1 - \mathrm{HC}(g_1) \cdot u_2 \cdot g_2,$$

with $u_i \in T$ and $u_i \mathrm{HT}(g_i) = \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$. Hence $t_i = u \cdot u_i$, and because $s \nmid m_1 g_1 + m_2 g_2$, $a_1 \mathrm{HC}(g_1) + a_2 \mathrm{HC}(g_2) = 0$ and so $\frac{a_1}{\mathrm{HC}(g_2)} = -\frac{a_2}{\mathrm{HC}(g_1)}$. Now,

$$\begin{aligned} m_1 g_1 + m_2 g_2 &= a_1 t_1 g_1 + a_2 t_2 g_2, \\ &= a_1 u u_1 g_1 + a_2 u u_2 g_2, \\ &= \frac{a_1}{\mathrm{HC}(g_2)} \mathrm{HC}(g_2)\, u u_1 g_1 + \frac{a_2}{\mathrm{HC}(g_1)} \mathrm{HC}(g_1)\, u u_2 g_2, \\ &= \underbrace{\left[\frac{a_1}{\mathrm{HC}(g_2)} \cdot u\right]}_{=:a \cdot u} \cdot \left[\mathrm{HC}(g_2)\, u_1 g_1 - \mathrm{HC}(g_1)\, u_2 g_2\right], \qquad (3.5.1) \\ &= a \cdot u \cdot \mathrm{spol}(g_1, g_2). \end{aligned}$$

By hypothesis, $\mathrm{spol}(g_1, g_2) = 0$ or it has a t-representation for some $t < \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$. In case $\mathrm{spol}(g_1, g_2) = 0$, then $m g_1 + m_2 g_2 = 0$ and $\sum_{i=3}^{k} m_i g_i$ is a representation for f with head term less than s. Otherwise $\mathrm{spol}(g_1, g_2) \neq 0$ and has a t-representation, say $\mathrm{spol}(g_1, g_2) = \sum_{i=1}^{k'} m_i' g_i'$ where $g_i \in G$ for all i. Joining this to Equation 3.5.1 produces

$$f = \sum_{i=3}^{k} m_i g_i + au \sum_{i=1}^{k'} m_i' g_i',$$

which is again a contradiction since the head term of the first summand is less than s, and for the right hand, $ut < u \cdot \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2)) = s$. Therefore the above is a s'-representation with $s' < s$ and the claim is proved for $n_s = 2$. Now suppose $n_s > 2$ and w.l.o.g. assume $\mathrm{HT}(m_i g_i) = s$ for $i = 1, 2$. Then,

$$\begin{aligned} f &= \sum_{i=1}^{k} m_i g_i, \\ &= \underbrace{m_1 g_1 - \frac{\mathrm{HC}(m_1 g_1)}{\mathrm{HC}(m_2 g_2)} m_2 g_2}_{h_1} + \underbrace{\left(\frac{\mathrm{HC}(m_1 g_1)}{\mathrm{HC}(m_2 g_2)} + 1\right) m_2 g_2}_{h_2} + \underbrace{\sum_{i=3}^{k} m_i g_i}_{h_3}, \end{aligned}$$

where the term s does not appear in h_1, and does appear in h_3 $n_s - 2$ times and at most once in h_2, that is, $n_s - 1$ in total. By induction hypothesis, $h_1 + h_2 + h_3$ has a s'-representation with $s' < s$ and so does f, a contradiction. □

Definition 134. We call $s, t \in T$ **disjoint** if s and t have no variable in common, i.e., $\gcd(s, t) = 1$, which implies $\mathrm{lcm}(s, t) = st$.

Lemma 135 (Buchberger's First Criterion). *Let $f, g \in K[X_1, X_2, ..., X_n]$ with disjoint head terms. Then spol$(f, g) \underset{\{f,g\}}{\overset{*}{\to}} 0$.*

Proof. Assume that

$$f = \sum_{i=1}^{k} a_i s_i \text{ and } g = \sum_{j=1}^{l} b_j t_j,$$

are the representations of f, g as sum of monomials $a_i s_i$ and $b_j t_j$ with $s_i, t_j \in T$ so that $s_1 > s_2 > ... > s_k$ and $t_1 > t_2 > ... > t_l$. Since $\gcd(s_1, t_1) = 1$, we must have

$\operatorname{lcm}(s_1, t_1) = s_1 t_1$ and thus

$$\operatorname{spol}(f,g) = b_1 t_1 f - a_1 s_1 g = b_1 t_1 \sum_{i=2}^{k} a_i s_i - a_1 s_1 \sum_{j=2}^{l} b_j t_j.$$

We claim that the two sums have no terms in common. If $t_1 s_i = s_1 t_j$ for some $2 \leq i \leq k$ and $2 \leq j \leq l$, then $s_i t_1$ being a common multiple of s_1 and t_1, is divided by $\operatorname{lcm}(s_1 t_1) = s_1 t_1$. It follows that $s_1 t_1 \leq s_i t_1$ and thus $s_1 \leq s_i$, a contradiction.

Now we write $a_1 s_1 = f - \sum_{i=2}^{k} a_i s_i$, and substituting in $\operatorname{spol}(f,g)$, we have

$$\operatorname{spol}(f,g) \quad = \quad b_1 t_1 \sum_{i=2}^{k} a_i s_i + \sum_{j=2}^{l} b_j t_j f + \sum_{j=2}^{l} b_j t_j \sum_{i=2}^{k} a_i s_i.$$

We now claim that by reducing the above expression modulo g eliminating the term $t_j \mathrm{HT}(f)$ for $j = 2, ..., l$, we only eliminate the sum $\sum_{j=2}^{l} b_j t_j f$. To see this notice that $\mathrm{HT}(f)$ is neither present on the first sum nor in the third one since f, g have disjoint terms and $s_1 = \mathrm{HT}(f)$ is not it any of them. Hence

$$\begin{aligned} \operatorname{spol}(f,g) \quad &\xrightarrow[f]{*} \quad b_1 t_1 \sum_{i=2}^{k} a_i s_i + \sum_{j=2}^{l} b_j t_j \sum_{i=2}^{k} a_i s_i \\ &= \quad g \sum_{i=2}^{k} a_i s_i \\ &\xrightarrow[g]{*} \quad 0. \end{aligned}$$

□

REMARK 136. If $s, t, u \in T$. The following are equivalent:

1) $t \mid \operatorname{lcm}(s,u)$

2) $\operatorname{lcm}(s,t) \mid \operatorname{lcm}(s,u)$

3) $\operatorname{lcm}(t,u) \mid \operatorname{lcm}(s,u)$.

PROOF. (i)⇔(ii): By definition $s, t \cdot a$ divides $\operatorname{lcm}(s, t \cdot a)$, and so does s, t. Hence $\operatorname{lcm}(s,t) \mid \operatorname{lcm}(s, t \cdot a)$. Now by (i), $\operatorname{lcm}(s,u) = t \cdot a$ for some $a \in T$, and hence, $\operatorname{lcm}(s,t) \mid \operatorname{lcm}(s, \operatorname{lcm}(s,u)) = \operatorname{lcm}(s,u)$. Conversely, $t \mid \operatorname{lcm}(s,t) \mid \operatorname{lcm}(s,u)$ and (i) holds. □

PROPOSITION 137 (Buchberger's Second Criterion). *Let F be a finite subset of $K[X_1, X_2, ..., X_n]$ and $g_1, g_2, p \in K[X_1, X_2, ..., X_n]$ such that the following hold:*

1) $\mathrm{HT}(p) \mid lcm(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$, and

2) $spol(g_i, p)$ has a t_i-representation with respect to F with $t_i < lcm(\mathrm{HT}(g_i), \mathrm{HT}(p))$ for $i = 1, 2$.

