Buchberger's algorithm for computing Gröbner bases

In the previous Chapter, we saw how multivariate polynomial division behave and how it requires a monomial ordering. The main goal of this chapter is to introduce Gröbner bases, a set of generators of an multivariate polynomial ideal with powerful properties. In particular, we will see that the division algorithm behaves well with this kind of polynomials. Furthermore, Buchberger's algorithm for computing Gröbner bases is described.

1 Monomial ideals and Dickson's lemma

To go further, we start by restricting our study to some special ideals, which are called *monomial ideals*. As suggested by their names, those are ideals which admit a basis composed of monomials. Our goal is to identify if such ideals then admit a finite basis.

We start with the formal definition of monomial ideals.

Definition 1. *An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a* monomial ideal *if there exists a subset $S \subset \mathbb{N}^n$ such that all elements of I are of the form*

$$\sum_{\alpha \in S} q_\alpha \underline{x}^\alpha$$

where $q_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. In that case, we write $I = \langle \underline{x}^\alpha \mid \alpha \in S \rangle$.

For instance $\langle x_1^2, x_2^2 \rangle$ and $\langle x_1 x_2^3, x_1^2 x_2 \rangle$ are monomial ideals.

The following lemma characterizes those monomials which actually lie in a given monomial ideal by using divisibility.

Lemma 2. *Let $I = \langle \underline{x}^\alpha \mid \alpha \in S \rangle$ be a monomial ideal. Then, a monomial $\underline{x}^\beta$ lies in I if and only if $\underline{x}^\beta$ is divisible by $\underline{x}^\alpha$ for some $\alpha \in S$.*

Proof. Let $\beta = (\beta_1, \ldots, \beta_n)$ and $\underline{x}^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$.

Assume first that $\underline{x}^\beta$ is a multiple of some monomial $\underline{x}^\alpha$ with $\underline{x}^\alpha \in I$. Then, applying the definition of ideals, one immediately conclude that $\underline{x}^\beta \in I$.

Assume now that $\underline{x}^\beta \in I$. Then, there exist polynomials $(q_1, \dots, q_s) \subset \mathbb{K}[x_1, \dots, x_n]$ and $(\underline{x}^{\alpha(1)}, \dots, \underline{x}^{(\alpha_s)})$ in the set S of the statement, such that

$$\underline{x}^\beta = q_1 \, \underline{x}^{\alpha(1)} + \cdots + q_s \, \underline{x}^{\alpha(s)}.$$

Writing $q_i = \sum_j q_{i,j} \underline{x}^{\gamma(i,j)}$ one obtains

$$\underline{x}^\beta = \sum_{i,j} q_{i,j} \underline{x}^{\gamma(i,j)} \underline{x}^{\alpha(i)}.$$

Now, on the right-hand side, collecting terms of the same multi-degree, one obtains that every term is divisible by some $x^{\alpha(i)}$ (since they are in finite number). □

From the above lemma, one can deduce that the set of monomials in a monomial ideal are the ones in

$$\alpha + \mathbb{N} = \{\alpha + \gamma \mid \gamma \in \mathbb{N}$$

for all $\alpha \in S$.

The above lemma allows us solve the ideal membership problem for monomial ideals.

Lemma 3. *Let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be a monomial ideal and let $f \in \mathbb{K}[x_1, \dots, x_n]$. Then the following statements are equivalent:*

- *$f \in I$;*
- *Every term of f lies in I;*
- *f is a $\mathbb{K}$-linear combination of the monomials in I.*

Proof. The proof of the next lemma is left to the reader. □

Exercise 1

Prove the above lemma.

A consequence of the last statemnt of the above lemma is that a monomial ideal is uniquely determined by its monomials. We deduce the following corollary.

Corollary 4. *Let I and J be two monomial ideals. The following statements are equivalent:*

- *$I = J$;*
- *the set of monomials in I coincide with the set of monomials in J.*

We state now the main result of this paragraph. It establishes that monomial ideals in $\mathbb{K}[x_1, \dots, x_n]$ are finitely generated.

Theorem 5 (Dickson's lemma)**.** *Let $I = \langle \underline{x}^\alpha \mid \alpha \in S \rangle$ be a monomial ideal. Then there exists a* finite *subset S' of S such that $I = \langle \underline{x}^\alpha \mid \alpha \in S' \rangle$.*

In particular, I has a finite basis.

We will not study the proof of the above result. Despite this, observe how important it is: it establishes that every monomial ideal is finite and that one can find a finite monomial basis.

Observe that from this result, combined with previous lemmas, one obtains the following result which solves the ideal membership problem for monomial ideals.

Lemma 6. *Let $I = \langle \underline{x}^{\alpha(1)}, \ldots, \underline{x}^{\alpha(s)} \rangle$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and f be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. The polynomial f lies in I if and only if the remainder of the division of f by $[\underline{x}^{\alpha(1)}, \ldots, \underline{x}^{\alpha(s)}]$ is zero.*

Proof. The proof is left to the reader. □

Exercise 2

Write the formal proof of the above lemma.

Dickson's lemma can also be used to prove important properties of monomial orderings.

Corollary 7. *Let $\succ$ be a relation on $\mathbb{N}^n$ such that:*

(1) $\succ$ is a total ordering on $\mathbb{N}^n$;

(2) If $\alpha \succ \beta$ and $\gamma \in \mathbb{N}^n$, then $\alpha + \gamma \succ \beta + \gamma$.

Then $\succ$ is well-ordering if and only if $\alpha \succeq 0$ for all $\alpha \in \mathbb{N}^n$.

Proof. We start by assuming that $\succ$ is a monomial ordering. Then, $\mathbb{N}^n$ contains a smallest element for $\succ$, say α. We need to prove that $\alpha \succeq (0, \ldots, 0)$. Assume, by contradiction, that $(0, \ldots, 0) \succ \alpha$. Then, using (2), one deduces that $\alpha \succ 2\alpha$ which contradicts the fact that α is the smallest element of $\mathbb{N}^n$ for $\succ$.

We prove now that if $\succ$ is such that:

- $\succ$ is a total ordering on $\mathbb{N}^n$;
- If $\alpha \succ \beta$ and $\gamma \in \mathbb{N}^n$, then $\alpha + \gamma \succ \beta + \gamma$;
- and for any $\alpha \in \mathbb{N}^n$, $\alpha \succeq 0$;

then $\succ$ is a well-ordering, i.e. any non-empty subset A of $\mathbb{N}^n$ contains a least element of $\mathbb{N}^n$.

Take a non-empty subset A of $\mathbb{N}^n$ and consider the monomial ideal $I = \langle \underline{x}^{\alpha} \mid \alpha \in A \rangle$. By Dickson's lemma, there exists a finite subset A' of A such that $I = \langle \underline{x}^{\alpha} \mid \alpha \in A' \rangle$. Since A' is finite and $\succ$ is a total ordering, one can sort the monomials in A', i.e. we have $A' = \{\alpha(1), \ldots, \alpha(s)\}$ with

$$\alpha(s) \succ \cdots \succ \alpha(1).$$

We claim that $\alpha(1)$ is the smallest element in A. This is clear for monomials in A'. Take now $\alpha \in A \setminus A'$. Then, $\underline{x}^{\alpha} \in I$ and using Lemma 2, one deduces that $\underline{x}^{\alpha}$ is divisible by some $\underline{x}^{\alpha(i)}$ for

$1 \leqslant i \leqslant s$. We deduce that there exists $\gamma \in \mathbb{N}$ such that $\alpha = \alpha(i) + \gamma$. Since $\gamma \geq 0$ by assumption, using (2) again, one deduces that

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + (0, \ldots, 0) \geq \alpha(i).$$

Since $\alpha(i) > \alpha(1)$, we are done. □

Observe that using the result of the above lemma, one can rewrite the definition of monomial orderings as follows.

A relation $>$ of $\mathbb{N}^n$ is a monomial ordering if the following holds:

- $>$ is a total ordering on $\mathbb{N}^n$;
- If $\alpha > \beta$ and $\gamma \in \mathbb{N}^n$, then $\alpha + \gamma > \beta + \gamma$;
- and for any $\alpha \in \mathbb{N}^n$, $\alpha \geq 0$;

This makes much easier the task of checking if a given ordering is a monomial one.

We study now under which condition a basis of a monomial ordering is unique.

