GRÖBNER BASES

MARCUS TRESSL

ABSTRACT. A quick reference.

CONTENTS

1. MONOMIAL ORDERINGS

We will use multi index notation for elements of $\mathbb{N}_0^n$ (here $\mathbb{N} = \{1, 2, 3, ...\}$ and $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$): For $\alpha \in \mathbb{N}_0^n$, we write

$$\begin{aligned} \alpha! &= \alpha_1! \cdot ... \cdot \alpha_n! \\ |\alpha| &= \alpha_1 + ... + \alpha_n \end{aligned}$$

1.1. **Definition.** The **monomials in n variables**, formally is the monoid $\mathbb{N}_0^n$ equipped with addition, written multiplicatively. We write $X = (X_1, ..., X_n)$ and the set of monomials as

$$\text{Mon}(X) = \{X^\alpha \mid \alpha \in \mathbb{N}_0^n\},$$

where $X^\alpha = X_1^{\alpha_1} ... X_n^{\alpha_n}$. $\text{Mon}(X)$ is partially ordered by

$$X^\alpha | X^\beta \iff \alpha \le \beta \iff \alpha_i \le \beta_i \ (1 \le i \le n)$$

Note that

$$X^\alpha | X^\beta \iff \text{ there is } Y \in \text{Mon}(X) \text{ with } X^\beta = Y X^\alpha.$$

The neutral element of $\text{Mon}(X)$ is $X^0 = X_1^0 ... X_n^0$ and denoted by 1.

We denote by $\deg_{X_i} U$ the degree of $U \in \text{Mon}(X)$ in X_i.

Date: January 4, 2025.

2000 *Mathematics Subject Classification.* Primary: XXXXX, Secondary: XXXXX.

1.2. **Theorem.** *(Dickson's Lemma)*
Let $M \subseteq \mathrm{Mon}(X)$. Then there is a finite subset $B \subseteq M$ such that

$$M \subseteq B\cdot \mathrm{Mon}(X)\ (:= \{b\cdot a \mid b \in B, a \in \mathrm{Mon}(X)\}).$$

Each such set B is called a **Dickson basis of** *M.*

Proof. By induction on n, where the case $n = 1$ is obvious.
$\underline{n-1 \Rightarrow n}$. Pick $X^\alpha \in M$. For each pair $(i,p) \in \{1,...,n\} \times \{0,...,\alpha_i\}$, let

$$M_{(i,p)} = \{U \in M \mid \deg_{X_i} U = p\}$$

and

$$M^*_{(i,p)} = \{V \in \mathrm{Mon}(X) \mid X_i^p \in M_{(i,p)}\}.$$

Thus $M_{(i,p)} = X_i^p\cdot M^*_{(i,p)}$ and the degree of X_i in any element of $M^*_{(i,p)}$ is 0. Thus $M^*_{(i,p)}$ is a set of monomial in at most $n-1$ variables and by the induction hypothesis there is a finite subset $C_{(i,p)}$ of $M^*_{(i,p)}$ with

$$M^*_{(i,p)} \subseteq C_{(i,p)}\cdot \mathrm{Mon}(X_1,...,X_{i-1},X_{i+1},...,X_n) \subseteq C_{(i,p)}\cdot \mathrm{Mon}(X).$$

Then $B_{(i,p)} := X_i^p\cdot C_{(i,p)} \subseteq X_i^p\cdot M^*_{(i,p)} \subseteq M$ and

$$B := \{X^\alpha\} \cup \bigcup_{(i,p)\in\{1,...,n\}\times\{0,...,\alpha_i\}} B_{(i,p)} \subseteq M$$

is finite. We claim that $M \subseteq B\cdot \mathrm{Mon}(X)$. Take $U \in M$. If there is some $i \in \{1,...,n\}$ and some $p \in \{0,...,\alpha_i\}$ with $\deg_{X_i} U = p$, then $U \in M_{(i,p)} = X_i^p M^*_{(i,p)} \subseteq X_i^p C_{(i,p)}\cdot \mathrm{Mon}(X) = B_{(i,p)}\cdot \mathrm{Mon}(X) \subseteq B\cdot \mathrm{Mon}(X)$.

If for each $i \in \{1,...,n\}$ we have $\deg_{X_i} U \geq \alpha_i$, then $X^\alpha | U$, thus $U \in B\cdot \mathrm{Mon}(X)$, too. □

Remark. Dickson's lemma 1.2 can also be proved by using the noetherianity of $K[X]$ for any field K: Consider M as a subset of monomials from $K[X]$. Since $K[X]$ is noetherian, there is a finite subset $B \subseteq M$ with $(B) = (M)$. It then follows easily that B has the required properties (this will be made explicit in 3.3 below). However, we will see that we get the noetherianity of $K[X]$ for free in our course on Gröbner bases (cf. 4.3)

1.3. **Definition.** A **monomial ordering** on $\mathrm{Mon}(X)$ is a total ordering $<$ on $\mathrm{Mon}(X)$ satisfying

$$U < V \Rightarrow UW < VW$$

for all $U, V, W \in \mathrm{Mon}(X)$.