Then the S-polynomial $spol(g_1, g_2)$ has a t-representation w.r.t. F for some $t < lcm(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$.

PROOF. By assumption (ii), $\operatorname{spol}(g_i, p)$ has a t_i-representation for $i = 1, 2$, say

$$\operatorname{spol}(g_1, p) = \sum_{i=1}^{k_1} m_{1i} f_{1i},$$

with $\max\{\operatorname{HT}(m_{1i} f_{1i}) \mid 1 \leq i \leq k_1\} < \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(p))$, and

$$\operatorname{spol}(p, g_2) = \sum_{i=1}^{k_2} m_{2i} f_{2i},$$

with $\max\{\operatorname{HT}(m_{2i} f_{2i}) \mid 1 \leq i \leq k_2\} < \operatorname{lcm}(\operatorname{HT}(p), \operatorname{HT}(g_2))$, where $m_{ij} \in M$ and $f_{ij} \in F$. Because $p \mid \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2))$, by the previous remark there exist $s_1, s_2 \in T$ with

$$\begin{aligned} s_1 \cdot \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(p)) &= \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2)), \\ s_2 \cdot \operatorname{lcm}(\operatorname{HT}(p), \operatorname{HT}(g_2)) &= \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2)). \end{aligned}$$

Let $a = \operatorname{HC}(g_1)$, $b = \operatorname{HC}(p)$, $c = \operatorname{HC}(g_2)$ and consider $u_1, v_1, u_2, v_2 \in T$ such that

$$\begin{aligned} \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(p)) &= u_1 \cdot \operatorname{HT}(g_1) = v_1 \cdot \operatorname{HT}(p), \\ \operatorname{lcm}(\operatorname{HT}(p), \operatorname{HT}(g_2)) &= u_2 \cdot \operatorname{HT}(p) = v_2 \operatorname{HT}(g_2). \end{aligned}$$

By the above, we can easily see that $s_1 v_1 = s_2 u_2$, and so

$$\begin{aligned} cs_1 \operatorname{spol}(g_1, p) + as_2 \cdot \operatorname{spol}(p, g_2) &= cs_1 (bu_1 g_1 - av_1 p) + as_2 (cu_2 p - bv_2 g_2) \\ &= cbs_1 u_1 g_1 - abs_2 v_2 g_2 \\ &= b \cdot \operatorname{spol}(g_1, g_2). \end{aligned}$$

Substituting $\operatorname{spol}(g_1, p)$ and $\operatorname{spol}(g_2, p)$ by its representations on the above equation, we get

$$\operatorname{spol}(g_1, g_2) = \frac{1}{b} \left(cs_1 \sum_{i=1}^{k_1} m_{1i} f_{1i} + as_2 \sum_{i=1}^{k_2} m_{2i} f_{2i} \right). \tag{3.5.2}$$

By the choice of these representations, we may conclude that

$$\begin{aligned} s_1 \cdot \operatorname{HT}(m_{1i} f_{1i}) &< s_1 \cdot \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(p)) \\ &= \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2)), \end{aligned}$$

for $1 \leq i \leq k_1$, and similarly,

$$\begin{aligned} s_2 \cdot \operatorname{HT}(m_{2i} f_{2i}) &< s_2 \cdot \operatorname{lcm}(\operatorname{HT}(p), \operatorname{HT}(g_2)) \\ &= \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2)), \end{aligned}$$

for $1 \leq i \leq k_2$. Now if we let t be a maximal of $s_1 \cdot \operatorname{HT}(m_{1j} f_{1j})$ for $1 \leq j \leq k_1$ and $s_2 \cdot \operatorname{HT}(m_{2j} f_{2j})$ for $1 \leq j \leq k_2$, then we see that Equation 3.5.2 is a t-representation of $\operatorname{spol}(g_1, g_2)$ and $t < \operatorname{lcm}(\operatorname{HT}(g_1), \operatorname{HT}(g_2))$. □

Proposition and lemma above can be used to improve Buchberger's Algorithm (Algorithm 5). Before to present the implementations, we shall discuss the idea behind of this results. We discuss the possible implementations described in paper [2], and give the Algorithm 7 of [1]. Certainly, the algorithm is due to Buchberger and was first published in [3].

For an speed up of the Buchberger's algorithm (Algorithm 5), three different strategies may apply.

1) The order of selection of pairs the pairs $\{g_1, g_2\}$ for which the S-polynomials are formed have a crucial influence on the complexity of the algorithm. As general rule, pairs whose least common multiple of their head terms are minimal w.r.t. $\leq$ should be treated first. This strategy is known as **normal strategy**.

2) Each time a new polynomial is adjoined to the basis, all the other polynomials may be reduced using also the new polynomial. Moreover, if this process is carried out in the course of the algorithm, the result is a reduced Gröbner basis.

3) Since the most expensive operations in the algorithm are the reduction of the normal form h modulo G in the **while**-loop, application of Buchberger's criterion's allows us to detect if a certain S-polynomial h can be reduced to zero without carrying out the reduction.

In the following algorithm, we implement strategies (i) and (iii). The reader is advised to consult [2], page 196, as it discusses the use of three different strategies

THEOREM 138. *Let F be a finite subset of $K[X_1, X_2, ..., X_n]$. Suppose the ground field is computable and the term order on T is decidable. Then Algorithm 7 computes a Gröbner basis G in $K[X_1, X_2, ..., X_n]$ such that* $\mathrm{Id}(G) = \mathrm{Id}(F)$.

PROOF.

Algorithm 7 GRÖBNERNEW1

Specification: $G \leftarrow$ **GRÖBNERNEW1** (F)
Construction of a Gröbner basis G for $\mathrm{Id}(F)$
Given: $F =$ a finite subset of $K[X_1, X_2, ..., X_n]$
Find: $G =$ a finite subset of $K[X_1, X_2, ..., X_n]$ such that G is a Gröbner basis in $K[X_1, X_2, ..., X_n]$ with $\mathrm{Id}(G) = \mathrm{Id}(F)$
begin
$G \leftarrow F$ % It is also possible to set $G \leftarrow$ **REDUCTION** (F)
$B \leftarrow \{\{g_1, g_2\} \mid g_1, g_2 \in G$ **with non-disjoint head terms,** $g_1 \neq g_2\}$
create a matrix M **with boolean entry** $M(g_1, g_2)$ **for each** $g_1, g_2 \in G$ **with** $g_1 \neq g_2$

for all $\{g_1, g_2\}$ with $g_1, g_2 \in G$ with $g_1 \neq g_2$ **do**
if $\{g_1, g_2\} \in B$ **then** $M(g_1, g_2) \leftarrow$**false**
else $M(g_1, g_2) \leftarrow$**true end**
end
while $B \neq \emptyset$ **do**
select $\{g_1, g_2\}$ form B with $\mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$
minimal among all pairs in B
$B \leftarrow B \setminus \{\{g_1, g_2\}\}$
$M(g_1, g_2) \leftarrow$**true**
if there does not exist $p \in G$ with:
$\mathrm{HT}(p) \mid \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$ and $M(g_1, p) = M(g_2, p) =$ **true**,
then
$h \leftarrow$ **spol** (g_1, g_2)
h_0 some normal form of h modulo G
if $h_0 \neq 0$ **then**
for all $g \in G$ **do**
enlarge M by an entry for $\{h_0, g\}$
if $\mathrm{HT}(g), \mathrm{HT}(h_0)$ are disjoint **then**
$M(g, h_0) \leftarrow$ **true**
else
$B \leftarrow B \cup \{\{g, h_0\}\}$
$M(g, h_0) \leftarrow$**false**
end if
end for
$G \leftarrow G \cup \{h_0\}$
end if
end if
end while
return (G)
end GRÖBNERNEW1

Termination: The algorithm terminates since an infinite loop would be an infinite loop of the Buchberger's Algorithm (Algorithm 5).

