2.3. The notion of a Gröbner basis

Before we start with the technical details, let us briefly review the historical development leading to the concept of Gröbner bases. In his seminal paper of 1890 David Hilbert [1] gave a proof of his famous Basis Theorem as well as of the structure and length of the sequence of syzygy modules of a polynomial system. Implicitly he also showed that the Hauptproblem (the main problem of the theory of polynomial ideals, according to B.L. van der Waerden), i.e. the problem whether $f \in I$ for a given polynomial f and polynomial ideal I, can be solved effectively. Hilbert's solution of the Hauptproblem (and similar problems) was reinvestigated by G. Hermann [2] in 1926. She counted the field operations required in this effective procedure and arrived at a double exponential upper bound in the number of variables. In fact, Hermann's, or for that matter Hilbert's, algorithm always actually achieves this worst case double exponential complexity. The next important step came when B. Buchberger, in his doctoral thesis [3] of 1965 advised by W. Gröbner, introduced the notion of a Gröbner basis (he did not call it that at this time) and also gave an algorithm for computing it. Gröbner bases are very special and useful bases for polynomial ideals. In subsequent publications Buchberger exhibited important additional applications of his Gröbner bases method, e.g. to the solution of systems of polynomial equations. In the worst case, Buchberger's Gröbner bases algorithm is also double exponential in the number of variables, but in practice there are many interesting examples which can be solved in reasonable time. But still, in the worst case, the double exponential behaviour is not avoided. And, in fact, it cannot be avoided by any algorithm capable of solving the Hauptproblem, as was shown by E.W. Mayr and A.R. Meyer in 1982.

When we are solving systems of polynomial (algebraic) equations such as

$$\begin{array}{rcl} f_1(x_1,\ldots,x_n) & = & 0\ , \\ & \vdots & \\ f_m(x_1,\ldots,x_n) & = & 0\ , \end{array}$$

the important parameters are the number of variables n and the degree d of the polynomials $f_1,\ldots,f_m$. The Buchberger algorithm for constructing Gröbner bases is at the same time a generalization of Euclid's algorithm for computing the greatest common divisor (GCD) of univariate polynomials (the case $n = 1$) and of Gauss' triangularization algorithm for linear systems (the case $d = 1$). Both these algorithms are concerned with solving systems of polynomial equations, and they determine a canonical basis (either the GCD of the inputs or a triangularized form of the system) for the given polynomial

[1] D.Hilbert, *Über die Theorie der algebraischen Formen*, Math. Annalen 36, 473–534 (1890)

[2] G.Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Annalen 95, 736–788 (1926)

[3] B.Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Dissertation, Univ. Innsbruck (1965)

system. Buchberger's algorithm can be seen as a generalization to the case of arbitrary n and d.

Definition 2.3.0. Let K be a field and $K[X] = K[x_1, \dots, x_n]$ the polynomial ring in n indeterminates over K. A subset I of $K[X]$ is a *(polynomial) ideal* of $K[X]$, iff it is closed under the formation of linear combinations; i.e., for $m \in \mathbb{N}$, $f_1, \dots, f_m \in I$ and $p_1, \dots, p_m \in K[X]$, also

$$\sum_{i=1}^{m} p_i f_i \ \in I \ .$$

If F is any subset of $K[X]$ we write $\langle F \rangle$ or ideal(F) for the ideal generated by F in $K[X]$.

$$\langle F \rangle \ = \ \{ \sum_{i=1}^{m} p_i f_i \mid m \in \mathbb{N},\ f_i \in F,\ p_i \in K[X]\}$$

i.e. $\langle F \rangle$ consists of all linear combinations (also the empty linear combination $0 = \sum_{i=1}^{0} p_i f_i$) of F over $K[X]$.
F is called a *basis* or *generating set* of $\langle F \rangle$.

By $[X]$ we denote the monoid (under multiplication) of *power products* $x_1^{i_1} \cdots x_n^{i_n}$ in $x_1, \dots, x_n$. $1 = x_1^0 \dots x_n^0$ is the unit element in the monoid $[X]$. $\mathrm{lcm}(s,t)$ denotes the least common multiple of the power products s, t. □

Definition 2.3.1.

(i) A commutative ring with 1 in which the *basis condition* holds, i.e. in which every ideal has a finite basis, is called a *Noetherian ring.*

(ii) Let $\succ$ be a binary relation of the set M; i.e. $\succ \subseteq M \times M$. $\succ$ is *Noetherian* or has the *termination property* iff there is no infinite sequence of the form $x_1 \succ x_2 \succ \cdots$.

□

Theorem 2.3.2.

(a) *In a Noetherian ring there are no infinite properly ascending chains of ideals; and vice versa.*

(b) (Hilbert's Basis Theorem) *If R is a Noetherian ring then also the univariate polynomial ring $R[x]$ is Noetherian.*

(c) *If K is a field, then $K[x_1, \dots, x_n]$ is a Noetherian ring.*

Proof: (a) Suppose that R is Noetherian. Let

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

be an ascending chain of ideals in R. Consider

$$I \ := \ \bigcup_{i=0}^{\infty} I_i \ .$$

I is an ideal in R, so it has a finite basis. This basis must be contained in some I_k; so

$$I_k = I_{k+1} = \cdots \ .$$

On the other hand, suppose that an ideal I in R does not have a finite basis.
Choose a non-zero element $r_0 \in I$; then $I_0 := \langle r_0 \rangle \neq I$.
Choose $r_1 \in I \setminus I_0$; then $I_1 := \langle r_0, r_1 \rangle \neq I$.
This process can be continued indefinitely, yielding an infinite properly ascending chain of ideals in R.