Proposition 8. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a monomial ideal. There exists $S = \{\underline{x}^{\alpha(1)}, \ldots, \underline{x}^{\alpha(s)}\}$ such that:*

- *S a monomial basis of I;*
- *for any (i, j) in $\{1, \ldots, s\}$ with $i \neq j$, $\underline{x}^{\alpha(i)}$ does not divide $\underline{x}^{\alpha(j)}$.*

Such a basis is unique. It is called a minimal basis *of I.*

Proof. We deduce from Dickson's lemma that I has a finite basis. Removing from this basis monomials which are divisible by the other ones, one obtains a minimal basis ; this shows the existence of a minimal basis.

We prove now uniqueness. Take two minimal bases for I, say $\alpha(1), \ldots, \alpha(s)$ and $\beta(1), \ldots, \beta(t)$. Since $\underline{x}^{\alpha(1)} \in I$, Lemma 2 implies that there exists $\beta(i)$ such that $\underline{x}^{\beta(i)}$ divides $\underline{x}^{\alpha(1)}$. Besides, $\underline{x}^{\beta(i)} \in I$ and we deduce, using again Lemma 2, that there exists $\alpha(j)$ such that $\underline{x}^{\alpha(j)}$ divides $\underline{x}^{\beta(i)}$. All in all, we obtain that $\underline{x}^{\alpha(j)}$ divides $\underline{x}^{\alpha(1)}$, which, by minimality of the basis, implies that $j = 1$. We deduce from that, that $\beta(i) = \alpha(1)$. Repeating the argumentation for all other elements of the basis $\beta(1), \ldots, \beta(t)$ ends the proof. □

Exercise 3

Give minimal monomial basis of $\langle x_1^2, x_1x_2, x_2^2\rangle$, $\langle x_1^3, x_1^3x_2, x_1^3x_2^2, x_2^2, x_2\rangle$.

Exercise 4

Prove that a monomial ideal in $\mathbb{K}[x_1]$ admits a unique generator.
What is the maximal number of generators of a monomial ideal in $\mathbb{K}[x_1, x_2]$? Give an example.

2 Hilbert basis theorem and Gröbner bases

Now, we tackle the problem of establishing that any ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ is finitely generated, i.e. there exists $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$. In other words, any ideal of $\mathbb{K}[x_1, \ldots, x_n]$ admits a finite basis.

This generalizes (partly) Dickson's lemma to arbitrary ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and we will actually rely on it.

A key tool for doing that is the use of monomial orderings that we introduced previously. Indeed, any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ admits a *unique* leading term. Hence, given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, one is able to define the ideal of its leading terms and rely on the study of monomial ideals.

Definition 9. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal which is not $\{0\}$ and $\succ$ be a monomial ordering for $\mathbb{K}[x_1, \ldots, x_n]$.*

- *We denote by $\mathsf{LT}(I)$ the set of leading terms of non-zero elements of I*
- *We denote by $\langle \mathsf{LT}(I) \rangle$ the ideal generated by the elements of $\mathsf{LT}(I)$.*

We emphasize a fact that is important for the sequel. Given $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$, and $I = \langle f_1, \ldots, f_s \rangle$, $\langle \mathsf{LT}(I) \rangle$ and $\langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_s) \rangle$ may be different ideals.

Exercise 5

Prove that $\langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_s) \rangle$ is contained in $\langle \mathsf{LT}(I) \rangle$.

Example 10. Let $I = \langle f_1, f_2 \rangle$ with $f_1 = x_1^3 - 2x_1x_2$ and $f_2 = x_1^2x_2 - 2x_2^2 + x_1$ and use the grlex ordering in $\mathbb{K}[x_1, x_2]$. Observe that

$$x_1 f_2 - x_2 f_1 = x_1^2.$$

We deduce that $x_1^2 \in I$ and then $x_1^2 \in \mathsf{LT}(I)$. However, x_1^2 is not divisible by $\mathsf{LT}(f_1) = x_1^3$ or $\mathsf{LT}(f_2) = x_1^2x_2$. Hence by Lemma 2, we deduce that $x_1^2 \notin \langle \mathsf{LT}(f_1), \mathsf{LT}(f_2) \rangle$.

This example is rather instructive. By performing algebraic combinations of a given generating set, one can "discover" new algebraic relations whose leading terms do not belong to the ideal generated by the leading terms of the input polynomials.

Exercise 6

Show that, in the previous example, $\langle x_1^2, x_1x_2, x_2^2 \rangle \subseteq \langle \mathsf{LT}(I) \rangle$.

Proposition 11. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ which is not $\{0\}$. The following holds.*

- *$\langle \mathsf{LT}(I) \rangle$ is a monomial ideal;*

- *There are $g_1, \dots, g_s$ in I such that $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s) \rangle$.*

Proof. We start with the first statement. Recall that $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g) \mid g \in I \rangle$. Observe that, for any polynomial g, $\mathsf{LT}(g)$ and $\mathsf{LM}(g)$ differ by a constant factor in $\mathbb{K}$. Hence, any polynomial that is an algebraic combination of a finite subset of $\{\mathsf{LT}(g) \mid g \in I\}$ is an algebraic combination of a finite subset of $\{\mathsf{LM}(g) \mid g \in I\}$. Hence, one has $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LM}(g) \mid g \in I \rangle$.

We prove now the second statement. We have $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g) \mid g \in I \rangle$. Applying Dickson's lemma, one deduces that there exists a finite subset $\{\mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s)\}$ of $\{LT(g) \mid g \in I\}$ which generates I. Our claim follows. □

We can now prove the so-called Hilbert basis theorem. We will see that the multivariate division algorithm plays a key role for its proof (as for the univariate case where we were using the Euclidean division).

Theorem 12. *Let $I \subset \mathbb{K}[x_1, \dots, x_n]$. It admits a finite basis $g_1, \dots, g_s$, i.e. $I = \langle g_1, \dots, g_s \rangle$.*

Besides, when fixing a monomial ordering $\succ$ on $\mathbb{K}[x_1, \dots, x_n]$, one can find such a basis such that

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s) \rangle.$$

Proof. The easiest case is when $I = \{0\}$; indeed we take trivially $\{0\}$ as a generating set.

Assume now that I contains non-zero polynomials. We choose first a monomial ordering $\succ$ and consider the monomial ideal $\langle \mathsf{LT}(I) \rangle$. Using Proposition 11, we deduce that there exists $(g_1, \dots, g_s)$ of I such that

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s) \rangle.$$

We prove below that we also have $I = \langle g_1, \dots, g_s \rangle$.

Since, by construction, each polynomial g_i lies in I, one has $\langle g_1, \dots, g_s \rangle \subset I$. We prove now the reverse inclusion and take $f \in I$. Applying the division algorithm on f and $(g_1, \dots, g_s)$, one obtains that

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

with $q_i \in \mathbb{K}[x_1, \dots, x_n]$ and no term of r is divisible by any of the terms $\mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s)$. If $r = 0$, we are done ; one can conclude that $f \in \langle g_1, \dots, g_s \rangle$.

If $r \neq 0$, then, since $r \in I$, we have $\mathsf{LT}(r) \in \langle \mathsf{LT}(I) \rangle$. Using Lemma 2, we deduce that $\mathsf{LT}(r)$ is divisible by one of the terms $\mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s)$ which is a contradiction. □

We can now define Gröbner bases.

Definition 13. *Let $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \dots, x_n]$ and let $I \subset \mathbb{K}[x_1, \dots, x_n]$ which is not $\{0\}$.*

A finite subset $G = \{g_1, \dots, g_s\} \subset \mathbb{K}[x_1, \dots x_n]$ is said to be a Gröbner basis if

- $G \subset I$
- $\langle \mathsf{LT}(g_1), \dots, \mathsf{LT}(g_s) \rangle = \langle \mathsf{LT}(I) \rangle$.

Further, by convention, we set $\langle \emptyset \rangle = \{0\}$ and then $\emptyset$ is a Gröbner basis for the ideal $\{0\}$. Before studying properties of Gröbner bases, let us start by giving some examples.

Exercise 7

Prove that a subset $\{g_1, \ldots, g_s\} \subset I$ is a Gröbner basis of I (w.r.t. to some monomial ordering) if for any $f \in I$, $\mathsf{LT}(f)$ is divisible by one term in $\{\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)\}$.