Correctness: We first note that

$$F \subseteq G \subseteq \mathrm{Id}(F),$$

with G finite is an invariant of the **while**-loop. Thus the output G_{out} is a finite basis of the ideal $\mathrm{Id}(F)$. To see that G is a Gröbner basis, we verify the hypothesis of Theorem 133. Assume for contradiction that there exists a pair $\{g_1, g_2\} \in G_{out}$ such that $\mathrm{spol}(g_1, g_2)$ does not have a t-representation w.r.t. G_{out} for any $t < \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$. If g_1 and g_2 have disjoint head terms, then $\mathrm{spol}(g_1, g_2)$ would reduce to 0 modulo G_{out} by Buchberger's First Criterion (Lemma 135) and thus even have $\mathrm{spol}(g_1, g_2)$ has a standard representation w.r.t. G_{out} by Proposition 93. We may assume that g_1, g_2 have non disjoint head terms, that is, $(g_1, g_2) \in B$ and w.l.o.g. that $\{g_1, g_2\}$ was selected from the critical pair list B in first place w.r.t. some other pair with non disjoint head terms selected during the execution of the **while**-loop.

Moreover, we know that $\mathrm{spol}(g_1, g_2)$ does not reduce to 0 modulo G_{out} since otherwise it would even have a standard representation w.r.t. G_{out}. Hence, the pair $\{g_1, g_2\}$ did not pass the **if**-condition following the assignment $M(g_1, g_2) \leftarrow$ **true**, that is, there exists $p \in G$ with

$$\mathrm{HT}(p) \mid \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2)), \text{ and } M(g_1, p) = M(p, g_2) = \textbf{true}$$

at that point of the computation. Because the entry $M(g_i, p) =$ **true**, we conclude that either g_i and p have disjoint terms, or the pair $\{g_i, p\} \in B$ was selected form B at an earlier stage for $i = 1, 2$. By our choice of the pair $\{g_1, g_2\}$, the latter could not have happened, and so, g_i, p have disjoint terms. Hence, by Buchberger's First Criterion (Lemma 135), $\mathrm{spol}(g_i, p)$ has a t_i-representation for some $t_i < \mathrm{lcm}(\mathrm{HT}(g_i), \mathrm{HT}(p))$ for $i = 1, 2$, and Buchberger's Second Criterion (Proposition 137) provides the desired contradiction. □

Remark 139. [1] The normal strategy for the selection of critical pairs from B has shown efficiency in practice. Moreover, correctness of the above algorithm may be partially regarded as a consequence of this strategy. To see this, assume that at some point during computation, the par $\{g_1, g_2\}$ is selected form B, and there is, at this time, $p \in G$ with

$$\mathrm{HT}(p) \mid \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2)).$$

Then Buchberger's second criterion tells us that we should treat the pairs (p, g_1) and (p, g_2) we do not have to test the pair (g_1, g_2). In case $\mathrm{lcm}(\mathrm{HT}(g_i), \mathrm{HT}(p))$ properly divides $\mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$, by the normal strategy we deduce that $\{g_i, p\}$ is not a critical pair in B, and so $M(g_i, p) \leftarrow$**true** by initialization for $i = 1, 2$. Hence, by removing the normal strategy, we miss the Buchberger's second criterion.

Example 140. Consider the set $F = \{f_1, f_2, f_3\}$ as in Remark 34. Then $B = \{\{f_1, f_2\}, \{f_2, f_3\}, \{f_1, f_3\}\}$ upon initialization and $M(f_i, f_j) =$ **false** for $i \neq j$. We have $\mathrm{HT}(f_1) = x^2y$, $\mathrm{HT}(f_2) = x^3y$ and $\mathrm{HT}(f_3) = x^3y$, thus $\mathrm{lcm}(\mathrm{HT}(f_i), \mathrm{HT}(f_j)) = x^3y$ for $i \neq j$ and we can select any pair in B. Select $\{f_1, f_2\}$ and set $B = \{\{f_2, f_3\}, \{f_1, f_3\}\}$, $M(f_1, f_2) =$ **true**. Now, if $p \in G$ is such that $p \mid \mathrm{lcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))$, because there is only one entry of the matrix M set as true, condition $M(f_1, p) = M(f_2, p) =$ **true** cannot be satisfied. Hence, we consider $h \leftarrow \mathrm{spol}(f_1, f_2)$ and then calculate some $\xrightarrow[G]{}$-normal form h_0 of h. From Example 128, we known that $h_0 = \frac{7}{6}xy + \frac{5}{6}y + 2x^2 - \frac{11}{6}x - \frac{5}{2} \neq 0$, and so $M(f_i, h_0) =$ **true** for $1 \leq i \leq 3$ and $G = \{f_1, f_2, f_3, h_0\}$. However, no pair $\{f_i, h_0\}$ is added to B.

Now, restarting the while-loop, we select the pair $\{f_2, f_3\}$ form B, and set $B = \{\{f_1, f_3\}$. For the if-condition we have $h_0 \in G$ and $\mathrm{HT}(h_0) = xy \mid \mathrm{lcm}(\mathrm{HT}(f_2), \mathrm{HT}(f_3))$. Moreover, $M(f_i, h_0) = \mathbf{true}$ and so if-condition is not satisfied. Restarting the while-loop, we select the pair $\{f_1, f_3\}$ and set $B = \emptyset$. Now, just like before, the if condition is not satisfied by letting $p = h_0 \in G$ and the algorithm terminates.

We see that only one polynomial, h_0, was added to F in order to form a Gröbner basis for $\mathrm{Id}(F)$ whereas as shown is Example 128, Buchberger's algorithm introduces four new polynomials to F constructing a Gröbner basis for $\mathrm{Id}(F)$ with seven different polynomials. Clearly, Algorithm 7 constitutes an improvement of Buchberger's algorithm (Algorithm 5).

EXAMPLE 141. We now give an example of Algorithm 1. Let $G = F \cup \{h_0\}$ be the Gröbner basis of the example above. Then $\underset{G}{\to}$ is a locally confluent noetherian reduction relation that is adequate for $\equiv_{\mathrm{Id}(G)}$. Now consider the polynomials $f = x^2 - y$ and $g = xy + 2$, we want to know whether $[f] = [g]$ or not. Because f is already in $\underset{G}{\to}$-normal form, we only have to calculate a $\underset{G}{\to}$-normal form for g. By reducing $g \underset{G}{\to} g - \frac{6}{7}h_0$ we achieve the polynomial $g' = \frac{1}{7}\left(-12x^2 - 5y + 11x + 29\right)$ which is in normal form. Because $f \neq g'$, we conclude that $[f] \neq [g]$. In particular, we see that $[1]$,$[x^n]$ and $[y^n]$ for $n \in \mathbb{N}$ are different classes w.r.t. $\equiv_{\mathrm{Id}(G)}$

CHAPTER 4

Applications and specializations of Gröbner-bases

In Section 4.1 several applications of Gröbner theory are given. In Sections 4.2 and 4.3 we see how Gröbner theory is linked with the Euclid's algorithm the Gaussian elimination. Moreover we show how Gröbner theory generalizes this concepts and can be used in order to compute them.