Observe that a monomial ordering does not need to respect the poset structure given on monomials by multiplication. Moreover if $<$ is a monomial ordering, then also $>$ is a monomial ordering.

1.4. **Lemma and Definition.** *The following are equivalent for every monomial ordering $<$:*

(i) $1 < X_i$ *for all* $i \in \{1,...,n\}$.
(ii) $1 < U$ *for all* $U \in \mathrm{Mon}(X)$, $U \neq 1$.
(iii) $<$ *is compatible with* $|$, *i.e.* $U < UV$ *for all* $U, V \in \mathrm{Mon}(X)$, $V \neq 1$.
(iv) $<$ *is a well ordering*

If this is the case, then $<$ is called a **global** *monomial ordering. If the reverse order of $<$ is global, then $<$ is called a* **local** *monomial ordering. If $<$ is neither global nor local, then it is called a* **mixed** *ordering.*

Proof. It is obvious that (i),(ii) and (iii) are equivalent.

(iv)⇒(i). Suppose $X_1 < 1$. Then $\cdots < X_i^3 < X_i^2 < X_i < 1$, hence $<$ is not a well-ordering.

(iii)⇒(iv). Let $M \subseteq \mathrm{Mon}(X)$ be non empty. By Dickson's lemma 1.2, there is a finite subset $B \subseteq M$ with $M \subseteq B \cdot \mathrm{Mon}(X)$. Since $<$ is compatible with $|$, this implies that for each $U \in M$ there is some $V \in B$ with $V \leq U$. Since B is finite and totally ordered by $<$, the $<$-smallest element of B is a smallest element of M w.r.t. $<$. □

1.5. **Definition.** Let $<$ be a monomial ordering on $\mathrm{Mon}(X)$. Let R be a ring and let $f \in R[X]$, $f \neq 0$. Write

$$f = a_{\alpha_d} X^{\alpha_d} + ... + a_{\alpha_1} X^{\alpha_1}, \text{ with } X^{\alpha_d} > ... > X^{\alpha_1},$$

$d \geq 1$ and $a_{\alpha_d} \in R \setminus \{0\}$. We define

(i) $\mathrm{LM}(f) = X^{\alpha_d}$, the **leading monomial** of f.
(ii) $\deg_<(f) = \mathrm{LE}(f) = \alpha_d$, the **leading exponent** of f. We extend $\deg_<$ through 0 by $\deg_< 0 = -\infty$.
(iii) $\mathrm{LT}(f) = a_{\alpha_d} X^{\alpha_d}$, the **leading term** of f.
(iv) $\mathrm{LC}(f) = a_{\alpha_d}$, the **leading coefficient** of f.
(v) $\mathrm{tail}(f) = f - a_{\alpha_d} X^{\alpha_d}$, the **tail** of f.

Convention. We will also compare the exponents $\alpha \in \mathbb{N}_0^n$ with respect to a given monomial ordering, by

$$\alpha < \beta \iff X^\alpha < X^\beta.$$

1.6. **Observation.** *Let $<$ be a monomial ordering. Let R be a ring and let $f, g \in R[X]$.*

(i) If R is a domain, then $\deg_<(fg) = \deg_<(f) + \deg_<(g)$.
(ii) $\deg_<(f+g) \leq \max\{\deg_< f, \deg_< g\}$ and if $\deg_< f \neq \deg_< g$ then $\deg_<(f+g) = \max\{\deg_< f, \deg_< g\}$. □

1.7. *Notation.* Let R be a ring and let $f \in R[X]$. We say that a monomial M **occurs** in f or **appears** in f, if there are $k \geq 0$, $a_i \in R$, monomials $U_i \neq M$ $(1 \leq i \leq k)$ and some $a \in R$, $a \neq 0$ such that $f = aM + \sum_{i=1}^k a_i U_i$.

In particular no monomial occurs in the zero polynomial. Observe that by definition, the monomial X^α does **not** occur in $X^{\alpha+\beta}$ for every $\beta \neq (0, ..., 0)$.

1.8. *Examples.* The following are examples of global monomial orderings.

(i) The **lexicographic ordering** $<_{\mathrm{lex}}$, defined by

$$X^\alpha <_{\mathrm{lex}} X^\beta \iff \exists i \in \{1, ..., n\}: \ \alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1} \text{ and } \alpha_i < \beta_i.$$

To say this differently, $X^\alpha <_{\mathrm{lex}} X^\beta$ if and only if the left most non-zero entry in $\beta - \alpha \in \mathbb{Z}^n$ is positive. Note that this ordering depends on our choice of ordering the variables $X_1, ..., X_n$. Here we have $X_1 > ... > X_n$ (note that $(1, 0, ...) > (0, 1, ...)$).