(b) This is typically proven in a course on commutative algebra and algebraic geometry.

(c) A field K has only 2 ideals: $\langle 0 \rangle$ and $\langle 1 \rangle$. Both of them are finitely generated. So, by a series of applications of (b) be get the desired result. $\square$

So every ideal I in $K[X]$ has a finite basis, and if we are able to effectively compute with finite bases then we are dealing with all the ideals in $K[X]$.

Whenever a set M is equipped with a Noetherian relation $\succ$ we can apply the **Principle of Noetherian Induction** [4] for proving that a predicate P holds for all $x \in M$:
if for all $x \in M$

$$\big[\forall y \in M : (x \succ y) \Longrightarrow P(y)\big] \implies P(x)$$

then

$$\forall x \in M : P(x) \ .$$

Typical examples of Noetherian Induction are the induction on natural numbers $\mathbb{N}$ (with $\succ = >$) and induction on the term structure in term algebras (with $s \succ t \Longleftrightarrow t$ is a sub-term of s).

We will define a Gröbner basis of a polynomial ideal via a certain reduction relation for polynomials. A Gröbner basis will be a basis with respect to which the corresponding reduction relation is confluent. Before we can define the reduction relation on the polynomial ring, we have to introduce an ordering of the power products with respect to which the reduction relation should be decreasing.

Definition 2.3.3. Let $<$ be a strict ordering on $[X]$; i.e. $<$ is transitive and irreflexive. So $\leq$ is an ordering. We call $<$ an *admissible ordering*, if it is is compatible with the monoid structure of $[X]$; i.e.

(i) $1 = x_1^0 \dots x_n^0 < t$ for all $t \in [X] \setminus \{1\}$, and

(ii) $s < t \Longrightarrow su < tu$ for all $s, t, u \in [X]$. $\square$

Example 2.3.4. We give some examples of frequently used admissible orderings on $[X]$.

[4] see P.M. Cohn, *Algebra*, Wiley, New York (1974)

(a) The *lexicographic ordering* with $x_{\pi(1)} > x_{\pi(2)} > \ldots > x_{\pi(n)}$, π a permutation of $\{1, \ldots, n\}$:
$x_1^{i_1} \ldots x_n^{i_n} <_{lex,\pi} x_1^{j_1} \ldots x_n^{j_n}$ iff there exists a $k \in \{1, \ldots, n\}$ such that for all $l < k$ $i_{\pi(l)} = j_{\pi(l)}$ and $i_{\pi(k)} < j_{\pi(k)}$.
If $\pi = \text{id}$, we get the usual lexicographic ordering $<_{lex}$.

(b) The *graduated lexicographic ordering* w.r.t. the permutation π and the weight function $w : \{1, \ldots, n\} \to \mathbb{R}^+$:
for $s = x_1^{i_1} \ldots x_n^{i_n}, t = x_1^{j_1} \ldots x_n^{j_n}$ we define $s <_{glex,\pi,w} t$ iff

$$\Big(\sum_{k=1}^{n} w(k) i_k < \sum_{k=1}^{n} w(k) j_k\Big) \quad \text{or}$$

$$\Big(\sum_{k=1}^{n} w(k) i_k = \sum_{k=1}^{n} w(k) j_k \quad \text{and} \quad s <_{lex,\pi} t\Big).$$

We get the usual graduated lexicographic ordering $<_{glex}$ by setting $\pi = \text{id}$ and $w = 1_{const}$.

(c) The *graduated reverse lexicographic ordering*:
we define $s <_{grlex} t$ iff

$$\deg(s) < \deg(t) \quad \text{or}$$

$$(\deg(s) = \deg(t) \text{ and } t <_{lex,\pi} s, \text{ where } \pi(j) = n - j + 1).$$

(d) The *product ordering* w.r.t. $i \in \{1, \ldots, n-1\}$ and the admissible orderings $<_1$ on $X_1 = [x_1, \ldots, x_i]$ and $<_2$ on $X_2 = [x_{i+1}, \ldots, x_n]$:
for $s = s_1 s_2, t = t_1 t_2$, where $s_1, t_1 \in X_1, s_2, t_2 \in X_2$, we define $s <_{prod,i,<_1,<_2} t$ iff

$$s_1 <_1 t_1 \quad \text{or} \quad (s_1 = t_1 \text{ and } s_2 <_2 t_2). \qquad \square$$

Lemma 2.3.5. *Let $<$ be an admissible ordering on $[X]$.*

(i) If $s, t \in [X]$ and s divides t then $s \leq t$.

(ii) $<$ (or actually $>$) is Noetherian, i.e. there are no infinite chains of the form $t_0 > t_1 > t_2 > \ldots$, and consequently every subset of $[X]$ has a smallest element.