4.1. Applications

This section is a review of the applications of Gröbner theory shown in [2].

Given an ideal I and provided of a Gröbner basis G, two polynomials $f, g \in K[X_1, X_2, ..., X_n]$ are in the same equivalence class w.r.t. $\equiv_I$ iff $f - g \in I$ iff $f - g \xrightarrow[G]{*} 0$; this last formula can be be effectively computed by Buchberger's algorithm and Algorithm 2 (REDPOL). Then we have the first application of Gröbner theory.

PROPOSITION 142. *Let F be a finite subset of $K[X_1, X_2, ..., X_n]$, let $I = \mathrm{Id}(F)$ and assume that K is computable. Then the following hold:*

1) *The membership problem for the ideal I is decidable.*

2) *The residue class ring $K[X_1, X_2, ..., X_n]/I$ is computable.*

PROOF. (i) is obvious form the above commented while (ii) is consequence of (i) (see Example 60). □

REMARK 143. For the proof of the above result, we can also reason that given a Gröbner basis G for $\mathrm{Id}(F)$, $\xrightarrow[G]{}$ is a locally confluent noetherian reduction relation that is adequate for $\equiv_I$ by Theorem 105, Theorem 91 and Lemma 98, thus Algorithm 1 proofs claim (i).

PROPOSITION 144. *Let $K[X_1, X_2, ..., X_n]$, K a subfield of K', $n' \geq n$, and $K'[X_1, X_2, ..., X_{n'}]$. Then the following hold:*

1) *Suppose $\leq$ is a term order on T'. Then every Gröbner basis in $K[X_1, X_2, ..., X_n]$ w.r.t. the restriction of $\leq$ to T is a Gröbner basis in $K'[X_1, X_2, ..., X_{n'}]$ w.r.t. $\leq$.*

2) *Let F be a finite subset of $K[X_1, X_2, ..., X_n]$ and denote by*

$$Id_{K'}(F) \text{ and } Id_K(F)$$

the ideals generated by F in $K'[X_1, X_2, ..., X_{n'}]$ and $K[X_1, X_2, ..., X_n]$, respectively. Then

$$Id_{K'}(F) \cap K[X_1, X_2, ..., X_n] = Id_K(F).$$

PROOF. (i) Let $g_1, g_2 \in G$; then $\operatorname{spol}(g_1, g_2)$ is the same in $K[X_1, X_2, ..., X_n]$ and in $K'[X_1, X_2, ..., X_{n'}]$ and since $\operatorname{spol}(g_1, g_2) \xrightarrow[G]{*} 0$ in $K[X_1, X_2, ..., X_n]$, so it does in $K'[X_1, X_2, ..., X_{n'}]$. By Theorem 124, G is a Gröbner basis in $K'[X_1, X_2, ..., X_{n'}]$.

(ii) The inclusion $\supseteq$ is trivial. Now consider

$$f \in \operatorname{Id}_{K'}(F) \cap K[X_1, X_2, ..., X_n],$$

and let $G \subseteq K[X_1, X_2, ..., X_n]$ be a Gröbner basis of $\operatorname{Id}_K(F)$ w.r.t. some term order $\leq$. By (i), G is Gröbner basis in $K'[X_1, X_2, ..., X_{n'}]$ w.r.t. any term order on T' whose restriction to T equals $\leq$. Hence

$$\operatorname{Id}_{K'}(G) = \operatorname{Id}_{K'}(F),$$

and so $f \xrightarrow[G]{*} 0$. Since $f \in K[X_1, X_2, ..., X_n]$ and this reduction takes place in $K[X_1, X_2, ..., X_n]$, we see that $f \in \operatorname{Id}_K(G) = \operatorname{Id}_K(F)$ by Lemma 98. □

In the following, we focus on applying Gröbner bases theory for solving problems related with ideals of polynomials over a field and the residue class ring $K[X_1, X_2, ..., X_n]/\operatorname{Id}(F)$ for some finite set $F \subseteq K[X_1, X_2, ..., X_n]$. However we remark that further motivations and applications, as the uniform word problem or the computation of Syzygies, are in the kernel of this Gröbner basis theory.

PROBLEM 145. Given two finite sets $F_1, F_2 \subseteq K[X_1, X_2, ..., X_n]$ decide whether $\operatorname{Id}(F_1) \subseteq \operatorname{Id}(F_2)$.

SOLUTION. Compute G_2 a Gröbner basis for F_2. Then set $\operatorname{Id}(F_1) \subseteq \operatorname{Id}(F_2)$ iff for all $f \in F_1$, $f_1 \xrightarrow[G_2]{*} 0$. □

PROBLEM 146. Given two finite sets $F_1, F_2 \subseteq K[X_1, X_2, ..., X_n]$ decide whether $\operatorname{Id}(F_1) = \operatorname{Id}(F_2)$.

SOLUTION. Clearly application of solution before would lead to solve the equality problem. Other possible solution is to compute reduced Gröbner bases for F_1 and F_2, then $F_1 = F_2$ iff such bases are equal. □

PROPOSITION 147. *Let G be a Gröbner basis. Let*

$$B = \{[t] \mid t \in T \text{ and } t \notin \operatorname{mult}(\operatorname{HT}(G))\}.$$

Then B is a linearly independent vector basis for the vector space $K[X_1, X_2, ..., X_n]/\operatorname{Id}(G)$.

PROOF. By definition B is formed only by classes of terms. Moreover, if $[f] \in K[X_1, X_2, ..., X_n/\operatorname{Id}(G)]$ we may consider that f is in $\xrightarrow[G]{}$-normal form, and so it cannot be reduced modulo G, that is, if $t \in T(f)$ then $t \notin \operatorname{mult}(\operatorname{HT}(G))$, and so B is a generator system. Assume for contradiction that B is not linearly independent, then there exists a linear dependence

$$c_1 \cdot [t_1] + ... + c_l \cdot [t_l] = [0],$$

with $c_i \neq 0$ for some $1 \leq i \leq l$ and $[t_j] \in B$ for $j = 1, ..., l$. Hence

$$0 \neq f = c_1 \cdot t_1 + ... + c_l \cdot t_l \in \operatorname{Id}(G),$$

and so, by Theorem 105, f can be reduced to 0 modulo G. However, f is already in normal form because non of the t_i can be reduced modulo G, a contradiction. □

EXAMPLE 148. [2]Consider $G = \{f_1, f_2, f_3, h_0\}$ as in Example 140, that is

$$\begin{aligned} f_1 =& 3x^2y + 2xy + y + 9x^2 + 5x - 3, \\ f_2 =& 2x^3y - x - y + 6x^3 - 2x^2 - 3x + 3, \\ f_3 =& x^3y + x^2y + 3x^3 + 2x^2, \\ h_0 =& \frac{7}{6}xy + \frac{5}{6}y + 2x^2 - \frac{11}{6}x - \frac{5}{2}. \end{aligned}$$

By definition, $t \in \text{mult}(\text{HT}(F))$ iff $\text{HT}(f)$ divides t for some $f \in F$. Moreover, we also know that a term $x^{e_1}y^{e_2}$ divides $x^{d_1}y^{d_1}$ if and only if $e_1 \leq d_1$ and $e_2 \leq d_2$. Hence $\text{HT}(h_0) = xy$ does not divide 1, $x^n y^0$ and $x^0 y^n$ for any $n \in \mathbb{N}$. Because $\text{HT}(h_0)$ divides $\text{HT}(f_i)$ for $i = 1, 2, 3$, we conclude that $B = \{[1], [x^n], [y^n] \mid n \in \mathbb{N}\}$ is a linear independent basis of $K[X_1, X_2, ..., X_n]/\text{Id}(G)$.