(ii) The **graded lexicographic ordering** $<_{\mathrm{grlex}}$, defined by

$$X^\alpha <_{\mathrm{grlex}} X^\beta \iff |\alpha| < |\beta| \text{ or } |\alpha| = |\beta|, \alpha <_{\mathrm{lex}} \beta$$

(iii) The **graded reverse lexicographic ordering** $<_{\text{grlex}}$, defined by

$$X^\alpha <_{\text{grevlex}} X^\beta \iff |\alpha| < |\beta| \text{ or } |\alpha| = |\beta|, \beta <_{\text{lex}} \alpha$$

1.9. **Observation.** *The order type of the graded lexicographic ordering is the order type of $\mathbb{N}$.*

1.10. **Theorem.** (*Robbiano*)
Let $\sqsubset$ be the lexicographic ordering on $\mathbb{R}^n$ (with respect to some choice of coordinate axes). For $A \in \mathrm{GL}_n(\mathbb{R})$ define $<_A$ on $\mathrm{Mon}(X)$ via

$$X^\alpha <_A X^\beta \iff A\alpha \sqsubset A\beta.$$

Then $<_A$ is a monomial ordering and every monomial ordering is of this form. Observe that $<_A$ is global if and only if the first non-zero entry in each column of A is positive.

Proof. [GrePfi2008, Remark 1.2.7] □

2. A division algorithm

Let $X = (X_1, ..., X_n)$ and let $<$ be a global monomial ordering. Let K be a field and fix $f_1, ..., f_k \in K[X]$.

In this section we find for each $f \in K[X]$ polynomials $q_1, ..., q_k, r \in K[X]$ with

$$(*)_f \quad \begin{array}{l} f = q_1 f_1 + ... + q_k f_k + r, \quad \deg_< q_i f_i \leq \deg_< f \ (1 \leq i \leq k), \\ \text{such that none of the leading monomials of any } f_i \\ \text{divides any monomial occurring in } r. \end{array}$$

Explicitly, the condition on r means $r = 0$ or $r = \sum a_i M_i$ with $a_i \in K$, $a_i \neq 0$ and monomials M_i such that $\mathrm{LM}(f_j) \nmid M_i$ for all i, j. Also notice that by 1.6, we know $\deg_<(r) = \deg_<(f - \sum q_i f_i) \leq \deg_<(f)$[1]

2.1. **Lemma.** *(Step 1: modifies one of the q_i)*
Let $g, f_1, ..., f_k \in K[X] \setminus \{0\}$. Let $i \in \{1, ..., n\}$ be such that $\mathrm{LM}(f_i)$ divides $\mathrm{LM}(g)$. Define

$$\tilde{g} = g - \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)} f_i$$

Then $\deg_< \tilde{g} < \deg_< g$ (by definition) and every solution $q_1, ..., q_k, r$ of $(*)_{\tilde{g}}$ gives the solution $q_1, ..., q_{i-1}, q_i + \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)}, q_{i+1}, ..., q_k, r$ of $(*)_g$. In particular

$$g \equiv \tilde{g} \bmod (f_1, ..., f_k).$$

Proof. Obvious. □

2.2. **Lemma.** *(Step 2: modifies r)*
Let $g, f_1, ..., f_k \in R[X] \setminus \{0\}$. Suppose for all $i \in \{1, ..., n\}$, $\mathrm{LM}(f_i)$ does not divide $\mathrm{LM}(g)$. Define

$$\hat{g} := g - \mathrm{LT}(g).$$

Then $\deg_< \hat{g} < \deg_< g$ (by definition) and every solution $q_1, ..., q_k, r$ of $(*)_{\hat{g}}$ gives the solution $q_1, ..., q_k, r + \mathrm{LT}(g)$ of $(*)_g$.

Proof. Obvious. □

[1]In the 1-variable case, the latter condition simply means $\deg f_j > \deg r$. Hence in this case the division algorithm is the ordinary division with remainder for univariate polynomials.

Iterating 2.1 and 2.2 starting with $g = f$ as long as the output $\tilde{g}$, $\hat{g}$, resp. is non zero will terminate, since at each step the leading exponent of the output is strictly smaller than the leading monomial of the input g (observe that $<$ is global, hence a well ordering by 1.4).

Thus, when the iteration stops we have $g = 0$, we choose $q_1 = ...q_k = r = 0$ and work back to obtain a solution of $(*)_f$.

3. Monomial ideals

Again, let K be a field and let $X = (X_1, ..., X_n)$.

3.1. **Definition.** A **monomial ideal** of $K[X]$ is an ideal of $K[X]$ generated (as an ideal) by a set of monomials.

3.2. **Lemma.** *Let I be a monomial ideal generated by $M \subseteq \mathrm{Mon}(X)$ and let $f \in K[X]$. The following are equivalent:*
(i) $f \in I$.
(ii) Every monomial that occurs in f lies in I.
(iii) f is a K-linear combination of monomials from I.
(iv) Every monomial that occurs in f is divisible by some monomial from M.

