

# Gröbner Basis Fundamentals

Reinhard Lüftenegger

Mathematical Foundations of Cryptography – WT 2020/21 – IAIK, TU Graz

# Overview

## Divisibility and Division Algorithms

- Roadmap to Gröbner Bases
- Polynomials and Polynomial Long Division

## Gröbner Bases

- Buchberger's Algorithm



[mqchallenge.org](http://mqchallenge.org)

# Why Care About Gröbner Bases in Cryptography?

Gröbner Bases are used as a tool for ...

- ... cryptanalysis of symmetric key primitives such as stream and block ciphers or hash functions.
- ... cryptanalysis of public key primitives, especially for cryptosystems based on multivariate quadratic equations.
- ... a general tool for solving systems of polynomial equations.

## “God Made the Integers, all the Rest is the Work of Man”

Many concepts of modern algebra evolved out of a careful study of number systems like  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and polynomials over them. Among others, we have had a look at rings, ideals and quotient rings.

Do you remember the following concepts from the realm of the integers?

- Divisibility and division with remainder
- Greatest common divisors
- (Extended) Euclidean algorithm

**In this lecture:** We generalise and carry over above concepts to **multivariate** polynomial rings and see how they connect to Gröbner bases.

# Divisibility and Division Algorithms

# First things first

A Gröbner basis is ...

## Definition

... a finite set of generators  $\{g_1, \dots, g_k\}$  for a polynomial ideal  $I$  in  $\mathbb{F}[X_1, \dots, X_n]$  such that the ideal generated by the leading terms of  $g_1, \dots, g_k$  is equal to the ideal generated by all the leading terms of polynomials in  $I$ .

## It Is All About Ideals

**Fundamental task:** Find all solutions  $(x_1, \dots, x_n) \in \mathbb{F}^n$  to a system of polynomial equations

$$f_1(x_1, \dots, x_n) = f_2(x_1, \dots, x_n) = \dots = f_k(x_1, \dots, x_n) = 0.$$

**In other words:** We are looking for the set of all common zeros of  $f_1, \dots, f_k$

$$V(f_1, \dots, f_k) := \{(x_1, \dots, x_n) \in \mathbb{F}^n : f_i(x_1, \dots, x_n) = 0, \text{ for all } 1 \leq i \leq k\}.$$

This is equivalent to asking for the set of all common zeros of polynomials in  $\text{Id}(f_1, \dots, f_k)$ . I.e. we have

$$V(f_1, \dots, f_k) = V(\text{Id}(f_1, \dots, f_k)).$$

**Quintessence:** Instead of working with the set of polynomials  $\{f_1, \dots, f_k\}$  from the initial system, we switch to the ideal  $\text{Id}(f_1, \dots, f_k)$  generated by these polynomials.



## The Generating Set Matters

**Observation:** A different generating set for  $\text{Id}(f_1, \dots, f_k)$  may make it easier to solve the corresponding equation system.

**Example:** Consider the equation system

$$\begin{aligned}x^2 + y^2 + 2x + 2y + 2 &= 0 = f_1(x, y, z), \\-2x^2 + y^2 - z^2 + 2y - 4x - 2z - 2 &= 0 = f_2(x, y, z), \\4x^2 + 3y^2 + z^2 + 8x + 6y + 2z + 8 &= 0 = f_3(x, y, z).\end{aligned}$$

# Roadmap to Gröbner Bases I

- **Fact 1**  
Polynomial equation system  $\longrightarrow$  Generated ideal

## Consequence: We Need Multivariate Division I

**Question:** How do we proceed to find another generating set for a multivariate ideal  $\text{Id}(f_1, \dots, f_k)$ ?

**Counterquestion:** Well, how do we proceed in the univariate case?

**Example:** Consider the two univariate polynomials  $f_1(X) = 3(X + 1)(X - 2)^2$  and  $f_2(X) = 2(X - 3)(X + 1)(X - 2)(X - 4)$  over  $\mathbb{Q}$ . To find another generating set for  $\text{Id}(f_1, f_2)$  we apply the Euclidean algorithm and calculate  $g := \text{gcd}(f_1, f_2) = (X + 1)(X - 2)$ . Then

$$f_1 = q_1 g \text{ and } f_2 = q_2 g$$

and therefore  $\text{Id}(f_1, f_2) \subseteq \text{Id}(g)$ . We obtain the reverse inclusion with the Extended Euclidean Algorithm via Bezout's identity

$$g = \text{gcd}(f_1, f_2) = a \cdot f_1 + b \cdot f_2$$

for some  $a, b \in \mathbb{Q}[X]$ . Hence  $\text{Id}(g) = \text{Id}(f_1, f_2)$ .

**Quintessence:** We need a notion of multivariate polynomial long division!

## Consequence: We Need Multivariate Division II

**Question:** Can we identify any requirement for multivariate long division?

**Answer:** Indeed, we can. It relates to the structure of ideals in  $\mathbb{F}[X_1, \dots, X_n]$ .

**Remember:** The univariate polynomial ring  $\mathbb{F}[X]$  over a field  $\mathbb{F}$  is a principal ideal domain (as are the integers  $\mathbb{Z}$ ).