PROBLEM 149. Find a basis for the vector space $K[X_1, X_2, ..., X_n]/\text{Id}(F)$ and for any two elements $[u], [v] \in B$ find a linear representation of $[u] \cdot [v]$ in terms of the basis elements in B (i.e. find the multiplication table for $K[X_1, X_2, ..., X_n]/\text{Id}(F)$).

SOLUTION. Compute G a Gröbner basis for $\text{Id}(F)$ and set B as in proposition above as basis of the residue class ring. For the representation of $[u] \cdot [v]$ w.r.t. B, we calculate a $\underset{G}{\rightarrow}$-normal form h of $u \cdot v$; thus any term in h is in $\text{mult}(\text{HT}(G))$ since h is not reducible modulo G, and so $h \in B$. □

PROBLEM 150. Given a finite set $F \subseteq K[X_1, X_2, ..., X_n]$ such that $K[X_1, X_2, ..., X_n]/\text{Id}(F)$ is a finite dimensional vectorial space. Given two polynomials f, h, find g such that $fg \equiv_I h$ in $K[X_1, X_2, ..., X_n]/I$ where $I = \text{Id}(F)$.

SOLUTION. Compute G, a Gröbner basis for $\text{Id}(F)$. Represent f and h as linear combination of the elements in B and represent g as a linear combination of elements of B (which is finite) with unknown coefficients. Thus, one gets a finite linear system of equations for the unknown coefficients, which is solvable iff a solution g exists. □

REMARK 151. In particular, we can calculate the inverse of an element $f \in K[X_1, X_2, ..., X_n]/\text{Id}(G)$.

EXAMPLE 152. Consider the set $H = G \cup \{x^3, y^2\}$ where F is as in Example 140. Then $B = \{[1], [x], [x^2], [y]\}$ is a basis of $K[X_1, X_2, ..., X_n]/\text{Id}(H)$. Consider the polynomials $f = 3x^2 + 1$ and $h = 3y - 2$ in $K[X_1, X_2, ..., X_n]$, we want to find g such that $[f] \cdot [g] = [h]$. Clearly, $[f] = 3[x^2] + [1]$ and $[h] = 3[y] + -2[1]$; we write

$$g = a_1[1] + a_2[x] + a_3[x^2] + a_4[y].$$

We see that $[x^2] \cdot [1] = [x^2]$, $[x^2] \cdot [x] = [x^3] = [0]$ since $x^3 \in \text{mult}(\text{HT}(H))$, $[x^2] \cdot [x^2] = [x^4] = [0]$ since $x^4 \in \text{mult}(x^3)$and $[x^2] \cdot [y] = [x^2y] = [0]$ since $x^2y = \text{HT}(f_1)$. Hence, the equation $[f] \cdot [g] = [h]$ can be written as

$$(3a_1[x^2]) + (a_1[1] + a_2[x] + a_3[x^2] + a_4[y]) = +3[y] + -2[1],$$

and so, we have the linear system

$$\begin{aligned} a_1 &= -2, \\ a_2 &= 0, \\ 3a_1 + a_3 &= 0, \\ a_4 &= 3. \end{aligned}$$

which has unique solution $[g]$, where $g = 3y + 6x^2 - 2$.

DEFINITION 153. For a set $F \subseteq K[X_1, X_2, ..., X_n]$, we say that $a = (a_1, a_2, ..., a_n)$ is a solution for F, if $f(a) = 0$ for all $f \in F$.

PROBLEM 154. Given a finite set $F \subseteq K[X_1, X_2, ..., X_n]$, decide whether F has finitely or infinitely many solutions.

SOLUTION. Compute a Gröbner basis G for $\mathrm{Id}(F)$ w.r.t. some term order. We claim that F has finitely many solutions iff for all $i = 1, ..., n$ a power of product of the form $X_i^{j_i}$ occurs among $\mathrm{HT}(G)$.

It is known that F has finitely many solutions iff the vector space $K[X_1, X_2, ..., X_n]/\mathrm{Id}(F)$ has finite vector space dimension, and by problem 147 we know that

$$B = \{[t] \mid t \in T \text{ and } t \notin \mathrm{mult}(\mathrm{HT}(G))\},$$

is a basis for the residue class ring. If for all $i = 1, ..., n$, a power of product of the form $X_i^{j_i}$ occurs among $\mathrm{HT}(G)$, then the set $B = \left\{[X_i]^j \mid 0 \leq j < j_i, i = 1, ..., n\right\}$ is finite. Conversely, if condition above does not occur for some $1 \leq i \leq n$, then $\left\{\left[X_i^j\right] \mid j \in \mathbb{N}\right\} \subseteq B$ since otherwise, $X_i^j \in \mathrm{mult}(\mathrm{HT}(G))$ for some j, and so $X_i^{j'} \in \mathrm{HT}(G)$ for some $j' \leq j$. □

PROPOSITION 155. *Let $G \subseteq K[X_1, X_2, ..., X_n]$ be a Gröbner basis w.r.t. the inverse lexicographical ordering. Then*

$$\mathrm{Id}(G) \cap K[X_1, X_2, ..., X_i] = Id(G \cap K[X_1, X_2, ..., X_i]).$$

for $i = 1, ..., n$ where the ideal on right side is formed in $K[X_1, X_2, ..., X_i]$.

PROOF. If $g \in \mathrm{Id}(G) \cap K[X_1, X_2, ..., X_i]$, then g can be reduced to 0 modulo G. Moreover, since we are using the inverse lexicographical ordering, g can be reduced to zero subtracting $b_j \cdot u_j \cdot g_j$ where $b_j \in K$, u_j is a monomial in $K[X_1, X_2, ..., X_i]$ and $g_j \in G$ is such that $\mathrm{HT}(g_j)$ contains only the indeterminates form the set $\{X_1, X_2, ..., X_i\}$. Hence all power products occurring in g_j contains only indeterminates in this set (just like u_j). Thus, we obtain a representation for g of the form

$$g = \sum b_j \cdot u_j g_j,$$

which shows that $T(g) \subseteq T(X_1, X_2, ..., X_i)$. Thus, we may conclude that $g \in \mathrm{Id}(G \cap K[X_1, X_2, ..., X_i])$. □

PROBLEM 156. Given a Gröbner basis G in $K[X_1, X_2, ..., X_n]$, such that G has finitely many solutions. Find $p \in \mathrm{Id}(G) \cap K[X_1]$ with minimal degree provided that $\mathrm{Id}(G) \cap K[X_1] \neq \emptyset$.

Solution. First recall that X_1 is set for convenience, that is, we can find the polynomial with minimal degree in $\mathrm{Id}(G) \cap K[X_i]$ for very i provided that $\mathrm{Id}(G) \cap K[X_i] \neq \emptyset$.

The calculus of the minimal polynomial p can be carried out by the following algorithm:

Algorithm 8 MINIPOL

Specification: $p \leftarrow \mathrm{UNIPOL}(G)$
Given: a Gröbner basis G in $K[X_1, X_2, ..., X_n]$
Find: a polynomial p in $G \cap K[X_1]$ with minimal degree
$i = 1$
repeat $p_i =$ a normal form of X_1^i modulo G
$i = i + 1$
until there exists $(d_0, ..., d_{i-1}) \neq (0)$ with $d_0 + d_1 p_1 + ... + d_{i-1} p_{i-1} = 0$
$r = i - 1$
return $p = d_r X_1^r + d_{r-1} X_1^{r-1} + ... + d_1 X_1 + d_0$
end MINIPOL

Because G has finitely many solutions, no scalar $\lambda \in K$ is in G, and so every polynomial $p \in \mathrm{Id}(G) \cap K[X_1]$ has degree greater or equal than one. With this, *Correctness* should be clear whereas *Termination* is consequence of $\mathrm{Id}(G) \cap K[X_1] \neq \emptyset$. □

Problem 157. Given a finite set $F \subseteq K[X_1, X_2, ..., X_n]$, find all solutions of F provided that F has finitely many solutions.