Proof. (iv)⇒(iii)⇒(ii)⇒(i) is clear.
(i)⇒(iv). Let $U_1, ..., U_k \in M$ and $f_1, ..., f_k \in K[X]$ with $f = f_1U_1 + ... + f_kU_k$. Let V be a monomial occurring in f. Then V also occurs in $f_1U_1 + ... + f_kU_k$. However, every monomial occurring in $f_1U_1 + ... + f_kU_k$ is divisible by some monomial from M. □

3.3. **Corollary.** *Let $M \subseteq \mathrm{Mon}(X)$ and let U be another monomial. Then*

$$U \in (M) \iff V|U \text{ for some } V \in A.$$

□

Let $<$ be a global monomial ordering.

3.4. **Definition.** Let Z be a subset of $K[X]$. We define the **leading ideal** $L(Z)$ of Z as

the ideal of $K[X]$ generated by all the $\mathrm{LM}(f)$ with $f \in Z$.

Obviously, $L(Z)$ is a monomial ideal.

3.5. *Warning.* If $f, g \in K[T, Y]$, T, Y single variables, then in general $L(f, g)$ is **not** equal to $L(I)$, with $I = (f, g)$.

Proof. We work with $<_{\text{grlex}}$. Take $f = T^3 - 2TY$, $g = T^2Y - 2Y^2 + T$. Then $T^2 = T\cdot g - Y\cdot f \in I$, but $T^2 \notin (T^3, T^2Y) = L(f, g)$. □

3.6. **Proposition.** *Let $I \subseteq K[X]$ be an ideal. Then there is a finite subset G of I with $L(G) = L(I)$.*

Proof. By noetherianity or by Dickson's lemma 1.2. □

4. Gröbner bases

Wolfgang Gröbner, 1899-1980 (Österreich)

4.1. **Definition.** Let $I \subseteq K[X]$ be an ideal. A **Gröbner basis** of I is a finite subset G of I with $L(G) = L(I)$.

A subset G of $K[X]$ is called a Gröbner basis, if G is a Gröbner basis of the ideal generated by G.

4.2. **Theorem.** *Let $f_1, ..., f_k$ be a Gröbner basis of an ideal I and let $f \in K[X]$.*

Let $q_1, ..., q_k, r \in K[X]$ with

$$f = q_1 f_1 + ... + q_k f_k + r$$

such that none of the leading monomials of any f_i divides the leading monomial of r. (Notice that by section 2 there are $q_1, ..., q_k, r \in K[X]$ with this property; in fact we have much more information, but for this theorem we only need a weak assumption.)

Then

$$f \in I \iff r = 0.$$

In particular, every Gröbner basis of I generates I as an ideal.

Proof. If $f \in I$ then also $r \in I$ and so $\mathrm{LM}(r) \in (I)$. Since $f_1, ..., f_k$ is a Gröbner basis of I, $\mathrm{LM}(r) \in (LM(f_1), ..., \mathrm{LM}(f_r))$. Now if $r \neq 0$, then by 3.2, $\mathrm{LM}(r)$ is divisible by some $\mathrm{LM}(f_i)$, a contradiction. □

4.3. **Corollary.** *$K[X]$ is noetherian.*

Proof. Let I be an ideal of $K[X]$. By 3.6 (which has a proof not using the noetherianity of $K[X]$), I has a finite Gröbner basis. By 4.2, I is generated by such a basis. □

4.4. **Corollary.** *Let $\{g_1, ..., g_k\} \subseteq K[X]$ be a Gröbner basis and let $f \in K[X]$. Then there is a unique $r \in K[X]$ with the following two properties:*

(i) $f \equiv r \bmod (g_1, ..., g_k)$.

(ii) No leading term of any of the g_i divides any monomial occurring in r.

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm of section 2.

r is called the **normal form** *of f with respect to $\{g_1, ..., g_k\}$.*

Proof. Existence of r has been shown in section 2. If $r' \in K[X]$ also has properties (i) and (ii), then $r - r' \in I := (g_1, ..., g_k)$ and no leading term of any of the g_i divides any monomial occurring in $r - r'$. By 4.2, $r - r' = 0$. □

5. Characterisation of Gröbner bases via S-polynomials

Throughout we work with a global monomial ordering $<$. For $\alpha, \beta \in \mathbb{N}_0^n$ let $\alpha \vee \beta = (\max\{\alpha_1, \beta_1\}, ..., \max\{\alpha_1, \beta_1\})$. Hence $X^{\alpha\vee\beta} = \mathrm{lcm}(X^\alpha, X^\beta)$ (in $\mathrm{Mon}(X)$ and in $K[X]$).

