Chapter 2

Gröbner bases

2.1 Existence and construction of Gröbner bases

The material of this chapter is largely taken from [Win96], where also proofs of theorems are given.

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 D. Hilbert 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, 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 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 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, the important parameters are the number of variables n and the degree of the polynomials d. 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 system. Buchberger's algorithm can be seen as a generalization to the case of arbitrary n and d.

Let K be a computable field and $K[X] = K[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates over K. If F is any subset of $K[X]$ we write $\langle F \rangle$ or ideal(F) for the ideal generated by F in $K[X]$. By $[X]$ we denote the monoid (under multiplication) of *power products* $x_1^{i_1} \cdots x_n^{i_n}$ in $x_1, \ldots, x_n$. $1 = x_1^0 \ldots x_n^0$ is the unit element in the monoid $[X]$. $\mathrm{lcm}(s,t)$ denotes the least common multiple of the power products s, t.

Commutative rings with 1 in which the *basis condition* holds, i.e. in which every ideal has a finite basis, are usually called *Noetherian rings*. This notation is motivated by the following lemma.

Lemma 2.1.1. *In a Noetherian ring there are no infinitely ascending chains of ideals.* □

Theorem 2.1.2. (Hilbert's Basis Theorem) *If R is a Noetherian ring then also the univariate polynomial ring $R[x]$ is Noetherian.*

A proof of Hilbert's Basis Theorem will be given in a later chapter. Hilbert's Basis Theorem implies that the multivariate polynomial ring $K[X]$ is Noetherian, if K is a field. 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 $K[X]$.

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 2.1.1. Let $<$ be an ordering on $[X]$ that is compatible with the monoid structure, i.e.
(i) $1 = x_1^0 \ldots x_n^0 < t$ for all $t \in [X] \setminus \{1\}$, and
(ii) $s < t \Longrightarrow su < tu$ for all $s, t, u \in [X]$.
We call such an ordering $<$ on $[X]$ an *admissible ordering*. □

Example 2.1.1. We give some examples of frequently used admissible orderings on $[X]$.

(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 $\pi = \mathrm{id}$, 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

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

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

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

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

(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

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

A complete classification of admissible orderings is given by L. Robbiano in 1985.

Lemma 2.1.3. *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.

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 2.1.2. 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),
$\mathrm{in}(f) := \mathrm{lc}(f)\mathrm{lpp}(f)$ (*initial* of f),
$\mathrm{red}(f) := f - \mathrm{in}(f)$ (*reductum* of f),
$\mathrm{lpp}(F) := \{\mathrm{lpp}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{lc}(F) := \{\mathrm{lc}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{in}(F) := \{\mathrm{in}(f) \mid f \in F \setminus \{0\}\}$,
$\mathrm{red}(F) := \{\mathrm{red}(f) \mid f \in F \setminus \{0\}\}$. $\square$

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

Definition 2.1.3. Any admissible ordering $<$ on $[X]$ induces a partial ordering $\ll$ on $R[X]$, the *induced ordering*, in the following way:
$f \ll g$ iff $f = 0$ and $g \neq 0$ or
$f \neq 0$, $g \neq 0$ and $\mathrm{lpp}(f) < \mathrm{lpp}(g)$ or
$f \neq 0$, $g \neq 0$, $\mathrm{lpp}(f) = \mathrm{lpp}(g)$ and $\mathrm{red}(f) \ll \mathrm{red}(g)$. $\square$

Lemma 2.1.4. *$\ll$ (or actually $\gg$) is a Noetherian partial ordering on $R[X]$.* $\square$

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

Definition 2.1.4. 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 $g \longrightarrow_f h$. $\square$

Example 2.1.2. 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 $g \longrightarrow_{f,2,x_2} h$. $\square$

Definition 2.1.5. Let $\longrightarrow$ be a reduction relation, i.e. a binary relation, on a set X.