Solution. Compute a Gröbner basis G a w.r.t. the inverse lexicographical order. Because G has finitely many solutions, as argued in Problem 154, $X_i^{j_i}$ occurs among $\mathrm{HT}(G)$ for some $j_i \in \mathbb{N}$ for all $i = 1, ..., n$. In particular $\mathrm{Id}(G) \cap K[X_1] \neq \emptyset$.

Now, we are under the hypothesis of the previous problem and the calculus of the solutions can be carried out by the following algorithm:

Algorithm 9 SOLUTIONS

Specification: $S \leftarrow$ **SOLUTIONS** (G)
Given: a Gröbner basis G in $K[X_1, X_2, ..., X_n]$
Find: all solutions of G
begin
$p =$ **MINPOL** (G)
$S_1 = \{(a) \mid p(a) = 0\}$
for $i = 1, ..., n-1$ **do**
$S_{i+1} = \emptyset$
for all $(a_1, a_2, ..., a_i) \in S_i$ **do**
$H \leftarrow \{g'(a_1, a_2, ..., a_i, X_{i+1}) \mid g' \in G'\}$ where
$G' = G \cap K[X_1, X_2, ..., X_{i+1}] \setminus K[X_1, X_2, ..., X_i]$
$p = \gcd(H)$
$S_{i+1} = S_{i+1} \cup \{(a_1, a_2, ..., a_i, a) \mid p(a) = 0\}$
end
end
return S_n
end SOLUTIONS

Termination of the algorithm is clear. Let's check *Correctness*. If $a = (a_1, a_2, ..., a_n)$ is a solution of G, we proof by induction that $(a_1, a_2, ..., a_i) \in S_i$ for $i = 1, ..., n$. For $i = 1$, since $p \in \mathrm{Id}(G)$ we have $p(a_1) = 0$, and so $a_1 \in S_1$. Now we assume the result is true for i, we show that $(a_1, a_2, ..., a_{i+1}) \in S_{i+1}$. Because a is a solution of G, there exist $g \in G$ with $\mathrm{HT}(g) = X_{i+1}^{j_{i+1}}$ for some $j_{i+1} \in \mathbb{N}$ (see Problem 154). Because G is Gröbner basis w.r.t. the inverse lexicographical order, the variables X_j with $j > i+1$ are not in g, and so g can be seen as a polynomial in G'. Hence $g(a_1, a_2, ..., a_i, X_{i+1}) \in H$ and so $p(X_{i+1}) = \gcd(H) \mid g(a_1, a_2, ..., a_i, X_{i+1})$. Because a is a solution of G, $g(a_1, a_2, ..., a_{i+1}) = 0$ since $g \in G'$, and so $p(a_{i+1}) = 0$, that is, $(a_1, a_2, ..., a_{i+1}) \in S_{i+1}$. We have shown that algorithm above computes the all the solutions of G. Now, if $f \in F$, then $f \in \mathrm{Id}(F) = \mathrm{Id}(G)$ and so $f = \lambda_1 g_1 + ... + \lambda_m g_m$ for some $\lambda_i \in K$, $g_i \in G$. Hence if $g(a) = 0$ for all $g \in G$, then $f(a) = 0$. We see that all the solutions of G are solutions of F, and repeating the argument for G, we conclude that the solutions of F and G are the same. □

Remark 158. The above algorithm is limited by the difficulty of finding the roots of a polynomial, however this is an intrinsic problem of the solvability if polynomial equations. Moreover, the determination of p as the polynomial in $K[X_1]$ is non deterministic since it can be computed by Problem 156.

Example 159. Consider F as in Remark 34. We know by Example 130 that $G = \left\{y + x^2 - \frac{3}{2}x - 3,\ x^3 - \frac{5}{2}x^2 - \frac{5}{2}x\right\}$ is a reduced Gröbner basis for $\mathrm{Id}(F)$ w.r.t. the inverse lexicographical order. Application of Algorithm 8 produced $p = x^3 - \frac{5}{2}x^2 - \frac{5}{2}x$ as result. To see this, note that x, x^2 are in $\underset{G}{\rightarrow}$-normal form, and so, the equation $d_0 + d_1 x + d_2 x^2 = 0$ only has trivial solution $d_0 = d_1 = d_2 = 0$. Then x^3 is the first power of x that is reducible modulo G, and $p_3 = \frac{5}{2}x^2 + \frac{5}{2}x$ is a normal form for x^3. Now the equation $d_0 + d_1 x + d_2 x^2 + d_3 p_3 = 0$ has as solution $d_0 = 0, d_1 = -\frac{5}{2}, d_3 = -\frac{5}{2}$ and $d_3 = 1$. Hence $p = x^3 - \frac{5}{2}x^2 - \frac{5}{2}x$ is a polynomial in $\mathrm{Id}(G) \cap K[x]$ with minimal degree.

Now, we have $S_1 = \left\{0, \frac{5}{4} - \frac{\sqrt{65}}{4}, \frac{5}{4} + \frac{\sqrt{65}}{4}\right\}$ and $G' = \left\{y + x^2 - \frac{3}{2}x - 3\right\}$. Hence, for each root of p, we have $H_0 = \{y - 3\}$, $H_{\frac{5}{4} - \frac{\sqrt{65}}{4}} = \left\{y - \frac{\sqrt{65}}{4} + \frac{3}{4}\right\}$ and $H_{\frac{5}{4} + \frac{\sqrt{65}}{4}} = \left\{y + \frac{\sqrt{65}}{4} + \frac{3}{4}\right\}$. Because H has only one polynomial $p = \gcd(H)$ is its unique polynomial and so

$$S_2 = \left\{(a, b) \mid a \in \left\{0, \frac{5}{4} \pm \frac{\sqrt{65}}{4}\right\}, b \in \left\{3, \pm\frac{\sqrt{65}}{4} - \frac{3}{4}\right\}\right\},$$

are all the solutions of G.

4.2. Euclid's Algorithm

The following is based on [4, pg. 95, Ex. 11].

We show that the result of the Euclid's algorithm in $K[x]$ for two polynomials $f, g \in K[x]$ is a reduced Gröbner basis for $\mathrm{Id}(\{f, g\})$ (after reducing the basis).

First, we describe the connection between division and Euclidean algorithms in $K[x]$ and Gröbner bases.

Given two polynomials $f, g \in K[x]$ with $g \neq 0$, by Theorem 27 there exist unique polynomials $q, r \in K[x]$ such that $f = qg + r$ with $r = 0$ or $r \neq 0$ and $\deg(r) < \deg(g)$. We now use this fact to show that the reduction relation $\underset{g}{\rightarrow}$ in $K[x]$ has unique normal form using the division algorithm (Theorem 27). Since $\underset{g}{\rightarrow}$ is noetherian, every polynomial $f \in K[x]$ has an least one normal form r, and we can find a finite $\rightarrow$-chain

$$f \underset{g}{\rightarrow} f - q_1 g \underset{g}{\rightarrow} f - q_1 g - q_2 g \underset{g}{\rightarrow} \ldots \underset{g}{\rightarrow} \underbrace{f - q_1 g - \ldots - q_n g}_{=r},$$

for some monomials $q_i \in M$. Because r cannot be reduced modulo g, $r = 0$ or $r \neq 0$ and $\deg(r) < \deg(g)$. Therefore, given that $f = (q_1 + q_2 + \ldots + q_n) g + r$, we see that $q = q_1 + q_2 + \ldots + q_n$ and r are the quotient and the remainder and so they are uniquely determined by f, g. Therefore, uniqueness of the remainder r implies $\underset{g}{\rightarrow}$ has unique normal form.