5.1. **Definition.** Let $f, g \in K[X] \setminus \{0\}$. Let $\alpha = \deg_< f$ and $\beta = \deg_< g$. The **S-polynomial** of f and g is defined as

$$S(f, g) = \frac{X^{\alpha\vee\beta}}{LT(f)} f - \frac{X^{\alpha\vee\beta}}{LT(g)} g.$$

5.2. *Remark.* Let $f_1, f_2 \in K[X] \setminus \{0\}$. By definition, $S(f_1, f_2)$ is of the form $q_1 f_1 + q_2 f_2$ for some $q_1, q_2 \in K[X]$. However, this in general is not the representation of $S(f_1, f_2)$ that we obtain from our division algorithm in section 2 for f_1, f_2.

The reason is that the division algorithm produces a representation

$$S(f_1, f_2) = q_1 f_1 + q_2 f_2 + r,$$

where $\deg_< g_i f_i \leq \deg_< S(f_1, f_2)$.

On the other hand in the representation of $S(f_1, f_2)$ of definition 5.1, this always fails if $\deg_< f_1 = \deg_< f_2$!

5.3. **Observation.** *Let $f, g \in K[X] \setminus \{0\}$, $\alpha = \mathrm{LE}(f), \beta = \mathrm{LE}(g)$.*

(i) $\deg_< S(f, g) < \alpha \vee \beta$.
(ii) $S(f, f) = 0$, $S(f, g) = -S(g, f)$ *and* $S(cf, g) = S(f, g)$ *for all* $c \in K \setminus \{0\}$.
(iii) If $\gamma, \delta \in \mathbb{N}_0^n$ *then*

$$S(X^\gamma f, X^\delta g) = X^{(\alpha+\gamma)\vee(\beta+\delta)\ -\ \alpha\vee\beta} S(f, g).$$

5.4. **Lemma.** *Let $\alpha \in \mathbb{N}_0^n$ and let $f_1, ..., f_k \in K[X]$ be with $\deg_< f_i = \alpha$. Let $c_1, ..., c_k \in K$ and $f := \sum_{i=1}^k c_i f_i$.*
If $\deg f < \alpha$, then f is a K-linear combination of all the $S(f_i, f_{i+1})$ with $1 \leq i < k$.

Proof. Let $d_i = \mathrm{LC}(f_i)$ and let $p_i = \frac{1}{d_i} f_i$. As $\deg_< f_i = \alpha$ for all i we have

$$(*) \qquad p_i - p_{i+1} = S(f_i, f_{i+1}) \text{ for all } 1 \leq i < k.$$

Now

$$\begin{aligned} f &= \sum_{i=1}^k c_i d_i p_i = \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ &\quad +(c_1 d_1 + ... + c_{k-1} d_{k-1})(p_{k-1} - p_k) + \\ &\quad +(c_1 d_1 + ... + c_k d_k) p_k. \end{aligned} \tag{5.1}$$

Since $\deg_< f_i = \alpha$ for all i and $\deg_< f < \alpha$ it is clear that $\sum_{i=1}^k c_i d_i = 0$. Hence the last summand in the sum (5.1) above vanishes. Thus, using (*), equation (5.1) reads as $f = c_1 d_1 S(f_1, f_2) + ... + (c_1 d_1 + ... + c_{k-1} d_{k-1}) S(f_{k-1}, f_k)$ as required. □

5.5. **Theorem.** (*Buchberger's criterion for Gröbner bases*)
Let $g_1, ..., g_k \in K[X]$. Then $\{g_1, ..., g_k\}$ is a Gröbner bases if and only if the remainder on division of $S(g_i, g_j)$ by $g_1, ..., g_k$ using the division algorithm of section 2 (in some order) is zero.

Proof. If $\{g_1, ..., g_k\}$ is a Gröbner bases then by 4.4, the remainder is 0 as $S(g_i, g_j) \in (g_1, ..., g_k)$.

Conversely suppose for all $i, j \in \{1, ..., k\}$ the remainder on division of $S(g_i, g_j)$ by $g_1, ..., g_k$ using the division algorithm of section 2 is zero. We have to show that for every $f \in I := (g_1, ..., g_k)$ we have $\mathrm{LT}(f) \in (\mathrm{LT}\, g_1, ..., \mathrm{LT}\, g_k)$. We write $f = \sum h_i g_i$ with $h_i \in K[X]$ and proceed by induction on $\alpha = \max_{i=1}^k \deg_< h_i g_i$. Note that this makes sense since $<$ is global, hence a well ordering. Let $I \subseteq \{1, ..., k\}$ be the set of all indices with $\deg_< h_i g_i = \alpha$.

Case 1. $\deg_< f = \alpha$.

Then $\mathrm{LT}(f)$ is a k-linear combination of the $\mathrm{LT}(h_i g_i)$ with $i \in I$. But this is only possible if one of the $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(f)$.

Case 2. $\deg_< f < \alpha$.