- $x \longrightarrow$ 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;
- x *is a* $\longrightarrow$*-normal form* of y iff $y \longrightarrow^* \underline{x}$. $\square$

Definition 2.1.6. (a) $\longrightarrow$ is *Noetherian* or has the *termination property* iff every reduction sequence terminates, i.e. there is no infinite sequence $x_1, x_2, \ldots$ in M such that $x_1 \longrightarrow x_2 \longrightarrow \ldots$.
(b) $\longrightarrow$ is *Church–Rosser* or has the *Church–Rosser property* iff $a \longleftrightarrow^* b$ implies $a \downarrow_* b$.
(c) $\longrightarrow$ is *confluent* iff $x \uparrow^* y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:

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

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

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

$\square$

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 2.1.5. (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.

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 2.1.6. *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* $g_1 + h \downarrow_F^* g_2 + h$. ☐

Theorem 2.1.7. *Let $F \subseteq K[X]$. The ideal congruence modulo $\langle F \rangle$ equals the reflexive–transitive–symmetric closure of $\longrightarrow_F$, i.e. $\equiv_{\langle F \rangle} = \longleftrightarrow_F^*$.* ☐

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 2.1.5. 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 $f \uparrow_F g$ [Buchberger 1965]. For that purpose he has introduced the notion of subtraction polynomials, or S–polynomials for short.

Definition 2.1.8. Let $f, g \in K[X]^*$, $t = \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$. Then

$$\mathrm{cp}(f,g) = \left(t - \frac{1}{\mathrm{lc}(f)} \cdot \frac{t}{\mathrm{lpp}(f)} \cdot f,\ t - \frac{1}{\mathrm{lc}(g)} \cdot \frac{t}{\mathrm{lpp}(g)} \cdot g\right)$$

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

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

$$\begin{tikzcd} & \underset{\bullet}{\mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))} \arrow[dl, "f"'] \arrow[dr, "g"] & \\ \overset{\bullet}{h_1} & & \overset{\bullet}{h_2} \end{tikzcd}$$

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

Theorem 2.1.8. (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 $f, g \in F$.*

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.

---

algorithm GRÖBNER_B(**in:** F; **out:** G);
[Buchberger algorithm for computing a Gröbner basis. F is a finite subset of $K[X]^*$; G is a finite subset of $K[X]^*$, such that $\langle G \rangle = \langle F \rangle$ and G is a Gröbner basis.]
(1) $G := F$;
    $C := \{\{g_1, g_2\} \mid g_1, g_2 \in G, g_1 \neq g_2\}$;
(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 □

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

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. $\langle \mathrm{in}(G) \rangle$. See Exercise 8.3.4.

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

Theorem 2.1.10. *Every ideal I in $K[X]$ has a Gröbner basis.* □

Example 2.1.3. 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):
(1) $\mathrm{spol}(f_1, f_2) = f_1 - yf_2 = -xy + y - 1 =: f_3$ is irreducible, so $G := \{f_1, f_2, f_3\}$.
(2) $\mathrm{spol}(f_2, f_3) = f_2 + xf_3 = xy \longrightarrow_{f_3} y - 1 =: f_4$, so $G := \{f_1, f_2, f_3, f_4\}$.
(3) $\mathrm{spol}(f_3, f_4) = f_3 + xf_4 = y - x - 1 \longrightarrow_{f_4} -x =: f_5$, so $G := \{f_1, \ldots, f_5\}$.
All the other S–polynomials now reduce to 0, so GRÖBNER_B terminates with

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

In addition to the original definition and the ones given in Theorem 1.8, there are many other characterizations of Gröbner bases. We list only a few of them.

Theorem 2.1.11. *Let I be an ideal in $K[X]$, $F \subseteq K[X]$, and $\langle F \rangle \subseteq I$. Then the following are equivalent.*
(a) F is a Gröbner basis for I.
(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) $\langle \mathrm{in}(F) \rangle = \langle \mathrm{in}(I) \rangle$.

The Gröbner basis G computed in Example 2.1.3 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 2.1.12. *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.

Observe that the elimination of basis polynomials described in Theorem 2.1.12(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 2.1.12 we can show that every ideal has a unique Gröbner basis after suitable pruning and normalization.