Proof:
(i) For some u we have $su = t$. By admissibility of $<$ this yields $s = 1s \leq us = t$.
(ii) Let $s_1 > s_2 > \cdots$ be a sequence of decreasing elements in $[X]$. Let K be any field. So

$$\langle s_1 \rangle \subset \langle s_1, s_2 \rangle \subset \cdots$$

is a properly ascending chain of ideals in $K[X]$. But $K[X]$ being Noetherian, this chain has to be finite $\square$

Throughout this chapter let R be a commutative ring with 1, K a field, X a set of variables, and $<$ an admissible ordering on $[X]$.

Definition 2.3.6. Let s be a power product in $[X]$, f a non-zero polynomial in $R[X]$, F a subset of $R[X]$.
By $\mathrm{coeff}(f, s)$ we denote the coefficient of s in f.
$\mathrm{lpp}(f) := \max_{<}\{t \in [X] \mid \mathrm{coeff}(f, t) \neq 0\}$ (*leading power product* of f),
$\mathrm{lc}(f) := \mathrm{coeff}(f, \mathrm{lpp}(f))$ (*leading coefficient* of f),
$\mathrm{initial}(f) := \mathrm{lc}(f)\mathrm{lpp}(f)$ (*initial* of f),
$\mathrm{red}(f) := f - \mathrm{initial}(f)$ (*reductum* of f),
$\mathrm{lpp}(F) := \{\mathrm{lpp}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{lc}(F) := \{\mathrm{lc}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{initial}(F) := \{\mathrm{initial}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{red}(F) := \{\mathrm{red}(f) \mid f \in F \setminus \{0\}\}$. □

If I is an ideal in $R[X]$, then $\mathrm{lc}(I) \cup \{0\}$ is an ideal in R. However, $\mathrm{initial}(I) \cup \{0\}$ in general is not an ideal in $R[X]$.

Definition 2.3.7. Any admissible ordering $<$ on $[X]$ induces a strict partial ordering $\ll$ on $R[X]$, the *induced ordering*, in the following way:

$$\begin{array}{lll} f \ll g & \text{iff} & f = 0 \text{ and } g \neq 0 \text{ or} \\ & & f \neq 0, g \neq 0 \text{ and } \mathrm{lpp}(f) < \mathrm{lpp}(g) \text{ or} \\ & & f \neq 0, g \neq 0, \mathrm{lpp(f)}=\mathrm{lpp(g)} \text{ and } \mathrm{red}(f) \ll \mathrm{red}(g). \end{array}$$ □

One of the central notions of the theory of Gröbner bases is the concept of polynomial reduction.

Definition 2.3.8. Let $f, g, h \in K[X]$, $F \subseteq K[X]$. We say that *g reduces to h w.r.t. f* ($g \longrightarrow_f h$) iff there are power products $s, t \in [X]$ such that s has a non–vanishing coefficient c in g ($\mathrm{coeff}(g, s) = c \neq 0$), $s = \mathrm{lpp}(f) \cdot t$, and

$$h = g - \frac{c}{\mathrm{lc}(f)} \cdot t \cdot f.$$

If we want to indicate which power product and coefficient are used in the reduction, we write

$$g \longrightarrow_{f,b,t} h, \qquad \text{where } b = \frac{c}{lc(f)}.$$

We say that *g reduces to h w.r.t. F* ($g \longrightarrow_F h$) iff there is $f \in F$ such that $g \longrightarrow_f h$. □

Example 2.3.9. Let $F = \{\ldots, f = x_1x_3 + x_1x_2 - 2x_3, \ldots\}$ in $\mathbb{Q}[x_1, x_2, x_3]$, and $g = x_3^3 + 2x_1x_2x_3 + 2x_2 - 1$. Let $<$ be the graduated lexicographic ordering with $x_1 < x_2 < x_3$. Then $g \longrightarrow_F x_3^3 - 2x_1x_2^2 + 4x_2x_3 + 2x_2 - 1 =: h$, and in fact $g \longrightarrow_{f,2,x_2} h$. □

Lemma 2.3.10. *For a given admissible ordering $<$ on $[X]$ and a subset F of $K[X]$ let $\ll$ be the induced ordering on $K[X]$ and $\longrightarrow_F$ the reduction w.r.t. F.*

(i) $\ll$ (or actually $\gg$) is a Noetherian strict partial ordering on $K[X]$.

(ii) $\longrightarrow_F$ is a Noetherian strict partial ordering on $K[X]$.

Proof: (i) We have to show that every sequence $f_1 \gg f_2 \gg \ldots$ is finite. This is achieved by Noetherian induction on $\text{lpp}(f_1)$ w.r.t. $>$.
Noetherian induction on $\text{lpp}(h)$ w.r.t. $>$:
Induction hypothesis:

$$\forall s \ : \ t > s \implies \text{sequence } g_1 \gg g_2 \gg \cdots \text{ with } \text{lpp}(g_1) = s \text{ is finite.}$$

show: sequence $h_1 \gg h_2 \gg \cdots$ with $\text{lpp}(h_1) = t$ is finite.
Let $t_i := \text{lpp}(h_i)$ (if some $h_i = 0$, then the sequence is obviously finite). Then we have $t = t_1 \geq t_2 \geq \cdots$. If all t_i are equal, then we have (by definition of $\ll$)

$$\text{red}(h_1) \gg \text{red}(h_2) \gg \cdots$$

and this must be finite by the induction hypothesis. Otherwise let j be such that $t > t_j$. Then

$$h_j \gg h_{j+1} \gg \cdots$$

is finite by the induction hypothesis. So the original sequence is also finite.
(ii) $\longrightarrow_F$ is a partial ordering on $K[X]$, which is contained in $\gg$. □

Definition 2.3.11. Let $\longrightarrow$ be a reduction relation, i.e. a binary relation, on a set M.