Then
$$f^* := \sum_{i \in I} \mathrm{LT}(h_i) g_i$$
has to satisfy $\deg_< f^* < \alpha$ as well, since
$$f - f^* = \sum_{i \in I} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{i \notin I} h_i g_i$$
has leading exponent $< \alpha$.

For each $i \in I$, $\mathrm{LT}(h_i) g_i$ has leading exponent α and we can apply 5.4: There are $c_{ij} \in K$ $(i, j \in I)$ with
$$(*) \qquad f^* = \sum_{i,j \in I} c_{ij} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j).$$
By 5.3(ii) and (iii) we have
$$S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j) = X^{\alpha - \beta(i,j)} S(g_i, g_j),$$
where $\beta(i, j) = \mathrm{LE}(g_i) \vee \mathrm{LE}(g_j)$.

By assumption, the remainder on division of $S(g_i, g_j)$ by $g_1, ..., g_k$ using the division algorithm of section 2 is zero. Hence for all $i, j \in I$, there are $q_{ijl} \in K[X]$ with
$$\deg_< q_{ijl} g_l \leq \deg_< S(g_i, g_j) \ (l \in \{1, ..., k\})$$
such that
$$S(g_i, g_j) = \sum_{l=1}^{k} q_{ijl} g_l.$$
Substituting this in $(*)$ gives
$$(+) \qquad f^* = \sum_{i,j \in I} c_{ij} X^{\alpha - \beta(i,j)} S(g_i, g_j) = \sum_{i,j \in I, l \in \{1,...,k\}} c_{ij} X^{\alpha - \beta(i,j)} q_{ijl} g_l.$$
Since $\deg_< S(g_i, g_j) < \deg_< S(g_i) \vee \deg_< S(g_j) = \beta(i, j)$ we get $\deg_< q_{ijl} g_l < \beta(i, j)$ from the choice of the q_{ijl}. Therefore $\deg_< c_{ij} X^{\alpha - \beta(i,j)} q_{ijl} g_l < \alpha$.

Hence in equation $(+)$ we have rewritten f^* as a $K[X]$-linear combination of the $g_1, ..., g_k$ where each summand has leading exponent $< \alpha$. Since also every summand in $f - f^*$ has leading exponent $< \alpha$, f itself can be written as a $K[X]$-linear combination of the $g_1, ..., g_k$ where each summand has leading exponent $< \alpha$. Thus, we may apply the induction hypothesis. □

5.6. **Corollary.** *A finite subset* $\{g_1, ..., g_k\}$ *of* $K[X]$ *is a Gröbner basis if and only if for all* $f, q_1, ..., q_k, r \in K[X]$ *with*
$$f = q_1 g_1 + ... + q_k g_k + r$$
such that $\deg_< q_i f_i \leq \deg_< f$ *and none of the leading monomials of any* g_i *divides the leading monomial of* r*, we have*
$$f \in (g_1, ..., g_k) \iff r = 0.$$

Proof. Every Gröbner bases has this property by 4.2. Conversely, the property implies that the remainder on division of $S(g_i, g_j)$ by $g_1, ..., g_k$ using the division algorithm of section 2 is zero. Hence by 5.5, G is a Gröbner basis. □

6. Buchberger's Algorithm

Throughout we work with a global monomial ordering $<$.

6.1. **Lemma.** *Let $f_1, ..., f_k \in K[X]$. Let $i, j \in \{1, ..., k\}$ and let r be the remainder on division of $S(f_i, f_j)$ by $f_1, ..., f_k$ using the division algorithm of section 2.*
If $r \neq 0$, then $\mathrm{LT}(r) \notin (\mathrm{LT}(f_1), ..., \mathrm{LT}(f_k))$.

Proof. The division algorithm, says that none of the leading monomials of any f_i divides any monomial occurring in r. Now apply 3.3. □

6.2. **Theorem.** (*Buchberger's Algorithm*)
Let $f_1, ..., f_k \in K[X]$. Write $F := \{f_1, ..., f_k\}$ and define

$$F^\dagger = \begin{cases} F & \text{if the remainder on division of } S(f_i, f_j) \text{ by } f_1, ..., f_k \text{ using the} \\ & \text{division algorithm of section 2 is } 0 \text{ for all } i, j \in \{1, ..., k\}, \\ F \cup \{r\} & \text{otherwise, where } r \text{ is some remainder as above, } r \neq 0. \end{cases}$$

Define $F^0 := F$ and $F^{m+1} = (F^m)^\dagger$. Then
- *(i) $(F^m) = (F)$ for all m*
- *(ii) For some m we have $F^m = F^{m+1}$ and F^m is a Gröbner basis of (F).*
  Explicitly we may choose m to be the number of monomials that are of $\deg_<$ at most $\max\{\deg_< f_1, \ldots, \deg_< f_k\}$ for the global monomial ordering $<$.