Definition 2.1.9. 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 $g \in G$. $\square$

From Theorem 2.1.12 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 2.1.13. *Every ideal in $K[X]$ has a unique finite normed reduced Gröbner basis.*

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

For a 0–dimensional ideal I in regular position a very strong structure theorem has been derived by Gianni and Mora. I is in *regular position* w.r.t. the variable x_1, if $a_1 \neq b_1$ for any two different zeros $(a_1, \ldots, a_n), (b_1, \ldots, b_n)$ of I. Clearly it is very likely that an arbitrary 0–dimensional ideal is in regular position w.r.t. x_1. Otherwise, nearly every linear change of coordinates will make the ideal regular.

Theorem 2.1.14. (Shape Lemma) *Let I be a radical 0–dimensional ideal in $K[X]$, regular in x_1. Then there are $g_1(x_1), \ldots, g_n(x_1) \in K[x_1]$ such that g_1 is squarefree, $\deg(g_i) < \deg(g_1)$ for $i > 1$ and the normed reduced Gröbner basis F for I w.r.t. the lexicographic ordering $<$ with $x_1 < \cdots < x_n$ is of the form*

$$\{g_1(x_1), x_2 - g_2(x_1), \ldots, x_n - g_n(x_1)\}.$$

On the other hand, if the normed reduced Gröbner basis for I w.r.t. $<$ is of this form, then I is a radical 0–dimensional ideal.

Proof: Since I is in regular position, the first coordinates of zeros of I are all different, say $a_{11}, \ldots, a_{1m}$. Then the squarefree polynomial $g_1(x_1) = \prod_{i=1}^{m}(x_1 - a_{1i})$ is in $I \cap K[x_1]$ and so it has to be in F. Since by the observation above m is the dimension of $K[X]_{/I}$, the normed reduced Gröbner basis for I has to have the specified form.

To prove the converse, let $a_{11}, \ldots, a_{1m}$ be the zeros of $g_1(x_1)$. Then the zeros of I are $\{(a_{1i}, g_2(a_{1i}), \ldots, g_n(a_{1i}) \mid i = 1, \ldots, m\}$. □

2.2 Solving ideal theoretic problems by Gröbner bases

Computation in the vector space of polynomials modulo an ideal

The ring $K[X]_{/I}$ of polynomials modulo the ideal I is a vector space over K. A Gröbner basis G provides a basis for this vector space.

Theorem 2.2.1. *The irreducible power products modulo G, viewed as polynomials with coefficient 1, form a basis for the vector space $K[X]_{/I}$ over K.*

Ideal membership

By definition Gröbner bases solve the *ideal membership problem* for polynomial ideals, i.e.

given: $f, f_1, \ldots, f_m \in K[X]$,
decide: $f \in \langle f_1, \ldots, f_m \rangle$.

Let G be a Gröbner basis for $I = \langle f_1, \ldots, f_m \rangle$. Then $f \in I$ if and only if the normal form of f modulo G is 0.

Example 2.2.1. Suppose that we know the polynomial relations (axioms)

$$\begin{aligned} 4z - 4xy^2 - 16x^2 - 1 &= 0, \\ 2y^2 z + 4x + 1 &= 0, \\ 2x^2 z + 2y^2 + x &= 0 \end{aligned}$$

between the quantities x, y, z, and we want to decide whether the additional relation (hypothesis)

$$g(x, y) = 4xy^4 + 16x^2y^2 + y^2 + 8x + 2 = 0$$

follows from them, i.e. whether we can write g as a linear combination of the axioms or, in other words, whether g is in the ideal I generated by the axioms.

Trying to reduce the hypothesis g w.r.t. the given axioms does not result in a reduction to 0. But we can compute a Gröbner basis for I w.r.t. the lexicographic ordering with $x < y < z$, e.g. $G = \{g_1, g_2, g_3\}$ where

$$\begin{aligned} g_1 &= 32x^7 - 216x^6 + 34x^4 - 12x^3 - x^2 + 30x + 8, \\ g_2 &= 2745y^2 - 112x^6 - 812x^5 + 10592x^4 - 61x^3 - 812x^2 + 988x + 2, \\ g_3 &= 4z - 4xy^2 - 16x^2 - 1. \end{aligned}$$

Now $g \longrightarrow_G^* 0$, i.e. $g(x, y) = 0$ follows from the axioms. □

Radical membership

Sometimes, especially in applications in geometry, we are not so much interested in the ideal membership problem but in the *radical membership problem*, i.e.

given: $f, f_1, \ldots, f_m \in K[X]$,
decide: $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$.