- $x \longrightarrow$ means x is *reducible*, i.e. $x \longrightarrow y$ for some y;
- $\underline{x}_{\longrightarrow}$ means x is *irreducible* or *in normal form* w.r.t. $\longrightarrow$. We omit mentioning the reduction relation if it is clear from the context;
- $x \downarrow y$ means that x and y have a *common successor*, i.e. $x \longrightarrow z \longleftarrow y$ for some z;
- $x \uparrow y$ means that x and y have a *common predecessor*, i.e. $x \longleftarrow z \longrightarrow y$ for some z;
- by $\longleftarrow$ we mean the inverse relation, by $\longleftrightarrow$ the symmetric closure, and by $\longrightarrow^*$ the reflexive-transitive closure; so, $\longleftrightarrow^*$ is the symmetric-reflexive-transitive closure of $\longrightarrow$;
- x *is a* $\longrightarrow$*-normal form* of y iff $y \longrightarrow^* \underline{x}$. □

Definition 2.3.12. A reduction relation can have the following important properties.

(a) $\longrightarrow$ is *Church–Rosser* or has the *Church–Rosser property* iff $a \longleftrightarrow^* b$ implies $a \downarrow_* b$.

(b) $\longrightarrow$ is *confluent* iff $x \uparrow^* y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:

$$\begin{tikzcd} & u \arrow[dl, "*"'] \arrow[dr, "*"] & \\ x \arrow[dr, "*"'] & & y \arrow[dl, "*"] \\ & v & \end{tikzcd}$$

(c) $\longrightarrow$ is *locally confluent* iff $x \uparrow y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:

$$\begin{tikzcd}
 & u \arrow[dl] \arrow[dr] & \\
x \arrow[dr, "*"'] & & y \arrow[dl, "*"] \\
 & v &
\end{tikzcd}$$

□

As a consequence of the Noetherianity of admissible orderings we get that $\longrightarrow_F$ is Noetherian for any set of polynomials $F \subset K[X]$. So, in contrast to the general theory of rewriting, termination is not a problem for polynomial reductions. But we still have to worry about the Church-Rosser property.

Theorem 2.3.13. *These crucial properties of reduction relations are closely related.*

(a) $\longrightarrow$ *is Church–Rosser if and only if* $\longrightarrow$ *is confluent.*

(b) (Newman Lemma) *Let* $\longrightarrow$ *be Noetherian. Then* $\longrightarrow$ *is confluent if and only if* $\longrightarrow$ *is locally confluent.*

(c) (Refined Newman Lemma) *Let* $\longrightarrow$ *be a reduction on* M *and* $<$ *a partial Noetherian ordering on* M *s.t.* $\longrightarrow \subseteq >$. *Then* $\longrightarrow$ *is confluent if and only if for all* $x, y, z \in M$*:*

$$x \longleftarrow z \longrightarrow y \quad \text{implies} \quad x \longleftrightarrow^*_{(<z)} y$$

i.e. all intermediate elements w *in the chain* $x \longleftrightarrow^* y$ *satisfy* $w < z$. *In this case we say* x *and* y *are connected w.r.t.* $\longrightarrow$ *below* z.

Proof: For (a) and (b) see Theorem 8.1.2 in [Winkler 1996].
For (c) see Theorem 8.1.3 in [Winkler 1996]. □

As an immediate consequence of the previous definitions we get that the reduction relation $\longrightarrow$ is (nearly) compatible with the operations in the polynomial ring. Moreover, the reflexive–transitive–symmetric closure of the reduction relation $\longrightarrow_F$ is equal to the congruence modulo the ideal generated by F.

Lemma 2.3.14. *Let* $a \in K^*$, $s \in [X]$, $F \subseteq K[X]$, $g_1, g_2, h \in K[X]$.

(a) $\longrightarrow_F \subseteq \gg$,

(b) $\longrightarrow_F$ *is Noetherian,*

(c) if $g_1 \longrightarrow_F g_2$ *then* $a \cdot s \cdot g_1 \longrightarrow_F a \cdot s \cdot g_2$,

(d) if $g_1 \longrightarrow_F g_2$ *then* $g_1 + h \downarrow^*_F g_2 + h$.