Corollary 14. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Then there exists a Gröbner basis for $(I, \succ)$. Moreover, any Gröbner basis for $(I, \succ)$ is a basis for I.*

Proof. Following the construction in the proof of Theorem 12, one obtains the existence of a Gröbner basis for $(I, \succ)$. Still using the proof of Theorem 12, note that we were able to prove that if $\langle \mathsf{LT}(G) \rangle = \langle \mathsf{LT}(I) \rangle$ with $G \subset I$, then $\langle G \rangle = I$. □

Remark. Note that the proof of Corollary 14 is not constructive ; we cannot derive an algorithm from it. We will see later how to compute Gröbner bases.

Consider, as we did before in Example 10, the polynomials $f_1 = x_1^3 - 2x_1x_2$ and $f_2 = x_1^2x_2 - 2x_2^2 + x_1$, $I = \langle f_1, f_2 \rangle$ and the *grlex* ordering $\succ_{grlex}$. We established that $x_1^2 \notin \langle \mathsf{LT}(I) \rangle$. Then, (f_1, f_2) is not a Gröbner basis for $(I, \succ_{grlex})$.

Exercise 8

Consider the linear polynomials $f_1 = x_1 + x_2 + x_3$ and $f_2 = x_2 - x_3$, the ideal $I = \langle f_1, f_2 \rangle$ and the *lex* ordering $\succ_{lex}$. What is $\langle \mathsf{LT}(I) \rangle$? What is a Gröbner basis for $(I, \succ_{lex})$ and how is it related with Gaussian elimination?

Finally, let us emphasize one consequence of the Hilbert basis theorem on polynomial ideals. Consider an ascending chain of ideals, which is a sequence of nested ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

As an example, one can consider the sequence

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \cdots \subseteq \langle x_1, \ldots, x_n \rangle.$$

Observe that when trying to augment the last ideal, only two situations can occur:

- either one adds a polynomial in $\langle x_1, \ldots, x_n \rangle$; note that these are polynomials with a constant zero coefficient in $\mathbb{K}$;
- or we add a polynomial f with a *non* constant zero coefficient in $\mathbb{K}$ and then one proves easily that $\langle x_1, \ldots, x_n, f \rangle = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$.

Exercise 9

Use the division algorithm in $\mathbb{K}[x_1, \ldots, x_n]$ to prove the above facts.

This example illustrates that when considering sequences of nested ideals, at some point, the largest ideal stabilizes.

Theorem 15. *Let a sequence of nested ideals*

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

in $\mathbb{K}[x_1, \ldots, x_n]$. *Then, there exists* $k \geqslant 0$ *such that*

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

Proof. Assume first that $I = \cup_{i=0}^{\infty} I_i$ is an ideal (we will prove this claim further). By the Hilbert basis theorem, there is a finite set of generators, say $f_1, \ldots, f_s$ for I ; in other words, $I = \langle f_1, \ldots, f_s \rangle$. Since each generator lies in some I_i ; take the smallest k such that I_k contains all the generators $f_1, \ldots, f_s$. Note that $I \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$. But since I is the union of all the I_i's we have $I_k \subseteq I_{k+1} \subseteq \cdots \subseteq I$ which ends the proof.

It remains to prove that I is an ideal. Since $0 \in I_i$ for any i, we deduce that $0 \in I$. Now take f and g in I. Then, there exist i and j such that $f \in I_i$ and $g \in I_j$. Without loss of generality, assume that $j \geqslant i$. Since $I_i \subseteq I_j$ by assumption, we deduce that $f \in I_j$ as well and then $f + g \in I_j$. Therefore, $f + g \in I$. Finally, take $h \in \mathbb{K}[x_1, \ldots, x_n]$ and $f \in I$. Then, there exists i such that $f \in I_i$ which implies that $hf \in I_i$ and we conclude that $hf \in I$. This finishes the proof. □

3 Properties of Gröbner bases

We have shown that all ideals of $\mathbb{K}[x_1, \ldots, x_n]$ admit a Gröbner basis (once a monomial ordering has been chosen). An important question now is to obtain a criterion which enables us to decide if a given finite set of polynomials if a Gröbner basis. This criterion is called Buchberger's criterion.

We start with some properties of Gröbner bases.

Proposition 16. *Let* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal,* $\succ$ *be a monomial ordering and let* $G = (g_1, \ldots, g_s)$ *be a Gröbner basis for* $I, \succ$.

Take $f \in \mathbb{K}[x_1, \ldots, x_n]$. *There exists a* unique $r \in \mathbb{K}[x_1, \ldots, x_n]$ *such that:*

(a) No term of r *is divisible by any of* $\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)$;

(b) There exists $g \in I$ *such that* $f = g + r$.

Also, r *is the remainder of the division of* f *by* G *for any ordering on the elements of* G *used during the division algorithm.*

Proof. Using the division algorithm on input f and $[g_1, \ldots, g_s]$ one obtains that there exist $(q_1, \ldots, q_s)$ and r such that

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

with r having no term divisible by any of the $\mathsf{LT}(g_i)$'s (for $1 \leqslant i \leqslant s$). Taking $g = q_1 g_1 + \cdots + q_s g_s$ yields the existence statement.

Now, we prove uniqueness. Assume, by contradiction, that there exist also g' and r' such that $g' \in I$ and no term of r' is divisible by one of the terms $\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)$. Then, we have

$$r - r' = g' - g$$

from which we deduce that $r - r'$ lies in I and then $\mathsf{LT}(r - r') \in \langle \mathsf{LT}(I) \rangle$. Remark now that $\mathsf{LT}(r - r')$ is also not divisible by any of the terms $\mathsf{LT}(g_i)$ (for $1 \leqslant i \leqslant s$). We deduce by Lemma 2 that $\mathsf{LT}(r - r') \notin \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle$ and then

$$\langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle \notin \langle \mathsf{LT}(I) \rangle.$$

This contradicts the fact that $G = (g_1, \ldots, g_s)$ is a Gröbner basis for $(I, \succ)$. □

The remainder r is also called *normal form* of f modulo G. Note that despite the fact that the remainder is unique, the quotients $(q_1, \ldots, q_s)$ arising during the division algorithm are not unique and actually depend on how the elements of G are listed and used during that algorithm.

Corollary 17. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal, $\succ$ be a monomial ordering and let $G = (g_1, \ldots, g_s)$ be a Gröbner basis for $I, \succ$ and let $f \in \mathbb{K}[x_1, \ldots, x_n]$.*

Then $f \in I$ if and only if the normal form of f modulo G is the zero polynomial.

Proof. We already observed that if the remainder r of the division of f by G is 0, then $f \in \langle G \rangle = I$. Assume now that $f \in I$ and take g, r as in Proposition 22. Since r is unique it is the zero polynomial (this is obvious taking $g = f$). □

Observe that, once we *know* a Gröbner basis for an ideal I, the above result gives us an algorithmic way to decide if a given polynomial f lies in I. Hence, once we will know how to *compute* Gröbner bases, we will have solved completely the ideal membership problem.

Definition 18. *Let $F = (f_1, \ldots, f_s)$ be an ordered list in $\mathbb{K}[x_1, \ldots, x_n]$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$. We denote by $\overline{f}^F$ the remainder of the multivariate division of f by F.*

Note that when G is a Gröbner basis, $\overline{f}^G$ does not depend on the way the elements of G are sorted.

Our goal is now to identify how to decide if a given set G in $\mathbb{K}[x_1, \ldots, x_n]$ (with a given monomial ordering $\succ$) is a Gröbner basis.

Recall that, from the definition of Gröbner bases (see Definition 13), a finite set $F = (f_1, \ldots, f_s)$ of polynomials is *not* a Gröbner basis if by taking algebraic combinations of it, we obtain a new polynomial whose leading term does not lie in $\langle \mathsf{LT}(\langle F \rangle) \rangle = \langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_s) \rangle$.

This can occur for instance when taking polynomials of the following form:

$$a\, \underline{x}^{\alpha} f_i - b\, \underline{x}^{\beta} f_j$$

choosing a, α and b, β in a way that cancels the leading terms of f_i or f_j. This is what happened in most of the pathological examples we already studied. This leads us to consider the following definition.

Definition 19. *Let f and g be in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$.*

- *If* $\mathsf{multidegree}(f) = \alpha$ *and* $\mathsf{multidegree}(g) = \beta$, *then take* $\gamma = (\gamma_1, \ldots, \gamma_n)$ *with* $\gamma_i = \max(\alpha_i, \beta_i)$ *for* $1 \leqslant i \leqslant n$.