The radical of an ideal I is the ideal containing all those polynomials f, some power of which is contained in I. So $f \in \text{radical}(I) \iff f^n \in I$ for some $n \in \mathbb{N}$. Geometrically $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$ means that the hypersurface defined by f contains all the points in the variety (algebraic set) defined by $f_1, \ldots, f_m$.

The following extremely important theorem relates the radical of an ideal I to the set of common roots $V(I)$ of the polynomials contained in I. We will give a proof of this theorem later.

Theorem 2.2.2. (Hilbert's Nullstellensatz) *Let I be an ideal in $K[X]$, where K is an algebraically closed field. Then* $\text{radical}(I)$ *consists of exactly those polynomials in $K[X]$ which vanish on all the common roots of I.*

By an application of Hilbert's Nullstellensatz we get that $f \in \text{radical}(\langle f_1, \ldots, f_m \rangle)$ if and only if f vanishes at every common root of $f_1, \ldots, f_m$ if and only if the system $f_1 = \ldots f_m = z \cdot f - 1 = 0$ has no solution, where z is a new variable. I.e.

$$f \in \text{radical}(\langle f_1, \ldots, f_m \rangle) \iff 1 \in \langle f_1, \ldots, f_m, z \cdot f - 1 \rangle.$$

So the radical membership problem is reduced to the ideal membership problem.

Equality of ideals

We want to decide whether two given ideals are equal, i.e. we want to solve the *ideal equality problem*:

given: $f_1, \ldots, f_m, g_1, \ldots, g_k \in K[X]$,
decide: $\underbrace{\langle f_1, \ldots, f_m \rangle}_{I} = \underbrace{\langle g_1, \ldots, g_k \rangle}_{J}$.

Choose any admissible ordering. Let G_I, G_J be the normed reduced Gröbner bases of I and J, respectively. Then by Theorem 2.1.13 $I = J$ if and only if $G_I = G_J$.

Solution of algebraic equations by Gröbner bases

We consider a system of equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0, \end{aligned} \tag{2.1}$$

where $f_1, \ldots, f_m \in K[X]$. The system (2.1) is called a system of polynomial or algebraic equations. First let us decide whether (2.1) has any solutions in $\overline{K}^n$, $\overline{K}$ being the algebraic closure of K. Let $I = \langle f_1, \ldots, f_m \rangle$.

Theorem 2.2.3 *Let G be a normed Gröbner basis of I. (2.1) is unsolvable in $\overline{K}^n$ if and only if $1 \in G$.*

Now suppose that (2.1) is solvable. We want to determine whether there are finitely or infinitely many solutions of (2.1) or, in other words, whether or not the ideal I is 0–dimensional.

Theorem 2.2.4. *Let G be a Gröbner basis of I. Then (2.1) has finitely many solutions (i.e. I is 0–dimensional) if and only if for every i, $1 \le i \le n$, there is a polynomial $g_i \in G$ such that $\mathrm{lpp}(g_i)$ is a pure power of x_i. Moreover, if I is 0–dimensional then the number of zeros of I (counted with multiplicity) is equal to $\dim(K[X]_{/I})$.*

The rôle of the Gröbner basis algorithm GRÖBNER_B in solving systems of algebraic equations is the same as that of Gaussian elimination in solving systems of linear equations, namely to triangularize the system, or carry out the elimination process. The crucial observation, first stated by Trinks in 1978, is the elimination property of Gröbner bases. It states that if G is a Gröbner basis of I w.r.t. the lexicographic ordering with $x_1 < \ldots < x_n$, then the i–th elimination ideal of I, i.e. $I \cap K[x_1, \ldots, x_i]$, is generated by those polynomials in G that depend only on the variables $x_1, \ldots, x_i$.