Proof: [Winkler 1996] Exercise 8.2(2).
(a), (b), (c) are obvious.
(d) Let s be the power product in g_1 that is reduced by $f \in F$, i.e. $s = u \cdot \mathrm{lpp}(f)$ for

some $u \in [X]$. If $\operatorname{coeff}(h,s) = 0$ then $g_1 + h \longrightarrow_f g_2 + h$. If $\operatorname{coeff}(h,s) = -\operatorname{coeff}(g_1,s)$ then $g_2 + h \longrightarrow_f g_1 + h$. Otherwise

$$g_1+h \;\longrightarrow_f\; g_1+h-\frac{\operatorname{coeff}(g_1+h,s)}{\operatorname{lc}(f)}\cdot u\cdot f \;=\; g_2+h-\frac{\operatorname{coeff}(g_2+h,s)}{\operatorname{lc}(f)}\cdot u\cdot f \;\longleftarrow_f\; g_2+h\;.$$

So in any case we have $g_1 + h \downarrow_F^* g_2 + h$. □

Theorem 2.3.15. *Let $F \subseteq K[X]$. The ideal congruence modulo $\langle F\rangle$ equals the reflexive–transitive–symmetric closure of $\longrightarrow_F$, i.e. $\equiv_{\langle F\rangle} = \longleftrightarrow_F^*$.*

Proof: [Winkler 1996] Exercise 8.2(3).
$\longleftrightarrow_F^*$ is the smallest equivalence relation containing $\longrightarrow_F$. If $g \longrightarrow_F h$ then, by the definition of the reduction relation, $g - h \in \langle F\rangle$, i.e. $g \equiv_{\langle F\rangle} h$. Because $\longrightarrow_F \subseteq \longleftrightarrow_F^*$ and $\equiv_{\langle F\rangle}$ is an equivalence relation we have $\longleftrightarrow_F^* \subseteq \equiv_{\langle F\rangle}$.
On the other hand, let $g \equiv_{\langle F\rangle} h$, i.e.

$$g \;=\; h + \sum_{j=1}^{m} c_j \cdot u_j \cdot f_j, \qquad \text{for } c_j \in K, u_j \in [X], f_j \in F.$$

If we can show $g \longleftrightarrow_F^* h$ for the case $m = 1$, then the statement follows by induction on m. $f_1 \longrightarrow_F 0$. So by Lemma 2.3.14 $g = h + c_1 \cdot u_1 \cdot f_1 \downarrow_F^* h$, and therefore $g \longleftrightarrow_F^* h$. □

So the congruence $\equiv_{\langle F\rangle}$ can be decided if $\longrightarrow_F$ has the Church–Rosser property. Of course, this is not the case for an arbitrary set F. Such distinguished sets (bases for polynomial ideals) are called Gröbner bases.

Definition 2.3.16. A subset F of $K[X]$ is a *Gröbner basis* (for $\langle F\rangle$) iff $\longrightarrow_F$ is Church–Rosser. □

A Gröbner basis of an ideal I in $K[X]$ is by no means uniquely defined. In fact, whenever F is a Gröbner basis for I and $f \in I$, then also $F \cup \{f\}$ is a Gröbner basis for I.

For testing whether a given basis F of an ideal I is a Gröbner basis it suffices to test for local confluence of the reduction relation $\longrightarrow_F$. This, however, does not yield a decision procedure, since there are infinitely many situations $f \uparrow_F g$. However, Buchberger has been able to reduce this test for local confluence to just testing a finite number of sitations $f \uparrow_F g$. For that purpose he has introduced the notion of subtraction polynomials, or S–polynomials for short.

Definition 2.3.17. Let $f, g \in K[X]^*$, $t = \operatorname{lcm}(\operatorname{lpp}(f), \operatorname{lpp}(g))$. Then

$$\operatorname{cp}(f,g) = \Big(t - \frac{1}{\operatorname{lc}(f)}\cdot\frac{t}{\operatorname{lpp}(f)}\cdot f,\; t - \frac{1}{\operatorname{lc}(g)}\cdot\frac{t}{\operatorname{lpp}(g)}\cdot g\Big)$$

is the *critical pair* of f and g. The difference of the elements of $\operatorname{cp}(f,g)$ is the *S–polynomial* $\operatorname{spol}(f,g)$ of f and g. □

If $\operatorname{cp}(f,g) = (h_1, h_2)$ then we can depict the situation graphically in the following way:

$$\begin{array}{ccc} & \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g)) & \\ & \bullet & \\ \swarrow_f & & \searrow_g \\ \bullet & & \bullet \\ h_1 & & h_2 \end{array}$$

The critical pairs of elements of F describe exactly the essential branchings of the reduction relation $\longrightarrow_F$.

Theorem 2.3.18. (Buchberger's Theorem) *Let F be a subset of $K[X]$.*

(a) F is a Gröbner basis if and only if $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2) of elements of F.

(b) F is a Gröbner basis if and only if $\mathrm{spol}(f, g) \longrightarrow_F^* 0$ for all $f, g \in F$.

Proof: (see also [Winkler 1996] Theorem 8.3.1)
(a) Obviously, if F is a Gröbner basis then $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2) of F.

On the other hand, assume that $g_1 \downarrow_F^* g_2$ for all critical pairs (g_1, g_2). By the Refined Newman Lemma (Theorem 2.3.13(c)) it suffices to show $h_1 \longleftrightarrow_{F(\ll h)}^* h_2$ for all h, h_1, h_2 such that $h_1 \longleftarrow_F h \longrightarrow_F h_2$.
Let s_1, s_2 be the power products that are eliminated in the reductions of h to h_1 and h_2, respectively. I.e. there are polynomials $f_1, f_2 \in F$, coefficients $c_1 = \mathrm{coeff}(h, s_1) \neq 0$, $c_2 = \mathrm{coeff}(h, s_2) \neq 0$, and power products t_1, t_2 such that

$$\begin{array}{lll} s_1 = t_1 \mathrm{lpp}(f_1), & h_1 = h - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 & \text{and} \\ s_2 = t_2 \mathrm{lpp}(f_2), & h_2 = h - \frac{c_2}{\mathrm{lc}(f_2)} t_2 f_2. & \end{array}$$