  We call $\underline{x}^\gamma$ *the* least common multiple *of* $LM(f)$ *and* $LM(g)$ *and we denote it by* $lcm(LM(f), LM(g))$.

- *The S-*polynomial *of f and g is the combination*

$$S(f,g) = \frac{x^\gamma}{\mathsf{LT}(f)} f - \frac{x^\gamma}{\mathsf{LT}(g)} g.$$

For example, let us take $f = x_1^3 x_2^2 - x_1^2 x_2^3 + x_1$ and $g = 3x_1^4 x_2 + x_2^2$ in $\mathbb{Q}[x_1, x_2]$ with the grlex ordering. Then $\gamma = (4, 2)$ and

$$\begin{aligned} S(f,g) &= \frac{x_1^4 x_2^2}{x_1^3 x_2^2} f - \frac{x_1^4 x_2^2}{3x_1^4 x_2} g \\ &= x_1 f - \frac{1}{3} x_2 g \\ &= -x_1^3 x_2^3 + x_1^2 - \frac{1}{3} x_2^3. \end{aligned}$$

Lemma 20. *Let $(p_1, \ldots, p_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ with* $\mathsf{multidegree}(p_i) = \delta \in \mathbb{N}^n$.
If $\sum_{i=1}^s p_i$ has multidegree less than δ then there exist $c_{i,j}$ in $\mathbb{K}$ for $1 \leqslant i < j \leqslant s$ such that

$$\sum_{i=1}^{s} p_i = \sum_{1 \leqslant i < j \leqslant s} c_{i,j}\, S(p_i, p_j)$$

Proof. Let $c_i = \mathsf{LC}(p_i)$ so that $c_i \underline{x}^\delta$ is the leading term of p_i (recall that all the p_i's have the same multi-degree δ by assumption). Since the multi-degree of the sum $\sum_{i=1}^s p_i$ is less than the multi-degree δ we deduce that

$$c_1 + \cdots + c_s = 0.$$

Observe now that since the p_i's have the same leading monomial, we have

$$S(p_i, p_j) = \frac{1}{c_j} p_i - \frac{1}{c_i} p_j.$$

Hence, we have

$$\sum_{i=1}^{s-1} c_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} - \frac{c_1 + \cdots + c_{s-1}}{c_s} p_s.$$

Using $c_1 + \cdots + c_{s-1} = -c_s$, we deduce that

$$\sum_{i=1}^{s-1} c_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} + p_s.$$

It remains to prove that $S(p_i, p_j)$ has multi-degree less than δ. This is trivial from the relation $S(p_i, p_j) = \frac{1}{c_j} p_i - \frac{1}{c_i} p_j$ that we already observed. □

Theorem 21 (Buchberger's criterion)**.** *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$.*

Let $G = (g_1, \ldots, g_s)$ be a basis I. Then G is a Gröbner basis for I, $\succ$ if and only if for all $1 \leqslant i < j \leqslant s$, $\overline{S(g_i, g_j)}^G = 0$.

Proof. We trivially have $S(g_i, g_j) \in I$. Then, since G is a Gröbner basis, the remainder of the division of $S(g_i, g_j)$ by G is unique and 0 (Corollary 23).

Now, we assume that $\overline{S(g_i, g_j)}^G = 0$ for all $1 \leqslant i < j \leqslant s$ and we will prove that this implies that G is a Gröbner basis for $I = \langle G \rangle$ (and the monomial ordering used for the division algorithm and the S-polynomial.

To prove that G is a Gröbner basis, we will prove that if we take $f \in I = \langle G \rangle$, then $\mathsf{LT}(f) \in \langle \mathsf{LT}(G) \rangle$.

First, since $f \in \langle G \rangle$, there exists a sequence $(q_1, \ldots, q_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that

$$f = q_1 g_1 + \cdots + q_s g_s.$$

Using Lemma **??**, we deduce that

$$\mathsf{multidegree}(f) \leqslant \max(\mathsf{multidegree}(q_i g_i) \mid q_i g_i \neq 0).$$

Let δ denote $\max(\mathsf{multidegree}(q_i g_i) \mid q_i g_i \neq 0)$. Since $\succ$ is a well-ordering, amongst all possible δ, there exists a minimal one. Recall that we have $\mathsf{multidegree}(f) \leqslant \delta$.

When there is equality, one deduces that for some i, $\mathsf{LT}(f) = \mathsf{LT}(q_i g_i) = \mathsf{LT}(q_i)\mathsf{LT}(g_i)$ and then $\mathsf{LT}(f)$ is divisible by $\mathsf{LT}(g_i)$ and we can conclude that $\mathsf{LT}(f) \in \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle$. Note that at this stage, we did not use $\overline{S(g_i, g_j)}^G = 0$.

But it remains to consider the situation where $\mathsf{multidegree}(f) \prec \delta$. The proof strategy is then to use $\overline{S(g_i, g_j)}^G = 0$ to contradict the minimality of δ.

Write

$$\begin{aligned} f &= \sum_{\mathsf{multidegree}(q_i g_i) = \delta} q_i g_i + \sum_{\mathsf{multidegree}(q_i g_i) \prec \delta} q_i g_i \\ &= \sum_{\mathsf{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i + \sum_{\mathsf{multidegree}(q_i g_i) = \delta} (\mathsf{LT}(q_i) - q_i) g_i \sum_{\mathsf{multidegree}(q_i g_i) \prec \delta} q_i g_i \end{aligned}$$

Note that all terms in the second and third sum in the right-hand side of the above equality have multi-degree less than δ.

Observe that the sum $\sum_{\mathsf{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i$ satisfies the assumptions of Lemma 26 (taking $p_i = q_i g_i$). Using that Lemma, one deduces that

$$\sum_{\mathsf{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i = \sum c_{i,j} S(p_i, p_j)$$

with $c_{i,j} \in \mathbb{K}$. One can easily establish that

$$S(p_i, p_j) = \underline{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)$$

for $\underline{x}^{\gamma_{i,j}} = lcm(\mathsf{LM}(g_i), \mathsf{LM}(g_j))$ since $p_i = q_i g_i$ for all i. We deduce that

$$\sum_{\text{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i = \sum c_{i,j}\, \underline{x}^{\delta - \gamma_{i,j}}\, S(g_i, g_j).$$

Now we use $\overline{S(g_i, g_j)}^{G} = 0$. From the division algorithm, we deduce that

$$S(g_i, g_j) = \sum_{\ell} h_\ell g_\ell$$

with $h_\ell \in \mathbb{K}[x_1, \ldots, x_n]$ and

$$\text{multidegree}(h_\ell g_\ell) \preceq \text{multidegree}(S(g_i, g_j)) \text{ for } h_\ell g_\ell \neq 0.$$

Observe also that $h_\ell g_\ell \neq 0$

$$\text{multidegree}(\underline{x}^{\delta - \gamma_{i,j}} h_\ell g_\ell) \preccurlyeq \text{multidegree}(\underline{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)) \prec \delta$$

since $\mathsf{LT}(S(g_i, g_j)) \prec lcm(\mathsf{LM}(g_i), \mathsf{LM}(g_j)) = \underline{x}^{\gamma_{i,j}}$ (you may formally prove this fact).

Finally, we deduce that $\sum_{\text{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i$ is a linear combination of the polynomials $\underline{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)$ which satisfy the above relations ; in particular they can be written as algebraic combinations of the g_j's, say $\tilde{h}_j g_j$ with $\text{multidegree}(\tilde{h}_j g_j) \prec \delta$. Substituting this in the formula

$$f = \sum_{\text{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i + \sum_{\text{multidegree}(q_i g_i) = \delta} (\mathsf{LT}(q_i) - q_i) g_i \sum_{\text{multidegree}(q_i g_i) \prec \delta} q_i g_i$$

yields a writing of f as an algebraic combination of the g_j's where all terms have multidegree less than δ. This is a contradiction. □

Let us illustrate how to use Buchberger's criterion.

Consider the ideal $\langle x_2 - x_1^2, x_3 - x_1^2 \rangle$ in $\mathbb{C}[x_1, x_2, x_3]$. We show now how to use Buchberger's criterion to prove that $G = (x_2 - x_1^2, x_3 - x_1^2)$ is a Gröbner basis considering the lexicographical ordering with $x_2 > x_3 > x_1$.