Theorem 2.2.5. (Elimination Property of Gröbner Bases) *Let G be a Gröbner basis of I w.r.t. the lexicographic ordering $x_1 < \ldots < x_n$. Then*

$$I \cap K[x_1, \ldots, x_i] = \langle G \cap K[x_1, \ldots, x_i] \rangle,$$

where the ideal on the right hand side is generated over the ring $K[x_1, \ldots, x_i]$.

A proof can be found in [Win96], Chap.8. Theorem 2.2.5 can clearly be generalized to product orderings, without changing anything in the proof.

Example 2.2.2 Consider the system of equations $f_1 = f_2 = f_3 = 0$, where

$$\begin{aligned} 4xz - 4xy^2 - 16x^2 - 1 &= 0, \\ 2y^2 z + 4x + 1 &= 0, \\ 2x^2 z + 2y^2 + x &= 0, \end{aligned}$$

are polynomials in $\mathbb{Q}[x, y, z]$. We are looking for solutions of this system of algebraic equations in $\overline{\mathbb{Q}}^3$, where $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

Let $<$ be the lexicographic ordering with $x < y < z$. The algorithm GRÖBNER_B applied to $F = \{f_1, f_2, f_3\}$ yields (after reducing the result) the reduced Gröbner basis $G = \{g_1, g_2, g_3\}$, where

$$\begin{aligned} g_1 =& 65z + 64x^4 - 432x^3 + 168x^2 - 354x + 104, \\ g_2 =& 26y^2 - 16x^4 + 108x^3 - 16x^2 + 17x, \\ g_3 =& 32x^5 - 216x^4 + 64x^3 - 42x^2 + 32x + 5. \end{aligned}$$

By Theorem 3.1 the system is solvable. Furthermore, by Theorem 3.2, the system has finitely many solutions. The Gröbner basis G yields an equivalent triangular system in which the variables are completely separated. So we can get solutions by solving the univariate polynomial g_3 and propagating the partial solutions upwards to solutions of the full system. The univariate polynomial g_3 is irreducible over $\mathbb{Q}$, and the solutions are

$$(\alpha,\ \pm\frac{1}{\sqrt{26}}\sqrt{\alpha}\sqrt{16\alpha^3-108\alpha^2+16\alpha-17},\ -\frac{1}{65}(64\alpha^4-432\alpha^3+168\alpha^2-354\alpha+104)),$$

where α is a root of g_3. We can also determine a numerical approximation of a solution from G, e.g.

$$(-0.1284722871,\ 0.3211444930,\ -2.356700326).$$

□

Arithmetic of polynomial ideals

In commutative algebra and algebraic geometry there is a strong correspondence between radical polynomial ideals and algebraic sets, the sets of zeros of such ideals over the algebraic closure of the field of coefficients. For any ideal I in $K[x_1,\ldots,x_n]$ we denote by $V(I)$ the set of all points in $\mathbb{A}^n(\overline{K})$, the n–dimensional affine space over the algebraic closure of K, which are common zeros of all the polynomials in I. Such sets $V(I)$ are called *algebraic sets* (we will introduce algebraic sets below). On the other hand, for any subset V of $\mathbb{A}^n(\overline{K})$ we denote by $I(V)$ the ideal of all polynomials vanishing on V. Then for radical ideals I and algebraic sets V the functions $V(\cdot)$ and $I(\cdot)$ are inverses of each other, i.e.

$$V(I(V)) = V \quad \text{and} \quad I(V(I)) = I.$$

This correspondence extends to operations on ideals and algebraic sets in the following way:

ideal	algebraic set
$I+J$	$V(I)\cap V(J)$
$I\cdot J,\ I\cap J$	$V(I)\cup V(J)$
$I:J$	$V(I)-V(J)=\overline{V(I)-V(J)}$ (Zariski closure of the difference)

So we can effectively compute intersection, union, and difference of varieties if we can carry out the corresponding operations on ideals.