We distinguish two cases, depending on whether or not $s_1 = s_2$.
Case $s_1 \neq s_2$: w.l.o.g. assume $s_1 > s_2$. Let $a = \mathrm{coeff}(-\frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1, s_2)$. Then $\mathrm{coeff}(h_1, s_2) = c_2 + a$ and therefore ($\longrightarrow^*$ if coefficient is 0)

$$h_1 \ \longrightarrow_F^* \ h_1 - \frac{c_2 + a}{\mathrm{lc}(f_2)} t_2 f_2 \ = \ h - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 - \frac{c_2 + a}{\mathrm{lc}(f_2)} t_2 f_2.$$

On the other hand ($\longrightarrow^*$ if coefficient is 0)

$$h_2 \ \longrightarrow_F \ h_2 - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 \ \longrightarrow_F^* \ h_2 - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 - \frac{a}{\mathrm{lc}(f_2)} t_2 f_2 \ = \ h - \frac{c_1}{\mathrm{lc}(f_1)} t_1 f_1 - \frac{c_2 + a}{\mathrm{lc}(f_2)} t_2 f_2.$$

Thus, $h_1 \longleftrightarrow_{F(\ll h)}^* h_2$, in fact $h_1 \downarrow_F^* h_2$.
Case $s_1 = s_2$: let $s = s_1 = s_2$, $c = \mathrm{coeff}(h, s)$ and $h' = h - cs$. So for some power product t we have $s = t \cdot \mathrm{lcm}(\mathrm{lpp}(f_1), \mathrm{lpp}(f_2))$, and $h_1 = h' + c \cdot t \cdot g_1$, $h_2 = h' + c \cdot t \cdot g_2$, where $(g_1, g_2) = \mathrm{cp}(f_1, f_2)$. By assumption $g_1 \downarrow_F^* g_2$, i.e. there are $p_1, \ldots, p_k$ and $q_1, \ldots, q_l$ such that

$$g_1 = p_1 \longrightarrow_F \ldots \longrightarrow_F p_k = q_l \longleftarrow_F \ldots \longleftarrow_F q_1 = g_2.$$

So, by Lemma 2.3.14(c),

$$ctg_1 = ctp_1 \longrightarrow_F \ldots \longrightarrow_F ctp_k = ctq_l \longleftarrow_F \ldots \longleftarrow_F ctq_1 = ctg_2.$$

Applying Lemma 2.3.14(d) we get

$$h_1 = h' + ctp_1 \downarrow_F^* \ldots \downarrow_F^* h' + ctp_k = h' + ctq_l \downarrow_F^* \ldots \downarrow_F^* h' + ctq_1 = h_2.$$

All the intermediate polynomials in these reductions are less than h w.r.t. $\ll$. Thus, $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$.

(b) Every S–polynomial is congruent to 0 modulo $\langle F \rangle$. So by Theorem 2.3.15 $\mathrm{spol}(f,g) \longleftrightarrow_F^* 0$. If F is a Gröbner basis, this implies $\mathrm{spol}(f,g) \longrightarrow_F^* 0$.

On the other hand assume that $\mathrm{spol}(f,g) \longrightarrow_F^* 0$ for all $f, g \in F$. We use the same notation as in (a). In fact, the whole proof is analogous to the one for (a), except for the case $s_1 = s_2 = s$. So for $h_1 = h' + ctg_1 \longleftarrow_F h \longrightarrow_F h' + ctg_2 = h_2$ we have to show $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$.

$g_1 - g_2$ is the S–polynomial of $f_1, f_2 \in F$, so by the assumption $g_1 - g_2 \longrightarrow_F^* 0$. By Lemma 2.3.14 also $h_1 - h_2 = ct(g_1 - g_2) \longrightarrow_F^* 0$, i.e. for some $p_1, \ldots, p_k$ we have

$$h_1 - h_2 = p_1 \longrightarrow_F \ldots \longrightarrow_F p_k = 0.$$

Again by Lemma 2.3.14 we get

$$h_1 = p_1 + h_2 \downarrow_F^* \ldots \downarrow_F^* p_k + h_2 = h_2,$$

and therefore $h_1 \longleftrightarrow^*_{F(\ll h)} h_2$. □

Buchberger's theorem suggests an algorithm for checking whether a given finite basis is a Gröbner basis: reduce all the S–polynomials to normal forms and check whether they are all 0. In fact, by a simple extension we get an algorithm for constructing Gröbner bases.