Consider the S-polynomial

$$\begin{aligned} S(x_2 - x_1^2, x_3 - x_1^2) &= \frac{x_2 x_3}{x_2}(x_2 - x_1^2) - \frac{x_2 x_3}{x_3}(x_3 - x_1^3) \\ &= -x_3 x_1^2 + x_2 x_1^3. \end{aligned}$$

We next use the division algorithm and compute the normal form of $-x_3 x_1^2 + x_2 x_1^3$ modulo G. One finds that

$$-x_3 x_1^2 + x_2 x_1^3 = x_1^3(x_2 - x_1^2) + (-x_1^2)(x_3 - x_1^3) + 0.$$

Hence, the remainder is 0 and our claim follows.

Exercise 10

Is the above set G a Gröbner basis when considering the grevlex ideal with $x_1 \succ x_2 \succ x_3$?

Exercise 11

Show that if $g_1, \ldots, g_n \in \mathbb{K}[x_1, \ldots, x_n]$ are such that $\mathsf{LT}(g_i) = x_i^{\alpha_i}$ with $\alpha_i > 0$, then $g_1, \ldots, g_n$ is a

Exercise 12

Using the Buchberger criterion, design an algorithm which takes as input a finite polynomial family in $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering $\succ$, and decides whether G is a Gröbner basis w.r.t. $\succ$.
Analyze the complexity of such an algorithm.

Buchberger's criterion is also called the S-pair criterion. Recall that it is the main ingredient which alllows us to determine if given a finite polynomial subset of $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering, this polynomial subset is a Gröbner basis (w.r.t. the monomial ordering under consideration).

We see now that it is also the main ingredient of Buchberger's algorithm which, given as input a finite polynomial subset F in $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering $\succ$, computes a Gröbner basis for $\langle F \rangle$ w.r.t. $\succ$.

Exercise 13

Let f and g in $\mathbb{K}[x_1, \ldots, x_n]$ and $\underline{x}^\alpha$ and $\underline{x}^\beta$ be monomials. Prove that

$$S(\underline{x}^\alpha f, \underline{x}^\beta g) = \underline{x}^\gamma S(f, g)$$

with $\underline{x}^\gamma = \frac{lcm(\underline{x}^\alpha \mathsf{LM}(f), \underline{x}^\beta \mathsf{LM}(g))}{lcm(\mathsf{LM}(f), \mathsf{LM}(g))}$. Prove that $\underline{x}^\gamma$ is a monomial.

4 Properties of Gröbner bases

We have shown that all ideals of $\mathbb{K}[x_1, \ldots, x_n]$ admit a Gröbner basis (once a monomial ordering has been chosen). An important question now is to obtain a criterion which enables us to decide if a given finite set of polynomials if a Gröbner basis. This criterion is called Buchberger's criterion.

We start with some properties of Gröbner bases.

Proposition 22. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal, $\succ$ be a monomial ordering and let $G = (g_1, \ldots, g_s)$ be a Gröbner basis for $I, \succ$.*

Take $f \in \mathbb{K}[x_1, \ldots, x_n]$. There exists a unique *$r \in \mathbb{K}[x_1, \ldots, x_n]$ such that:*

(a) No term of r is divisible by any of $\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)$;

(b) There exists $g \in I$ such that $f = g + r$.

Also, r is the remainder of the division of f by G for any ordering on the elements of G used during the division algorithm.

Proof. Using the division algorithm on input f and $[g_1, \ldots, g_s]$ one obtains that there exist $(q_1, \ldots, q_s)$ and r such that

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

with r having no term divisible by any of the $\mathsf{LT}(g_i)$'s (for $1 \leqslant i \leqslant s$). Taking $g = q_1 g_1 + \cdots + q_s g_s$ yields the existence statement.

Now, we prove uniqueness. Assume, by contradiction, that there exist also g' and r' such that $g' \in I$ and no term of r' is divisible by one of the terms $\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)$. Then, we have

$$r - r' = g' - g$$

from which we deduce that $r - r'$ lies in I and then $\mathsf{LT}(r - r') \in \langle \mathsf{LT}(I) \rangle$. Remark now that $\mathsf{LT}(r - r')$ is also not divisible by any of the terms $\mathsf{LT}(g_i)$ (for $1 \leqslant i \leqslant s$). We deduce by Lemma 2 that $\mathsf{LT}(r - r') \notin \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle$ and then

$$\langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle \notin \langle \mathsf{LT}(I) \rangle.$$

This contradicts the fact that $G = (g_1, \ldots, g_s)$ is a Gröbner basis for $(I, \succ)$. □

The remainder r is also called *normal form* of f modulo G. Note that despite the fact that the remainder is unique, the quotients $(q_1, \ldots, q_s)$ arising during the division algorithm are not unique and actually depend on how the elements of G are listed and used during that algorithm.

Corollary 23. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal, $\succ$ be a monomial ordering and let $G = (g_1, \ldots, g_s)$ be a Gröbner basis for $I, \succ$ and let $f \in \mathbb{K}[x_1, \ldots, x_n]$.*

Then $f \in I$ if and only if the normal form of f modulo G is the zero polynomial.

Proof. We already observed that if the remainder r of the division of f by G is 0, then $f \in \langle G \rangle = I$. Assume now that $f \in I$ and take g, r as in Proposition 22. Since r is unique it is the zero polynomial (this is obvious taking $g = f$). □

Observe that, once we *know* a Gröbner basis for an ideal I, the above result gives us an algorithmic way to decide if a given polynomial f lies in I. Hence, once we will know how to *compute* Gröbner bases, we will have solved completely the ideal membership problem.

Definition 24. *Let $F = (f_1, \ldots, f_s)$ be an ordered list in $\mathbb{K}[x_1, \ldots, x_n]$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$. We denote by $\overline{f}^F$ the remainder of the multivariate division of f by F.*

Note that when G is a Gröbner basis, $\overline{f}^G$ does not depend on the way the elements of G are sorted.

Our goal is now to identify how to decide if a given set G in $\mathbb{K}[x_1, \ldots, x_n]$ (with a given monomial ordering $\succ$) is a Gröbner basis.

Recall that, from the definition of Gröbner bases (see Definition 13), a finite set $F = (f_1, \ldots, f_s)$ of polynomials is *not* a Gröbner basis if by taking algebraic combinations of it, we obtain a new polynomial whose leading term does not lie in $\langle \mathsf{LT}(\langle F \rangle) \rangle = \langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_s) \rangle$.

This can occur for instance when taking polynomials of the following form:

$$a\, \underline{x}^{\alpha} f_i - b\, \underline{x}^{\beta} f_j$$

choosing a, α and b, β in a way that cancels the leading terms of f_i or f_j. This is what happend in most of the pathological examples we already studied. This leads us to consider the following definition.

Definition 25. *Let f and g be in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$.*

- *If* multidegree$(f) = \alpha$ *and* multidegree$(g) = \beta$, *then take $\gamma = (\gamma_1, \ldots, \gamma_n)$ with $\gamma_i = \max(\alpha_i, \beta_i)$ for $1 \leqslant i \leqslant n$.*

  We call $\underline{x}^{\gamma}$ the least common multiple *of $LM(f)$ and $LM(g)$ and we denote it by $lcm(LM(f), LM(g))$.*

- *The S-*polynomial *of f and g is the combination*

$$S(f,g) = \frac{x^{\gamma}}{\mathsf{LT}(f)} f - \frac{x^{\gamma}}{\mathsf{LT}(g)} g.$$

For example, let us take $f = x_1^3 x_2^2 - x_1^2 x_2^3 + x_1$ and $g = 3x_1^4 x_2 + x_2^2$ in $\mathbb{Q}[x_1, \ldots, x_2]$ with the grlex ordering. Then $\gamma = (4, 2)$ and

$$\begin{aligned} S(f,g) &= \frac{x_1^4 x_2^2}{x_1^3 x_2^2} f - \frac{x_1^4 x_2^2}{3x_1^4 x_2} g \\ &= x_1 f - \frac{1}{3} x_2 g \\ &= -x_1^3 x_2^3 + x_1^2 - \frac{1}{3} x_2^3. \end{aligned}$$

Lemma 26. *Let $(p_1, \ldots, p_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ with* multidegree$(p_i) = \delta \in \mathbb{N}^n$.