Proof. (i) is obvious since $S(f, g) \in (f, g)$ for all polynomials f, g.
(ii) We have $F^0 \subseteq F^1 \subseteq F^2 \subseteq ....$ If this chain is proper, then by 6.1 also the sequence of leading ideals $L(F^0) \subseteq L(F^1) \subseteq L(F^2) \subseteq ...$ is proper, which contradicts noetherianity of $K[X]$. For the explicit estimate of m let $\gamma = \max\{\deg_< f_1, \ldots, \deg_< f_k\}$. We first show that each polynomial $p \in F^i$ has $\deg_<$ at most γ. This is true for $F = F^0$. If it is true for F^i, then the remainder r that is added to get to F^{i+1} also has $\deg_<$ at most γ as follows from 5.3(i) and the degree estimate of r from the algorithm in 2. Hence $p \in F^i$ has $\deg_<$ at most γ. But now, 6.1 implies that it is only possible to add at most m successive remainders to F. Hence $F^m = F^{m+1}$.

Hence we have $F^m = F^{m+1}$ for some m which means that the remainder on division of $S(f, g)$ by F^m (listed in some order) using the division algorithm of section 2 is 0 for all $f, g \in F^m$. By 5.5, we know that F^m is a Gröbner basis. □

7. Reduced Gröbner bases and the reduction process for minimal Gröbner bases

Throughout we work with a global monomial ordering $<$.

7.1. **Lemma.** *Let G be a Gröbner bases of an ideal I of $K[X]$. If $g \in G$ such that $\mathrm{LT}(g) \in L(G \setminus \{g\})$, then also $G \setminus \{g\}$ is a Gröbner basis of I.*

Proof. We have to show that $L(G \setminus \{g\}) = L(G)$. We have $L(G) = (\mathrm{LT}(f) \mid f \in G) \subseteq (\mathrm{LT}(f) \mid f \in G \setminus \{g\}) + (\mathrm{LT}(g)) \subseteq (\mathrm{LT}(f) \mid f \in G \setminus \{g\}) = L(G \setminus \{g\})$. □

7.2. **Definition.** A **minimal Gröbner basis** of an ideal of $K[X]$ is a Gröbner basis of I with the properties

M1: $\mathrm{LC}(g) = 1$ for all $g \in G$ and
M2: $\mathrm{LT}(g) \notin L(G \setminus \{g\})$ for all $g \in G$.

By 7.1, every Gröbner basis contains a minimal Gröbner basis.

7.3. **Lemma.** *If G and G' are minimal Gröbner bases of I, then*

$$\{\mathrm{LT}(g) \mid g \in G\} = \{\mathrm{LT}(g') \mid g' \in G'\}.$$

Proof. By symmetry we only need to show $\mathrm{LT}(g) \in \{\mathrm{LT}(g') \mid g' \in G'\}$ for each $g \in G$. Since $\mathrm{LT}(g) \in L(I) = L(G')$ there is some $g' \in G'$ with $\mathrm{LT}(g') | \mathrm{LT}(g)$ (cf. 3.3). Since $\mathrm{LT}(g') \in L(I) = L(G)$ there is some $g_1 \in G$ with $\mathrm{LT}(g_1) | \mathrm{LT}(g')$. We get $\mathrm{LT}(g_1) | \mathrm{LT}(g)$. Since G is minimal, this can only be if $g = g_1$. Since $\mathrm{LC}(g) = \mathrm{LC}(g') = 1$, $\mathrm{LT}(g') | \mathrm{LT}(g)$ and $\mathrm{LT}(g) | \mathrm{LT}(g')$ implies $g = g' \in G'$. □

7.4. **Proposition.** (*Reduction process for minimal Gröbner bases*)
Let G be a minimal Gröbner basis of an ideal I of $K[X]$ and let $g \in G$. Let $g' \in K[X]$ such that

there are $q_h \in K[X]$ for $h \in G \setminus \{g\}$ with $\deg_< q_h h \le \deg_< g$ and

$$g = \sum_{h \in G \setminus \{g\}} q_h h + g'$$

(Note that such q_h and g' exists by the division algorithm of section 2).

Then also $(G \setminus \{g\}) \cup \{g'\}$ is a minimal Gröbner basis of I.

Proof. We may assume that $g' \neq g$. Certainly $G \cup \{g'\}$ is a Gröbner basis of I. We first show that $\mathrm{LT}(g) = \mathrm{LT}(g')$.

As $\deg_< q_h h \le \deg_< g$ for all $h \in G \setminus \{g\}$ we have $\deg_< g' \le \deg_g$. Moreover, since $\deg_< q_h h \le \deg_< g$, the monomial $\mathrm{LM}(g)$ can not occur in $q_h h$ for any $h \in G \setminus \{g\}$ (otherwise there would be monomials U, V, U occurring in q_h, V occurring in h such that $UV = \mathrm{LM}(g)$ - as $\deg_< q_h h \le \deg_< g$ this means that $UV = \mathrm{LM}(q_h h)$ so $V = \mathrm{LM}(h)$ divides $\mathrm{LM}(g)$ in contradiction to our assumption that G is a minimal Gröbner basis). Hence $\mathrm{LM}(g)$ occurs in g' and $\deg_< g' \le \deg_g$ implies $\mathrm{LT}(g') = \mathrm{LT}(g)$.