Definition 2.2.1 Let I, J be ideals in $K[X]$.
The *sum* $I+J$ of I and J is defined as

$$I+J=\{f+g \mid f\in I, g\in J\}.$$

The *product* $I\cdot J$ of I and J is defined as

$$I\cdot J=\langle\{f\cdot g \mid f\in I, g\in J\}\rangle.$$

The *quotient* $I:J$ of I and J is defined as

$$I:J=\{f \mid f\cdot g\in I \text{ for all } g\in J\}.$$

□

Theorem 2.2.6 *Let $I=\langle f_1,\ldots,f_r\rangle$ and $J=\langle g_1,\ldots,g_s\rangle$ be ideals in $K[X]$.*
(a) $I+J=\langle f_1,\ldots,f_r,g_1,\ldots,g_s\rangle$.
(b) $I\cdot J=\langle f_ig_j \mid 1\le i\le r, 1\le j\le s\rangle$.
(c) $I\cap J=(\langle t\rangle\cdot I+\langle 1-t\rangle\cdot J)\cap K[X]$, where t is a new variable.
(d) $I:J=\bigcap_{j=1}^{s}(I:\langle g_j\rangle)$ and
$I:\langle g\rangle=\langle h_1/g,\ldots,h_m/g\rangle$, where $I\cap\langle g\rangle=\langle h_1,\ldots,h_m\rangle$.

Proof: (a) and (b) are easily seen.

(c) Let $f \in I \cap J$. Then $tf \in \langle t \rangle \cdot I$ and $(1-t)f \in \langle t-1 \rangle \cdot J$. Therefore $f = tf + (1-t)f \in \langle t \rangle \cdot I + \langle 1-t \rangle \cdot J$.

On the other hand, let $f \in (\langle t \rangle \cdot I + \langle 1-t \rangle \cdot J) \cap K[X]$. So $f = g(X,t) + h(X,t)$, where $g \in \langle t \rangle I$ and $h \in \langle 1-t \rangle J$. In particular, $h(X,t)$ is a linear combination of the basis elements $(1-t)g_1, \ldots, (1-t)g_s$ of $\langle 1-t \rangle J$. Evaluating t at 0 we get

$$f = g(X,0) + h(X,0) = h(X,0) \in J.$$

Simlilarly, by evaluating t at 1 we get $f = g(X,1) \in I$.
(d) $h \in I : J$ if and only if $hg \in I$ for all $g \in J$ if and only if $hg_j \in I$ for all $1 \leq j \leq s$ if and only if $h \in I : \langle g_j \rangle$ for all $1 \leq j \leq s$.
If $f \in \langle h_1/g, \ldots, h_m/g \rangle$ and $a \in \langle g \rangle$ then $af \in \langle h_1, \ldots, h_m \rangle = I \cap \langle g \rangle \subset I$, i.e. $f \in I : \langle g \rangle$. Conversely, suppose $f \in I : \langle g \rangle$. Then $fg \in I \cap \langle g \rangle$. So $fg = \sum b_k h_k$ for some $b_k \in K[X]$. Thus,

$$f = \sum b_k \cdot (\underbrace{h_k/g}_{polynomial}) \quad \in \quad \langle h_1/g, \ldots, h_m/g \rangle. \qquad \square$$

So all these operations can be carried out effectively by operations on the bases of the ideals. In particular the intersection can be computed by Theorem 2.2.6(c).

We always have $I \cdot J \subset I \cap J$. However, $I \cap J$ could be strictly larger than $I \cdot J$. For example, if $I = J = \langle x, y \rangle$, then $I \cdot J = \langle x^2, xy, y^2 \rangle$ and $I \cap J = I = J = \langle x, y \rangle$. Both $I \cdot J$ and $I \cap J$ correspond to the same variety. Since a basis for $I \cdot J$ is more easily computed, why should we bother with $I \cap J$? The reason is that the intersection behaves much better with respect to the operation of taking radicals (recall that it is really the radical ideals that uniquely correspond to algebraic sets). Whereas the product of radical ideals in general fails to be radical (consider $I \cdot I$), the intersection of radical ideals is always radical. For a proof see Theorem 8.4.10 in [Win96].