If $\sum_{i=1}^{s} p_i$ has multidegree less than δ then there exist $c_{i,j}$ in $\mathbb{K}$ for $1 \leqslant i < j \leqslant s$ such that

$$\sum_{i=1}^{s} p_i = \sum_{1 \leqslant i < j \leqslant s} c_{i,j}\, S(p_i, p_j)$$

Proof. Let $c_i = \mathsf{LC}(p_i)$ so that $c_i \underline{x}^{\delta}$ is the leading term of p_i (recall that all the p_i's have the same multi-degree δ by assumption). Since the multi-degree of the sum $\sum_{i=1}^{s} p_i$ is less than the multi-degree δ we deduce that

$$c_1 + \cdots + c_s = 0.$$

Observe now that since the p_i's have the same leading monomial, we have

$$S(p_i, p_j) = \frac{1}{c_j} p_i - \frac{1}{c_i} p_j.$$

Hence, we have

$$\sum_{i=1}^{s-1} c_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} - \frac{c_1 + \cdots + c_{s-1}}{c_s} p_s.$$

Using $c_1 + \cdots + c_{s-1} = -c_s$, we deduce that

$$\sum_{i=1}^{s-1} c_i S(p_i, p_s) = p_1 + \cdots + p_{s-1} + p_s.$$

It remains to prove that $S(p_i, p_j)$ has multi-degree less than δ. This is trivial from the relation $S(p_i, p_j) = \frac{1}{c_j} p_i - \frac{1}{c_i} p_j$ that we already observed. □

Theorem 27 (Buchberger's criterion)**.** *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$.*

Let $G = (g_1, \ldots, g_s)$ be a basis I. Then G is a Gröbner basis for I, $\succ$ if and only if for all $1 \leqslant i < j \leqslant s$, $\overline{S(g_i, g_j)}^G = 0$.

Proof. We trivially have $S(g_i, g_j) \in I$. Then, since G is a Gröbner basis, the remainder of the division of $S(g_i, g_j)$ by G is unique and 0 (Corollary 23).

Now, we assume that $\overline{S(g_i, g_j)}^G = 0$ for all $1 \leqslant i < j \leqslant s$ and we will prove that this implies that G is a Gröbner basis for $I = \langle G \rangle$ (and the monomial ordering used for the division algorithm and the S-polynomial.

To prove that G is a Gröbner basis, we will prove that if we take $f \in I = \langle G \rangle$, then $\mathsf{LT}(f) \in \langle \mathsf{LT}(G) \rangle$.

First, since $f \in \langle G \rangle$, there exists a sequence $(q_1, \ldots, q_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that

$$f = q_1 g_1 + \cdots + q_s g_s.$$

Using Lemma **??**, we deduce that

$$\mathsf{multidegree}(f) \leqslant \max(\mathsf{multidegree}(q_i g_i) \mid q_i g_i \neq 0).$$

Let δ denote $\max(\mathsf{multidegree}(q_i g_i) \mid q_i g_i \neq 0)$. Since $\succ$ is a well-ordering, amongst all possible δ, there exists a minimal one. Recall that we have $\mathsf{multidegree}(f) \leqslant \delta$.

When there is equality, one deduces that for some i, $\mathsf{LT}(f) = \mathsf{LT}(q_i g_i) = \mathsf{LT}(q_i)\mathsf{LT}(g_i)$ and then $\mathsf{LT}(f)$ is divisible by $\mathsf{LT}(g_i)$ and we can conclude that $\mathsf{LT}(f) \in \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle$. Note that at this stage, we did not use $\overline{S(g_i, g_j)}^G = 0$.

But it remains to consider the situation where $\mathsf{multidegree}(f) \prec \delta$. The proof strategy is then to use $\overline{S(g_i, g_j)}^G = 0$ to contradict the minimality of δ.

Write

$$\begin{aligned} f &= \sum_{\mathsf{multidegree}(q_i g_i) = \delta} q_i g_i + \sum_{\mathsf{multidegree}(q_i g_i) < \delta} q_i g_i \\ &= \sum_{\mathsf{multidegree}(q_i g_i) = \delta} \mathsf{LT}(q_i) g_i + \sum_{\mathsf{multidegree}(q_i g_i) = \delta} (\mathsf{LT}(q_i) - q_i) g_i \sum_{\mathsf{multidegree}(q_i g_i) < \delta} q_i g_i \end{aligned}$$

Note that all terms in the second and third sum in the right-hand side of the above equality have multi-degree less than δ.

Observe that the sum $\sum_{\text{multidegree}(q_i g_i)=\delta} \mathsf{LT}(q_i)g_i$ satisfies the assumptions of Lemma 26 (taking $p_i = q_i g_i$). Using that Lemma, one deduces that

$$\sum_{\text{multidegree}(q_i g_i)=\delta} \mathsf{LT}(q_i)g_i = \sum c_{i,j} S(p_i, p_j)$$

with $c_{i,j} \in \mathbb{K}$. One can easily establish that

$$S(p_i, p_j) = \underline{x}^{\delta-\gamma_{i,j}} S(g_i, g_j)$$

for $\underline{x}^{\gamma_{i,j}} = lcm(\mathsf{LM}(g_i), \mathsf{LM}(g_j))$ since $p_i = q_i g_i$ for all i. We deduce that

$$\sum_{\text{multidegree}(q_i g_i)=\delta} \mathsf{LT}(q_i)g_i = \sum c_{i,j}\, \underline{x}^{\delta-\gamma_{i,j}}\, S(g_i, g_j).$$

Now we use $\overline{S(g_i, g_j)}^{G} = 0$. From the division algorithm, we deduce that

$$S(g_i, g_j) = \sum_{\ell} h_\ell g_\ell$$

with $h_\ell \in \mathbb{K}[x_1, \ldots, x_n]$ and

$$\text{multidegree}(h_\ell g_\ell) \preceq \text{multidegree}(S(g_i, g_j)) \text{ for } h_\ell g_\ell \neq 0.$$

Observe also that $h_\ell g_\ell \neq 0$

$$\text{multidegree}(\underline{x}^{\delta-\gamma_{i,j}} h_\ell g_\ell) \leqslant \text{multidegree}(\underline{x}^{\delta-\gamma_{i,j}} S(g_i, g_j)) < \delta$$

since $\mathsf{LT}(S(g_i, g_j)) \prec lcm(\mathsf{LM}(g_i), \mathsf{LM}(g_j)) = \underline{x}^{\gamma_{i,j}}$ (you may formally prove this fact).

Finally, we deduce that $\sum_{\text{multidegree}(q_i g_i)=\delta} \mathsf{LT}(q_i)g_i$ is a linear combination of the polynomials $\underline{x}^{\delta-\gamma_{i,j}} S(g_i, g_j)$ which satisfy the above relations ; in particular they can be written as algebraic combinations of the g_j's, say $\tilde{h}_j g_j$ with $\text{multidegree}(\tilde{h}_j g_j) \prec \delta$. Substituting this in the formula

$$f = \sum_{\text{multidegree}(q_i g_i)=\delta} \mathsf{LT}(q_i)g_i + \sum_{\text{multidegree}(q_i g_i)=\delta} (\mathsf{LT}(q_i) - q_i)g_i \sum_{\text{multidegree}(q_i g_i)\prec\delta} q_i g_i$$

yields a writing of f as an algebraic combination of the g_j's where all terms have multidegree less than δ. This is a contradiction. □

Let us illustrate how to use Buchberger's criterion.

Consider the ideal $\langle x_2 - x_1^2, x_3 - x_1^2\rangle$ in $\mathbb{C}[x_1, x_2, x_3]$. We show now how to use Buchberger's criterion to prove that $G = (x_2 - x_1^2, x_3 - x_1^2)$ is a Gröbner basis considering the lexicographical ordering with $x_2 > x_3 > x_1$.

Consider the S-polynomial

$$\begin{aligned} S(x_2 - x_1^2, x_3 - x_1^2) &= \frac{x_2 x_3}{x_2}(x_2 - x_1^2) - \frac{x_2 x_3}{x_3}(x_3 - x_1^3) \\ &= -x_3 x_1^2 + x_2 x_1^3. \end{aligned}$$

We next use the division algorithm and compute the normal form of $-x_3x_1^2 + x_2x_1^3$ modulo G. One finds that

$$-x_3x_1^2 + x_2x_1^3 = x_1^3(x_2 - x_1^2) + (-x_1^2)(x_3 - x_1^3) + 0.$$

Hence, the remainder is 0 and our claim follows.