Since $\mathrm{LT}(g) = \mathrm{LT}(g')$ and $g \neq g'$ we have $\mathrm{LT}(g) \in L((G \cup \{g'\}) \setminus \{g\})$. Hence by 7.1, also $(G \cup \{g'\}) \setminus \{g\}$ is a Gröbner basis of I. As $g \neq g'$ we have $(G \cup \{g'\}) \setminus \{g\} = (G \setminus \{g\}) \cup \{g'\}$. Since $\mathrm{LT}(g) = \mathrm{LT}(g')$, we have

$$\{\mathrm{LT}(h) \mid h \in G\} = \{\mathrm{LT}(h') \mid h' \in (G \setminus \{g\}) \cup \{g'\}\}.$$

Hence by 7.3, $(G \setminus \{g\}) \cup \{g'\}$ is again a minimal Gröbner basis (any minimal Gröbner bases contained in $(G \setminus \{g\}) \cup \{g'\}$ must have the same leading terms as G). □

7.5. **Definition.** A **reduced Gröbner basis** of an ideal of $K[X]$ is a Gröbner basis of I with the properties

R1: $\mathrm{LC}(g) = 1$ for all $g \in G$ and
R2: For all $g \in G$, no monomial occurring in g lies in $L(G \setminus \{g\})$.

7.6. **Observation.** *If G, G' are minimal Gröbner bases of I, both containing $g \in K[X]$ and no monomial occurring in g lies in $L(G \setminus \{g\})$, then also no monomial occurring in g lies in $L(G' \setminus \{g\})$.*

Proof. By 7.3. □

7.7. **Theorem.** *Every ideal I of $K[X]$ has a unique (only depending on the global monomial ordering $<$) reduced Gröbner basis.*

Proof. We first show uniqueness. Let G, G' be reduced Gröbner bases of I. By symmetry we only need to show $G \subseteq G'$. Pick $g \in G$. Since G and G' are also minimal Gröbner bases of I there is some $g' \in G'$ with $\mathrm{LT}(g) = \mathrm{LT}(g')$ by 7.3. We claim that $g = g'$. Otherwise, as $g - g' \in I$, $\mathrm{LT}(g - g') \in L(G)$ and by 3.3, $\mathrm{LT}(g_1) | \mathrm{LT}(g - g')$ for some $g_1 \in G$. We have $g_1 \neq g$, since $\mathrm{LT}(g) = \mathrm{LT}(g')$, hence $\deg_< \mathrm{LT}(g - g') < \deg_< \mathrm{LT}(g)$ (recall that $<$ is compatible with $|$ by 1.4). Since G is a reduced Gröbner basis, $\mathrm{LT}(g_1) | \mathrm{LT}(g - g')$ and $g_1 \neq g$, $\mathrm{LM}(g - g')$ does not occur in g.

The same argument with interchanged role of G and G' shows that $\mathrm{LM}(g - g')$ does not occur in g', which contradicts $g - g' \neq 0$.

Hence we know that I has at most one reduced Gröbner basis and it remains to show that it actually has one. Let $G_0 = \{g_1, ..., g_k\}$ be a minimal Gröbner bases of I. Let g_1' be the remainder on division of g_1 by $G_0 \setminus \{g_1\}$ according to the division algorithm of section 2 and let $G_1 := \{g_1', g_2, ..., g_k\}$. Then no leading term of $g_2, ..., g_k$ divides any monomial occurring in g_1'. By 7.4, G_1 is again a minimal Gröbner bases of I. Hence G_1 is aminimal Gröbner bases of I such that condition R2 of 7.5 holds for g_1' and G_1.

Now we repeat the same argument for g_2 and G_1' instead of g_1 and G_0. We get a minimal Gröbner basis $G_2 := \{g_1', g_2', g_3, ..., g_k\}$ of I such that condition R2 of 7.5 holds for g_2' and G_2. By 7.6 applied to G_1, G_2 and g_1', condition R2 of 7.5 also holds for g_1' and G_2.

Continuing in this way, we obtain after k steps a Gröbner bases $G_k = \{g_1', ..., g_k'\}$ of I such that condition R2 of 7.5 holds for all $g_1', ..., g_k'$ and G_k. But this means, G_k is a reduced Gröbner bases of I. □

References

[GrePfi2008] Gert-Martin Greuel and Gerhard Pfister. A **Singular** introduction to commutative algebra. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX). 4

The University of Manchester, Department of Mathematics, Oxford Road, Manchester M13 9PL, UK

Email address: marcus.tressl@manchester.ac.uk