If we have the finite set $G = \{f, g\}$, then we may consider to reduce it. To do so Algorithm 3 (REDUCTION) may be applied to the univariate case $K[x]$, but as said before it specializes to the Euclid's algorithm.

Euclid's Algorithm: Given two polynomials $f, g \in K[x]$, with $g \neq 0$ and $\deg(f) \geq \deg(g)$ we perform the division of f by g. Then

$$f = q_1 g + r_1,$$

where q_1, r_1 are the quotient and the remainder of the division. If $r \neq 0$, because $\deg(r) < \deg(g)$ we can perform the division of g by r_1, and we have

$$g = q_2 r_1 + r_2,$$

where q_2, r_2 are the quotient and the remainder. If we set $i = 1$, division of r_i by r_{i+1} may be performed and a new remainder r_{i+2} may be taking in account, and division of r_{i+1} by r_{i+1} may proceed if $r_{i+1} \neq 0$. Repetition of this process leads to

a chain of remainders which is finite since $0 \leq \deg(r_i) < \deg(r_{i-1})$. Say we obtain

$$\begin{aligned} f &= q_1 g + r_1, \\ g &= q_2 r_1 + r_2, \\ r &= q_3 r_2 + r_3, \\ \cdots &\quad \cdots \quad \cdots \\ r_{k-2} &= q_k r_{k-1} + r_k, \\ r_{k-1} &= q_{k+1} r_k + r_{k+1}. \end{aligned}$$

Because division of r_k by r_{k+1} cannot be performed, $r_{k+1} = 0$ and r_k divides r_{k-1}. Euclid's theorem asserts that $\gcd(f,g) = \gcd(g, r_1)$ if $r_1 \neq 0$, and so $\gcd(f,g) = \gcd(r_i, r_{i+1})$ for all $i < k$. In particular $\gcd(f,g) = \gcd(r_{k-1}, r_k) = r_k$.

If $G = \{r_k\}$ our previous claim stands that $\mathrm{Id}(\{f,g\}) = \mathrm{Id}(G)$ and G is a reduced Gröbner basis.

In order to link Euclid's algorithm with Gröbner-bases theory we give the following version of Euclid's algorithm.

Recall that we write $r_{i-1} \xrightarrow[r_i]{*} r_{i+1}$ where r_{i+1} is a $\xrightarrow[r_i]{}$-normal form meaning that we perform the division of r_{i-1} by $r_i \neq 0$ with residue r_{i+1}.

Algorithm 10 EUCLID'S

Specification: $G \leftarrow$ EUCLID'S (f,g)
Given: $f, g \in K[x]$, with $g \neq 0$ and $\deg(f) \geq \deg(g)$
Find: $G = \{r_k\}$ so that $\{f,g\}$ reduces to G
begin
$r_{-1} = f$, $r_0 = g$
$i = 0$
while $r_i \neq 0$ **then**
  $G = \{r_{i-1}, r_i\}$
  Find r_{i+1} in $\xrightarrow[r_i]{}$-normal form so that $r_{i-1} \xrightarrow[r_i]{*} r_{i+1}$
  $i = i + 1$
end
$G = \{r_k\}$
return(G)
end EUCLID'S

Termination of the algorithm is clear.

Correctness: As before, say the **while**-loop ends at $i = k+1$ with $G = \{r_{k-1}, r_k\}$ and denote by G_i the set G during the $i+1$th run of the loop. We claim that the upgrading of G consist in a reduction of G, to see this note that $r_{i-1} \in G_i$ is reduced to r_{i+1} using $r_i \in G_i \setminus \{r_{i-1}\}$. Now, actualization of G_i consists in removing the polynomial r_{i-1} and joining r_{i+1}. Therefore G_0 reduces to G_k and since upon termination $r_{k+1} = 0$ and G_k reduces to $G_{k+1} = \{r_k\}$, G_k also reduces to G_{k+1}.

Because each run of the loop produces a reduction of G, $\mathrm{Id}(G)$ is an invariant of the loop and since upon initialization $G_0 = \{f,g\}$, then $\mathrm{Id}(\{f,g\}) = \mathrm{Id}(G_k) = \mathrm{Id}(G_{k+1})$. Now the claim G_{k+1} is a reduced Gröbner basis for $\mathrm{Id}(\{f,g\})$ immediately follows from uniqueness of the remainder in $K[x]$.

As consequence of our first claim, given that any two polynomials $f, g \in K[x]$ the set $\{f, g\}$ may be reduced to a set with only one element. Therefore, any finite set G can be reduced to a set with a unique element. Since $K[x]$ is noetherian, every ideal I is finitely generated and so I has a reduced Gröbner basis with a single element. Moreover, $K[x]$ is a principal ideal domain.

If we relate the division algorithm which asserts there exists of unique residues as the equivalent of Gröbner bases existence in $K[x]$, Euclid's algorithm should be related with Buchberger's algorithm for constructing such a basis.

EXAMPLE 160. Given $f = (x-1)\left(x^2-1\right) = x^3 - x^2 - x + 1$ and $g = (x-1)x^2 = x^3 - x^2$. If we set $G_0 = \{f, g\}$ the above algorithm may start by reducing f modulo g; in particular, we have $f \underset{g}{\to} f' = x - 1$ and $G_1 = \{f', g\}$. Now g can be reduced by to zero by means of f', and so the while-loop ends and $G_2 = \{f' = x - 1\}$ is the reduced Gröbner-bases for $\mathrm{Id}(\{f, g\})$,that is, $x - 1 = \gcd(f, g)$.

4.3. Gaussian elimination

The following is based on [4, pg. 95, Exercise 10].

Let $A = (a_{ij})$ be a $n \times m$ matrix with entries in K and let $f_i = a_{i1}x_1 + ... + a_{in}x_n$ be the linear polynomials in $K[x_1, x_2, ..., x_n]$ determined by the rows of A. Then consider $I = \mathrm{Id}(f_1, f_2, ..., f_n)$ and the lexicographical order in T. Now let $B(b_{ij})$ be the row echelon matrix determined by A and let $g_1, g_2, ..., g_t$ be the polynomials determined by the non-zero rows of B. We now show that $G = \{g_1, g_2, ..., g_t\}$ is a reduced Gröbner basis of I w.r.t the lexicographical order.

First, remark that by echelon matrix we refer to the matrix obtained after performing the Gauss elimination so to obtain an upper triangular matrix, and then perform again the row elimination, now, from down to top.

Row operation in the Gaussian elimination can be of three different types,

1) multiply a row by a scalar $a \in K$,
2) swap row i with row j, and
3) adding a row j to a row i multiplied by a scalar $a \in K$.