GRÖBNER_B(Buchberger algorithm for computing Gröbner bases)
for a given finite subset F of $K[X]^*$ and admissible ordering $>$ on $[X]$,
a finite subset G of $K[X]^*$ is computed,
such that $\langle G \rangle = \langle F \rangle$ and G is a Gröbner basis w.r.t. $>$.
$G := F$
$C := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$
while not all pairs $\{g_1, g_2\} \in C$ are marked **do**
    choose an unmarked pair $\{g_1, g_2\}$
    mark $\{g_1, g_2\}$
    $h :=$ normal form of $\mathrm{spol}(g_1, g_2)$ w.r.t. $\longrightarrow_G$
    if $h \neq 0$ **then**
        $\{C := C \cup \{\{g, h\} \mid g \in G\}$
        $G := G \cup \{h\}$ }
return G □

Every polynomial h constructed in GRÖBNER_B is in $\langle F \rangle$, so $\langle G \rangle = \langle F \rangle$ throughout GRÖBNER_B. Thus, by Theorem 1.8 GRÖBNER_B yields a correct result if it stops. The termination of GRÖBNER_B is a consequence of Dickson's Lemma which implies that in

$[X]$ there is no infinite chain of elements $s_1, s_2, \ldots$ such that $s_i \not| s_j$ for all $1 \leq i < j$. The leading power products of the polynomials added to the basis form such a sequence in $[X]$, so this sequence must be finite.

Theorem 2.3.19. (Dickson's Lemma) *Every $A \subseteq [X]$ contains a finite subset B, such that every $t \in A$ is a multiple of some $s \in B$.*

Proof: [Winkler 1996] 8.3.2. □

The termination of GRÖBNER_B also follows from Hilbert's Basis Theorem applied to the initial ideals of the sets G constructed in the course of the algorithm, i.e. $\langle \text{initial}(G) \rangle$.

The algorithm GRÖBNER_B provides a constructive proof of the following theorem.

Theorem 2.3.20. *Every ideal I in $K[X]$ has a finite Gröbner basis.* □

Example 2.3.21. Let $F = \{f_1, f_2\}$, with $f_1 = x^2y^2 + y - 1$, $f_2 = x^2y + x$. We compute a Gröbner basis of $\langle F \rangle$ in $\mathbb{Q}[x, y]$ w.r.t. the graduated lexicographic ordering with $x < y$. The following describes one way in which the algorithm GRÖBNER_B could execute (recall that there is a free choice of pairs in the loop):

$$\text{spol}(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3 \text{ is irreducible, so } G := \{f_1, f_2, f_3\};$$

$$\text{spol}(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4, \text{ so } G := \{f_1, f_2, f_3, f_4\};$$

$$\text{spol}(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5, \text{ so } G := \{f_1, \ldots, f_5\}.$$

All the other S–polynomials now reduce to 0, so GRÖBNER_B terminates with

$$G = \{x^2y^2 + y - 1, x^2y + x, -xy + y - 1, y - 1, -x\}.$$ □

In addition to the original definition and the ones given in Theorem 2.3.18, there are many other characterizations of Gröbner bases. We list only a few of them.

Theorem 2.3.22. *Let I be an ideal in $K[X]$, $F \subseteq K[X]$, and $\langle F \rangle = I$. Then the following are equivalent.*

(a) F *is a Gröbner basis for* I *(w.r.t.* $>$*).*

(b) $f \longrightarrow_F^* 0$ *for every* $f \in I$*.*

(c) $f \longrightarrow_F$ *for every* $f \in I \setminus \{0\}$*.*

(d) For all $g \in I, h \in K[X]$*: if* $g \longrightarrow_F^* \underline{h}$ *then* $h = 0$*.*

(e) For all $g, h_1, h_2 \in K[X]$*: if* $g \longrightarrow_F^* \underline{h_1}$ and $g \longrightarrow_F^* \underline{h_2}$ *then* $h_1 = h_2$*.*

(f) $\langle \text{initial}(F) \rangle = \langle \text{initial}(I) \rangle$*.*

(g) Every $h \in I$ *can be written as a bounded linear combination of elements in* F*; i.e. there are* $f_i \in F$, $h_i \in K[X]$, *s.t.* $h = \sum_{i=1}^n h_i f_i$ *with* $\text{lpp}(h_i f_i) \leq \text{lpp}(h)$ *for all* i*.*

Proof: For the equivalence of (a) – (f) see [Winkler 1996] Theorem 8.3.4.
Now for (g): If F is a Gröbner basis w.r.t $>$, then every $h \in I$ can be reduced to 0 modulo F; this leads to a bounded linear combination of elements of F representing h. On the other hand, if every $h \in I$ is a bounded linear combination, then there cannot be cancellation of highest power products in such a linear combination; so every $h \in I$ can be reduced modulo F; this is obviously equivalent to (c). □

The Gröbner basis G computed in Example 2.3.21 is much too complicated. In fact, $\{y-1, x\}$ is a Gröbner basis for the ideal. There is a general procedure for simplifying Gröbner bases.

Theorem 2.3.23. *Let G be a Gröbner basis for an ideal I in $K[X]$. Let $g, h \in G$ and $g \neq h$.*

(a) If $\mathrm{lpp}(g) \mid \mathrm{lpp}(h)$ then $G' = G \setminus \{h\}$ is also a Gröbner basis for I.

(b) If $h \longrightarrow_g h'$ then $G' = (G \setminus \{h\}) \cup \{h'\}$ is also a Gröbner basis for I.

Proof: [Winkler 1996] Theorem 8.3.5. □

Observe that the elimination of basis polynomials described in Theorem 2.3.23(a) is only possible if G is a Gröbner basis. In particular, we are not allowed to do this during a Gröbner basis computation. Based on Theorem 2.3.23 we can show that every ideal has a unique Gröbner basis after suitable pruning and normalization.