Exercise 14

Is the above set G a Gröbner basis when considering the grevlex ideal with $x_1 \succ x_2 \succ x_3$?

Exercise 15

Something general for polyomial sets of the form $X_i^{\alpha_i} +$ bla bla.

Exercise 16

Using the Buchberger criterion, design an algorithm which takes as input a finite polynomial family in $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering $\succ$, and decides whether G is a Gröbner basis w.r.t. $\succ$.
Analyze the complexity of such an algorithm.

Buchberger's criterion is also called the S-pair criterion. Recall that it is the main ingredient which alllows us to determine if given a finite polynomial subset of $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering, this polynomial subset is a Gröbner basis (w.r.t. the monomial ordering under consideration).

We see now that it is also the main ingredient of Buchberger's algorithm which, given as input a finite polynomial subset F in $\mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering $\succ$, computes a Gröbner basis for $\langle F \rangle$ w.r.t. $\succ$.

Exercise 17

Let f and g in $\mathbb{K}[x_1, \ldots, x_n]$ and $\underline{x}^\alpha$ and $\underline{x}^\beta$ be monomials. Prove that

$$S(\underline{x}^\alpha f, \underline{x}^\beta g) = \underline{x}^\gamma S(f, g)$$

with $\underline{x}^\gamma = \frac{lcm(\underline{x}^\alpha \mathrm{LM}(f), \underline{x}^\beta \mathrm{LM}(g))}{lcm(\mathrm{LM}(f), \mathrm{LM}(g))}$. Prove that $\underline{x}^\gamma$ is a monomial.

5 Buchberger's algorithm

Recall that the proof of Corollary 14 was not constructive: from this proof, we cannot derive an algorithm, which, given a basis F of an ideal $I = \langle F \rangle$ and a monomial ordering $\succ$ computes Gröbner bases G for I and $\succ$. This section is dedicated to describe such an algorithm, which was discovered by B. Buchberger in 1965.

Before giving a formal description of that algorithm, we start by outline the main ideas on which it underlines through an example.

5.1 Example

Let

$$f_1 = x_1^3 - 2x_1x_2$$
$$f_2 = x_1^2x_2 - 2x_2^2 + x_1$$

in $\mathbb{Q}[x_1, x_2]$ and let I be the ideal $\langle f_1, f_2\rangle$. We use the grevlex ordering.

We already observed that $\mathsf{LT}(S(f_1, f_2)) = -x_1^2 \notin \langle \mathsf{LT}(f_1), \mathsf{LT}(f_2)\rangle$ which implies that (f_1, f_2) is not a Gröbner basis (recall that by definition $S(f_1, f_2) \in \langle f_1, f_2\rangle$).

In some sense, we need to add a new element of the ideal $I = \langle f_1, f_2\rangle$ in the set $\{f_1, f_2\}$ which will augment $\langle \mathsf{LT}(f_1), \mathsf{LT}(f_2)\rangle$ and help to satisfy Buchberger's criterion.

At this stage of the course, it should not be a surprise that a natural candidate for this is $\overline{S(f_1, f_2)}^F$ with $F = \{f_1, f_2\}$. Indeed, recall that

- $S(f_1, f_2) \in \langle f_1, f_2\rangle$ which implies that $\overline{S(f_1, f_2)}^F \in \langle f_1, f_2\rangle$;
- Notice that $\overline{S(f_1, f_2)}^F = -x_1^2$ and then its leading term does not belong to $\langle \mathsf{LT}(F)\rangle$.

Now, let us set $F_3 = \{f_1, f_2, f_3\}$ with $f_3 = \overline{S(f_1, f_2)}^F$.

We obviously have $\langle \mathsf{LT}(F)\rangle \subsetneq \langle \mathsf{LT}(F_3)\rangle$; hence there is a chance that F_3 is a Gröbner basis. Let us try to decide this. To do so, we compute

$$S(f_1, f_3) = (x_1^3 - 2x_1x_2) - (-x_1)(-x_1^2) = -2x_1x_2.$$

We check easily that $\overline{S(f_1, f_3)}^{F_3} \neq 0$. Then one needs to add again a new polynomial to the current basis.

Remark. Observe that we could have computed $S(f_2, f_3)$ instead. It is a good exercise to investigate what would have happened in that case.

Using the same intuitive idea that we had, a natural candidate for being that new polynomial is

$$f_4 = \overline{S(f_1, f_3)}^{F_3} = -2x_1x_2$$

and we set $F_4 = \{f_1, f_2, f_3, f_4\}$.

Exercise 18

Prove that $\overline{S(f_1, f_2)}^{F_4} = 0$ and $\overline{S(f_1, f_3)}^{F_4} = 0$.

Using the result of the above exercise, we switch to study $\overline{S(f_1, f_4)}^{F_4}$. We have

$$S(f_1, f_4) = x_2(x_1^3 - 2x_1x_2) - \left(-\frac{1}{2}\right)x_1^2(-2x_1x_2) = -2x_1x_2^2 = x_2f_4.$$

Hence, we deduce quite easily that $\overline{S(f_1, f_4)}^{F_4} = 0$

We then study another pair polynomials in F_4, say (f_2, f_3). One has

$$S(f_2, f_3) = (x_1^2 x_2 - 2x_2^2 + x_1) - (-x_2)(-x_1^2) = -2x_2^2 + x_1$$

and $\overline{S(f_2, f_3)}^{F_4} = -2x_2^2 + x_1 \neq 0$.

5.2 Description of the algorithm

We can now describe Buchberger's algorithm. We start with its specification.

- **Input.** $F = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$ and a monomial ordering $\succ$.
- **Output.** A Gröbner basis $G \subset \mathbb{K}[x_1, \ldots, x_n]$ for $I, \succ$ with $F \subset G$.

Buchberger$(F, \succ)$

1. $G \leftarrow F$
2. Do
   - $G' = G$
   - for all pairs (f, g) in G' with $f \neq g$ do
     - $r \leftarrow \overline{S(f,g)}^{G'}$
     - if $r \neq 0$ then $G \leftarrow G \cup \{r\}$
3. until $G = G'$
4. return G

Observe that the above algorithm is pretty much the same as the treatment of the example we had at the beginning of this section.

5.3 Correctness

Theorem 28. *Let $F = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering. Then, on input F and $\succ$, Buchberger's algorithm above computes a Gröbner basis G, containing F, for $\langle f_1, \ldots, f_s \rangle, \succ$.*

Proof. We start by proving that $G \subset I$ at every step of the algorithm. This is of course true at the initialization since we take $G = F \subset I$. Next, observe that each time one adds to G a polynomial, it is of the form $\overline{S(f,g)}^{G'}$ for $(f, g) \in G' \subset G$. Hence, if $G \subset I$, then f and g also lie in I and consequently $\overline{S(f,g)}^{G'}$ does. Remark also that G contains the input sequence F.

Also, note that when the algorithm terminates, it returns $G = G'$ such that for all $(f, g) \in G \times G$, one has $\overline{S(f,g)}^{G} = 0$. We deduce then that G is a Gröbner basis for $\langle G \rangle = I, \succ$.

We prove now that the algorithm terminates. This will rely on the ascending chain condition that we established in the previous sections.

More precisely, observe that after going though the main loop, one has

$$\langle \mathsf{LT}(G') \rangle \subset \langle \mathsf{LT}(G) \rangle.$$

(because one has $G' \subset G$). The key ingredient now is that when $G' \neq G$, the above inclusion is strict. Indeed, if $r \in G \setminus G'$, then $\mathsf{LT}(r)$ is not divisible by any of the leading terms of the elements of G' and applying Lemma 2, one deduces that $\mathsf{LT}(r) \notin \langle \mathsf{LT}(G') \rangle$ while we obviously have $\mathsf{LT}(r) \in \langle \mathsf{LT}(G) \rangle$ (since $r \in G$).

Hence, the sequence of monomial ideals $\mathsf{LT}(G)$ is an ascending chain of nested ideals and applying Theorem 15, one concludes that this sequence will stabilize. The above paragraph shows that this sequence stabilizes when $G = G'$ which finishes to establish the termination of Buchbergeer's algorithm. □

The version of Buchberger's algorithm which is given above is a very elementary one which is intended to be as simple as possible to ensure the understanding of the reader of the main concepts and ingredient of Gröbner bases theory.