Theorem 2.2.7 *Let I, J be ideals in $K[X]$. Then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ ($\sqrt{I}$ means the radical of I).*

Example 2.2.3 Consider the ideals

$$\begin{aligned} I_1 &= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle, \\ I_2 &= \langle x, y^2 - 4 \rangle, \\ I_3 &= \langle x, y^2 - 2y \rangle, \\ I_4 &= \langle x, y^2 + 2y \rangle. \end{aligned}$$

The coefficients are all integers, but we consider them as defining algebraic sets in the affine plane over $\mathbb{C}$. In fact, $V(I_1)$ is the tacnode curve (compare Fig. 1.1.3). $V(I_2) = \{(0,2), (0,-2)\}$, $V(I_3) = \{(0,2), (0,0)\}$, $V(I_4) = \{(0,0), (0,-2)\}$.

First, let us compute the ideal I_5 defining the union of the tacnode and the 2 points in $V(I_2)$. I_5 is the intersection of I_1 and I_2, i.e.

$$\begin{aligned} I_5 = I_1 \cap I_2 &= (\langle z \rangle I_1 + \langle 1-z \rangle I_2) \cap \mathbb{Q}[x,y] \\ &= \langle -4y^2 + 8y^3 - 3y^4 + 12x^2y - 8x^4 - 2y^5 + y^6 - 3x^2y^3 + 2y^2x^4, \\ &\quad xy^2 - 2xy^3 + xy^4 - 3x^3y + 2x^5 \rangle. \end{aligned}$$

Now let us compute the ideal I_6 defining $V(I_5) - V(I_3)$, i.e. the Zariski closure of $V(I_5) \setminus V(I_3)$, i.e. the smallest algebraic set containing $V(I_5) \setminus V(I_3)$.

$$\begin{aligned}
I_6 = I_5 : I_3 &= (I_5 : \langle x \rangle) \cap (I_5 : \langle y^2 - 2y \rangle) \\
&= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \cap \\
&\quad \langle y^5 - 3y^3 + 2y^2 - 3x^2y^2 + 2yx^4 - 6x^2y + 4x^4,\ 2x^5 - 3x^3y + xy^2 - 2xy^3 + xy^4 \rangle \\
&= \langle y^5 - 3y^3 + 2y^2 - 3x^2y^2 + 2yx^4 - 6x^2y + 4x^4,\ 2x^5 - 3x^3y + xy^2 - 2xy^3 + xy^4 \rangle.
\end{aligned}$$

$V(I_6)$ is the tacnode plus the point $(0, -2)$.
Finally, let us compute the ideal I_7 defining $V(I_6) - V(I_4)$, i.e. the Zariski closure of $V(I_6) \setminus V(I_4)$.

$$\begin{aligned}
I_7 = I_6 : I_4 &= (I_6 : \langle x \rangle) \cap (I_6 : \langle y^2 + 2y \rangle) \\
&= \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \ \cap \ \langle 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \rangle \\
&= I_1.
\end{aligned}$$

So we get back the ideal I_1 defining the tacnode curve. □

The radical $\sqrt{I}$ of an ideal I generalizes the square-free part of a polynomial. For principal ideals $\langle p(x) \rangle$ in $K[x]$ the radical is simply the ideal generated by the square-free part of the generator p, i.e.

$$\sqrt{\langle p \rangle} \ = \ \langle q \rangle,$$

where $q(x)$ is the square-free part of $p(x)$. There are also algorithms for computing the radical of an ideal in $K[x_1, \ldots, x_n]$. Here we only show how to get the radical of a 0-dimensional ideal.

Theorem 2.2.8 *Let K be algebraically closed, I a 0-dimensional ideal in $K[x_1, ..., x_n]$. For each $i = 1, \ldots, n$, let p_i be the unique monic generator of $I \cap K[x_i]$, and let $\tilde{p}_i$ be the square-free part of p_i. Then*

$$\sqrt{I} = I + \langle \tilde{p}_1, \ldots, \tilde{p}_n \rangle.$$

A proof of this theorem can be found in [CLO98], p.39.

2.3 Basis conversion for 0-dimensional ideals — FGLM