The first case, applied to row i, produces the family of polynomials $F = \{f_1, ..., af_i, ..., f_n\}$ and it is clear that $I = \mathrm{Id}(F)$. In the second case, we have the family of polynomials $F = \{f_1, ..., f_{i-1}, f_j, f_i, ..., f_{j-1}, f_i, f_{i+1}, ..., f_n\}$ and again $I = \mathrm{Id}(F)$. Finally, the third case gives us the family $F = \{f_1, ..., f_i - af_j, ..., f_n\}$. We claim that $I = \mathrm{Id}(F)$. The relation $I \subseteq \mathrm{Id}(F)$ follows easily from the fact that

$$\begin{aligned} g &= a_1 f_1 + ... + a_n f_n \\ &= a_1 f_1 + ... + a_i(f_i - af_j + af_j) + ... + f_n \\ &= a_1 f_1 + ... + a_i(f_i - af_j) + ... + (a_j - a_i a) f_i + ... + f_n. \end{aligned}$$

Conversely, if $g \in I$ then

$$\begin{aligned} g &= a_1 f_1 + ... + a_i(f_i - af_j) + ... + f_n \\ &= a_1 f_1 + ... + a_i f_i + ... + (a_j - a_i a) f_j + ... + f_n \end{aligned}$$

and $\mathrm{Id}(F) \subseteq I$.

Because the family of polynomials $G = \{g_1, g_2, ..., g_t\}$ has been obtained from $\{f_1, f_2, ..., f_n\}$ by performing these operations, we conclude that $I = \mathrm{Id}(G)$.

To see that G is a Gröbner basis, we prove that $\operatorname{spol}(g_i, g_j) \underset{G}{\overset{*}{\to}} 0$ for all $g_i, g_j \in G$. Because g_i, g_j are defined by the echelon matrix B, we can write $g_i = x_r + g_i'$ and $g_j = x_k + g_j'$ where g_i', g_j' are linear polynomials in $K[x_{r+1}, ..., x_n]$ and $K[x_{k+1}, ..., x_n]$ respectively. Now, $\operatorname{spol}(g_i, g_j) = x_k x_r + x_k g_i' - x_r x_k - x_r g_j' = x_k g_i' - x_r g_j'$, and we write $g_i' = \sum_{t=1}^{\alpha} m_t$ as sums of monomials with $m_1 > m_2 > ... > m_\alpha$. Because $\operatorname{HT}(g_j) = x_k$, we may reduce $\operatorname{spol}(g_i, g_j) \underset{g_j}{\to} \operatorname{spol}(g_i, g_j) - m_1 g_j$ by eliminating $x_k \operatorname{HT}(g_i') = x_k \operatorname{HT}(m_1)$. Repeating this process up to m_α we get

$$\begin{aligned} \operatorname{spol}(g_i, g_j) &\underset{g_j}{\overset{*}{\to}} \operatorname{spol}(g_i, g_j) - m_1 g_j - ... - m_\alpha g_j \\ &= \operatorname{spol}(g_i, g_j) - (m_1 + m_2 + ... + m_\alpha) g_j \\ &= \operatorname{spol}(g_i, g_j) - g_i' \left(x_k + g_j'\right) \\ &= -x_r g_j' - g_i' g_j'. \end{aligned}$$

By repeating the argument for $-x_r g_j' - g_i' g_j'$ using $-x_r$ instead x_k and g_i instead of g_j, we have

$$-x_r g_j' - g_i' g_j' \underset{g_i}{\overset{*}{\to}} \left(-x_r g_j' - g_i' g_j'\right) - \left(-g_j' g_i\right) = -x_r g_j' - g_i' g_j' + g_j' x_r + g_j' g_i' = 0.$$

So far, we have proved that $\operatorname{spol}(g_i, g_j) \underset{\{g_i, g_j\}}{\overset{*}{\to}} 0$ for every pair $g_i \neq g_j \in G$, that is, G is a Gröbner basis.

Furthermore, G is reduced. Because we are dealing with linear equations, no term of the form $x_i x_j \in T(G)$. Then, if $g_i \underset{g_j}{\to} h$ by eliminating t, $t = \operatorname{HT}(g_j)$ and the claim follows since such reductions are equivalent to subtracting row j to row i multiplied by the appropriate factor in K, which cannot happen since the polynomials in G are defined by the non-zero rows of B, the echelon matrix of A.

Index

Nomenclature

$\mathrm{HC}(f)$	head coefficient of f
$\overset{*}{\leftrightarrow}$	reflexive-transitive closure of $\rightarrow$
$\overset{*}{\rightarrow}$	reflexive-transitive closure of $\rightarrow$
$\mathrm{C}(t, f)$	the coeficient of the term t in f
$\deg(f)$	degree of the polynomial f
$\Delta(M)$	diagonal of M
$\downarrow$	relation
$\equiv_I$	congruece relation modulo I
η	exponent map
$\leftrightarrow$	symmetric closure of $\rightarrow$
$\mathrm{Id}(F)$	ideal generated by F
$\leq'$	natural partial ordern on $\mathbb{N}^n$
$\mathcal{P}(X)$	power set of X
$\mathcal{P}_{fin}(X)$	set of all finite subsets of X
$\mathrm{mult}(S)$	the set of all multiples of elements of S
$\mathrm{HM}(f)$	head monomial of f
$\mathrm{HM}(I)$	set of head monomials of I
$\mid$	divisibility relation
$\overset{n}{\rightarrow}$	power of the relation $\rightarrow$
$\mathrm{red}(f)$	reductum
$\mathrm{spol}(g_1, g_2)$	S-polynomial of g_1 and g_2
$\mathrm{HT}(f)$	head term of f
$\mathrm{HT}(I)$	set of head terms of I
$A \triangle B$	symmetric difference or union without intersection of A and B
$C(f)$	the set of all coefficientes of f
$f \underset{P}{\rightarrow} g$	polynomial reduction
$f \underset{p}{\rightarrow} g$	polynomial reduction
$f \underset{P}{\rightarrow} g\,[t]$	polynomial reduction
$f \underset{p}{\rightarrow} g\,[t]$	polynomial reduction
M	the set of all monomials
$M/\sim$	quotient of M by the equivalence relation $\sim$
$M(f)$	the set of all monomials of f
r	(binary) relation
r_s	strict part
$r \circ s$	product of two relations
$R[X_1, X_2, ..., X_n]$	polynomial ring over R in the indeterminates $X_1, X_2, ..., X_n$

$R[X_1, X_2, ..., X_n] / \equiv_I$	residue class ring of the ring of polynomials
r^*	reflexive-transitive closure
r^+	transitive closure of r
r^{-1}	inverse relation
T	the set of all terms
$T(X_1, X_2, ..., X_n), T$	set of all terms with variables $X_1, X_2, ..., X_n$
$T(f)$	the set of all terms of f

Bibliography

[1] T. Becker, V. Weispfenning, and H. Kredel. *Grobner Bases - A Computational Approach to Commutative Algebra*. Corrected. Graduate Texts in Mathematics. Springer, 1993. ISBN: 0387979719,9783540979715,9780387979717,3540979719 (see pp. 3, 48, 51).

[2] N. Bose et al. Multidimensional systems theory. In: *Reidel, Dordrecht* (1985) (see pp. 3, 11, 39, 42, 48, 49, 53, 55).

[3] B. Buchberger. "A criterion for detecting unnecessary reductions in the construction of Grobner-bases". In: *Symbolic and algebraic computation*. Springer, 1979, pp. 3–21 (see pp. 44, 48).

[4] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra: with 91 illustrations*. 2nd ed. Undergraduate texts in mathematics. Springer, 2006. ISBN: 0387946802,9780387946801 (see pp. 9, 37, 59, 61).

[5] M. Reid. *Undergraduate commutative algebra*. Vol. 29. Cambridge University Press, 1995 (see p. 9).