Definition 2.3.24. Let G be a Gröbner basis in $K[X]$.
G is *minimal* iff $\mathrm{lpp}(g) \nmid \mathrm{lpp}(h)$ for all $g, h \in G$ with $g \neq h$.
G is *reduced* iff for all $g, h \in G$ with $g \neq h$ we cannot reduce h by g.
G is *normed* iff $\mathrm{lc}(g) = 1$ for all $g \in G$. □

From Theorem 2.3.23 we obviously get an algorithm for transforming any Gröbner basis for an ideal I into a normed reduced Gröbner basis for I. No matter from which Gröbner basis of I we start and which path we take in this transformation process, we always reach the same uniquely defined normed reduced Gröbner basis of I.

Theorem 2.3.25. *Every ideal in $K[X]$ has a unique finite normed reduced Gröbner basis.*

Proof: [Winkler 1996] Theorem 8.3.6. □

Observe that the normed reduced Gröbner basis of an ideal I depends, of course, on the admissible ordering $<$. Different orderings can give rise to different Gröbner bases. However, if we decompose the set of all admissible orderings into sets which induce the same normed reduced Gröbner basis of a fixed ideal I, then this decomposition is finite. This leads to the consideration of universal Gröbner bases. A universal Gröbner basis for I is a basis for I which is a Gröbner basis w.r.t. any admissible ordering of the power products.

If we have a Gröbner basis G for an ideal I, then we can compute in the vector space $K[X]_{/I}$ over K. The irreducible power products (with coefficient 1) modulo G form a basis of $K[X]_{/I}$. We get that $\dim(K[X]_{/I})$ is the number of irreducible power products modulo G. Thus, this number is independent of the particular admissible ordering.

Example 2.3.26. Let $I = \langle x^3y - 2y^2 - 1, x^2y^2 + x + y\rangle$ in $\mathbb{Q}[x, y]$. Let $<$ be the graduated lexicographic ordering with $x > y$. Then the normed reduced Gröbner basis of I has leading power products x^4, x^3y, x^2y^2, y^3. So there are 9 irreducible power products.

If $<$ is the lexicographic ordering with $x > y$, then the normed reduced Gröbner basis of I has leading power products x and y^9. So again there are 9 irreducible power products.

In fact, $\dim(\mathbb{Q}[x, y]_{/I}) = 9$. □

An inconstructive proof of the existence of Gröbner bases

The existence of a Gröbner basis for any given ideal I (in $K[x_1, \ldots, x_n]$) and admissible ordering $<$ can be proven without introducing reduction and S-polynomials. In the following we give an outline of such an inconstructive proof.

Definition 2.3.27. An ideal I in $K[x_1, \ldots, x_n]$ is a *monomial ideal* iff it has a monomial basis, i.e. a basis B s.t. every $f \in B$ is a monomial $ax_1^{j_1} \cdots x_n^{j_n}$, $a \in K$. □

Theorem 2.3.28. *Let I be an ideal in $K[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) *I is a monomial ideal.*

(ii) *If $f \in I$ and m is a monomial occurring in f, then $m \in I$.*

(iii) *I is generated by a finite monomial basis.*

Proof: (i) $\Longrightarrow$ (ii): By definition, for every $f \in I$ there exist finitely many monomials $m_1, \ldots, m_r$ in a monomial basis B such that

$$f = h_1m_1 + \cdots + h_rm_r$$

for some $h_1, \ldots, h_r \in K[x_1, \ldots, x_n]$. Hence, every monomial in f is divisible by one of the m_i and therefore in I.
(ii) $\Longrightarrow$ (iii): By Hilbert's Basis Theorem (Theorem 2.3.2(c)) the ideal I has a finite basis B'. Then the set

$$B := \{\ m \mid m \text{ occurs in some } f \in B'\ \}$$

is a finite monomial basis of I.
(iii) $\Longrightarrow$ (i): Trivial. □

We could have defined Gröbner bases in the following alternative way:

Definition 2.3.29. Let F be a basis of the ideal I. Then F is an *initial Gröbner basis* for I iff $\langle \text{initial}(F)\rangle = \langle \text{initial}(I)\rangle$. □

Theorem 2.3.22 implies that

$$F \text{ is a Gröbner basis for } I \quad \Longleftrightarrow \quad F \text{ is an initial Gröbner basis for } I.$$

Now we can prove the existence of (initial) Gröbner bases in the following way:

Theorem 2.3.30. *Every ideal I has a finite initial Gröbner basis.*

Proof: Let G be a finite monomial basis for $\langle \text{initial}(I) \rangle$; which exists because of Theorem 2.3.28(c).
For every $g \in G$ let f_g be in I s.t. $f_g = c \cdot g + \text{red}(f_g)$, for a constant $c \in K$.
Let $F := \{f_g \mid g \in G\}$.
Then clearly $\langle \text{initial}(F) \rangle = \langle \text{initial}(I) \rangle$.
Furthermore, F is a basis for I: for an arbitrary $f \in I$ there must be a $g \in G$ s.t. $g \mid \text{lpp}(f)$. So, by subtracting a suitable multiple of f_g from f, we generate $h = f - c \cdot f_g$ s.t. $h \in I$ and $\text{lpp}(h) < \text{lpp}(f)$. This process terminates because of the Noetherianity of $<$, leading to a representation of f as a linear combination of the polynomials in F. □