On the practical side, many improvements can (and must) be brought to this algorithm.

For instance, observe that once a remainder $\overline{S(f,g)}^{G'}$ is zero for some (f,g) in some G', it will stay zero in the next steps of the algorithm.

Exercise 19

Prove the above fact.

Then, one should keep track of that info and not recompute those remainders.

Exercise 20

Provide a new version and description of Buchberger's algorithm that exploits the above observation.

There are several algorithms for computing Gröbner bases. Buchberger's algorithms and its variants are important because they bring the foundations of the theory of Gröbner bases. Modern algorithms like Faugere's $F4$ and $F5$ algorithms, which are currently the most efficient, obviously rely on many facts that were raised by Gröbner bases theory.

5.4 Uniqueness and reduced Gröbner bases

Gröbner bases that are computed by the above Buchberger's algorithm are usually redundant in the sense that they contain useless generators. If one would have expected to decide the equality of ideals through their Gröbner bases, this is a strong obstruction.

The goal of this paragraph is to strengthen the requirements on Gröbner bases to yield uniqueness. The result below is a first step towards this goal.

Lemma 29. *Let $G \subset \mathbb{K}[x_1, \ldots, x_n]$ be a Gröbner basis for $I, \succ$. Assume that there exists $f \in G$ such that $\mathsf{LT}(f) \in \langle \mathsf{LT}(G \setminus \{f\}) \rangle$. Then $G \setminus \{f\}$ is also a Gröbner basis for $I, \succ$.*

Proof. From the assumptions, we have

$$\langle \mathsf{LT}(G) \rangle = \langle \mathsf{LT}(I) \rangle.$$

Also, since $\mathsf{LT}(f) \in \langle \mathsf{LT}(G \setminus \{f\}) \rangle$, one has

$$\langle \mathsf{LT}(G \setminus \{f\}) \rangle = \langle \mathsf{LT}(G) \rangle = \langle \mathsf{LT}(I) \rangle.$$

Our claim follows from the definition of Gröbner bases. □

From the above lemma, one notices that setting all leading coefficients to 1 (which can always be done by dividing $f \in G$ by $\mathsf{LC}(f)$) in a Gröbner basis G and removing from G all polynomials f such that $\mathsf{LT}(f) \in \langle \mathsf{LT}(G - \{f\}) \rangle$, one obtains a *minimal* Gröbner basis.

Exercise 21

Compute a minimal Gröbner basis of $\langle x_1^2 - x_2^2, x_1 x_2 \rangle$ for the lexicographical ordering. Deduce that *minimal Gröbner bases* do not necessarily form a *minimal set of generators.*

Definition 30. *Let G be a Gröbner basis in $\mathbb{K}[x_1, \ldots, x_n]$ for $I, \succ$. One says that G is a* minimal Gröbner basis *if*

- *for all $f \in G$, $\mathsf{LC}(f) = 1$;*
- *for all $f \in G$, $\mathsf{LT}(f) \notin \langle \mathsf{LT}(G - \{f\}) \rangle$.*

Recall that Proposition 8 establishes the uniqueness minimal bases of monomial ideals. The following lemma is to be related to that statement.

Lemma 31. *Let $G \subset \mathbb{K}[x_1, \ldots, x_n]$ be a minimal Gröbner basis for $I, \succ$. Then, the leading terms $\mathsf{LT}(g)$ for $g \in G$ form the unique minimal basis of $\langle \mathsf{LT}(I) \rangle$.*

Exercise 22

Prove the above lemma.

A natural question now is about the uniqueness of minimal Gröbner bases. The exercise below shows that such a statement is hopeless.

Exercise 23

Let $G = \{f_1, f_2, f_3\}$ in $\mathbb{Q}[x_1, x_2]$ with

$$f_1 = x_1^2, \qquad f_2 = x_1 x_2, \quad f_3 = x_2^2 - \frac{x_1}{2}.$$

- Prove that G is a Gröbner basis (using the *grlex* ordering) and decide if this is a minimal Gröbner basis;
- Let $\tilde{G} = \{\tilde{f_1}, f_2, f_3\}$ with $\tilde{f_1} = x_1^2 + x_1 x_2$. Prove that $\tilde{G}$ is also a Gröbner basis (still using the *grlex* ordering) and decide if this is a minimal Gröbner basis;
- Compare the ideals $\langle G \rangle$ and $\langle \tilde{G} \rangle$;
- Let $\tilde{G}_a = \{\tilde{f_{1,a}}, f_2, f_3\}$ with $\tilde{f_{1,a}} = x_1^2 + a\, x_1 x_2$ for any $a \in \mathbb{Q}$. Compare the ideals $\langle G \rangle$ and $\langle \tilde{G}_a \rangle$.

The above exercise leads us to the definition below.

Definition 32. *Let $G \subset \mathbb{K}[x_1, \ldots, x_n]$ be a Gröbner basis for $I, \succ$. One says that G is a* reduced Gröbner basis *if the following holds:*

- *for all $g \in G$, $\mathsf{LC}(g) = 1$;*
- *for all $g \in G$, no monomial of g lies in $\langle \mathsf{LT}(G - \{g\}) \rangle$.*

Theorem 33. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal which is not $\{0\}$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. Then, there exists a unique reduced Gröbner basis for $I, \succ$.*

Proof. We start with the existence of a reduced Gröbner basis for $I, \succ$. Take a minimal Gröbner basis G for $I, \succ$ and $g \in G$. We shall say that g is *fully reduced* w.r.t. G if no monomial of g lies in $\langle \mathsf{LT}(G - \{g\}) \rangle$. By the uniqueness of $\langle \mathsf{LT}(G) \rangle$ (because G is minimal ; see Lemma 31), we deduce that g is fully reduced w.r.t. any other minimal Gröbner basis for $I, \succ$.

Now, for $g \in G$, let $g' = \overline{g}^{G - \{g\}}$ and $G' = (G - \{g\}) \cup \{g'\}$. Observe that $\mathsf{LT}(g') = \mathsf{LT}(g)$ (because G is minimal, $\mathsf{LT}(g)$ is not divisible by any term in $\mathsf{LT}(G)$ and then appears in the remainder g'). Hence we deduce that $\langle \mathsf{LT}(G') \rangle = \langle \mathsf{LT}(G) \rangle$. Since we obviously have $G' \subset I$, we deduce that G' is a minimal Gröbner basis for $I, \succ$. Also note that for any $g' \in G'$, g' is fully reduced w.r.t. G'.

Now, applying the above process repeatedly for all elements g in G, one obtains a new basis G' until all elements are fully reduced (each time one performs such a reduction, the current basis changes but since the leading term ideal remains unchanged, those elements of G' which were fully reduced will stay fully reduced). In the end, one will obtain a reduced Gröbner basis for $I, \succ$ which establishes existence.

It remains to prove uniqueness. Let G and G' be two reduced bases for $I, \succ$. Then, according to what we previously established $\mathsf{LT}(G) = \mathsf{LT}(G')$ and for $g \in G$ there exists $g' \in G'$ such that $\mathsf{LT}(g) = \mathsf{LT}(g')$. We prove further that $g = g'$ which will establish that $G = G'$.

Since $g - g' \in I$, we have $\overline{g - g'}^{G} = 0$. Since $\mathsf{LT}(g) = \mathsf{LT}(g')$, these terms cancel in $g - g'$ and since G is reduced, none of the terms in $g - g'$ is divisible by an element of $\mathsf{LT}(G)$. Hence one has $\overline{g - g'}^{G} = g - g'$ and then $g - g' = 0$. □

A first application of these results is that it gives us a way to decide the equality of ideals.

For instance take two finite families F_1 and F_2 of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. If one wants to decide if $\langle F_1 \rangle = \langle F_2 \rangle$, then one chooses a monomial ordering $\succ$ and computes reduced bases G_1 and G_2 for these ideals and $\succ$. The equality $\langle F_1 \rangle = \langle F_2 \rangle$ holds if and only if $G_1 = G_2$.

Exercise 24

Show that $\langle x_1^3 + 1, x_1^2 - x_2 \rangle = \langle x_2^3 - 1, x_2^2 + x_1 \rangle$.