**Spoiler:** Multivariate polynomial rings do not admit this structure.

**Example:** Suppose, in  $\mathbb{F}[X, Y]$  the ideal generated by  $\{X, Y\}$  was principal, i.e., there was a polynomial  $f \in \mathbb{F}[X, Y]$  such that  $\text{Id}(X, Y) = \text{Id}(f)$ . Then

$$X = g \cdot f \text{ and } Y = h \cdot f.$$

Consequently  $\deg_X(f) = \deg_Y(f) = 0$ , which means that  $f$  was a constant and therefore  $\text{Id}(X, Y) = \text{Id}(f) = \mathbb{F}[X, Y]$ . A contradiction.

**Consequence for us:** To find a generating set for multivariate ideals it is desirable to have a division algorithm which handles **multiple** divisors.

## Roadmap to Gröbner Bases II

- **Fact 1**  
Polynomial equation system  $\longrightarrow$  Generated ideal
- **Fact 2**  
Multivariate division algorithm that handles multiple divisors

## The Intuition Behind Gröbner Bases

**Remember:** For any two integers (univariate polynomials)  $a, b$ , with  $b \neq 0$ , there are unique integers (univariate polynomials)  $q, r$  such that  $a = q \cdot b + r$  and  $|r| < |b|$  ( $\deg(r) < \deg(b)$ ). In particular we always have

$$r = 0 \iff a \in \text{Id}(b).$$

**Spoiler:** The division algorithm in multivariate polynomial rings doesn't satisfy this property anymore (more precisely, the direction " $\iff$ "). More on that later.

**Intuition behind Gröbner bases:** A set  $\{g_1, \dots, g_k\}$  is a Gröbner basis of the ideal  $I := \text{Id}(g_1, \dots, g_k)$  if and only if membership in  $I$  is equivalent to having a zero remainder  $r$  after division by  $g_1, \dots, g_k$ . In other words, for any polynomial  $a$  we have

$$r = 0 \iff a \in \text{Id}(g_1, \dots, g_k).$$

## Roadmap to Gröbner Bases III

- **Fact 1**  
Polynomial equation system  $\longrightarrow$  Generated ideal
- **Fact 2**  
Multivariate division algorithm that handles multiple divisors
- **Fact 3**  
Membership in an ideal equivalent with zero remainder

## Long Division of Polynomials in One Variable I

Long division of univariate polynomials is much like long division with integers. Let us tackle the following long division in  $\mathbb{Q}[X]$ : how would you carry out

$$(3X^4 + X^3 + 1) : (2X^3 + X) = ?$$



## Long Division of Polynomials in One Variable II

Let us highlight the aim of each step in the long division:

- By asking how often  $2X^3$  fits into  $3X^4$  we find a factor,  $\frac{3}{2}X$ , such that “dividend minus factor times divisor” does not contain the term  $3X^4$  anymore; we call this a **reduction**.
- Important fact about reductions: the resulting polynomial has degree strictly less than the initial one (the reason why the algorithm eventually terminates).

As is the case for integers, we have the following

### Theorem (Long Division with Univariate Polynomials)

Let  $\mathbb{F}$  be a field and  $g \in \mathbb{F}[X]$  be a non-zero polynomial. Then every polynomial  $f \in \mathbb{F}[X]$  can be written as

$$f = q \cdot g + r,$$

where  $q, r \in \mathbb{F}[X]$  are uniquely determined and either  $r = 0$  or  $\deg(r) < \deg(g)$ .

## Teaser: Long Division with Polynomials in Several Variables?

**Question:** Can we carry over the concept of long division to multivariate polynomials?

**Answer:** Yes, but the generalisation requires some care. Especially, how we achieve reductions.

Let's say, we wanted to perform a long division with the following polynomials in  $\mathbb{Q}[X, Y]$  by imitating the procedure over  $\mathbb{Q}[X]$ :

$$(X^6 + Y^7 + X^3Y^4 + 1) : (X + Y^3) = ?$$

Then we need to address (at least) two questions:

- Shall we begin with the term  $X$  or  $Y^3$  on the divisor side?
- Which term is the “pivot term” on the dividend side?

## Another Look at Univariate Polynomial Long division

**Observation:** Univariate long division uses an implicit notion of “order”.

**Explanation:** In every step of the division algorithm we take the monomial with the highest degree to achieve a reduction.

**Consequences:** We therefore need the notion of “order” in multivariate rings as well.

**Motivating Example:** How would you order the following terms in  $\mathbb{Q}[X, Y, Z]$ ?

$$4X, 2Y^5Z, Y^5, 1000 \text{ and } 1$$

**Takeaway:** Constant factors do not matter! Hence, we focus on monomials (rather than terms) in  $\mathbb{F}[X_1, \dots, X_n]$ .

**Intermezzo:** Let's have a closer look at how we “order” monomials in the univariate case.

## “Let There Be Order”: Monomial Order in $\mathbb{F}[X]$

**Observation:** Monomials in  $\mathbb{F}[X]$  are expressions of the form  $X^n$ , for  $n \in \mathbb{N}_0$  and we have a canonical order on  $\mathbb{N}_0$ .

**Consequence:** Given the order on  $\mathbb{N}_0$ , it is natural to set

$$X^0 = 1 \leq X \leq X^2 \leq \dots$$

or more generally for  $X^i, X^j \in \mathbb{F}[X]$  and  $i, j \in \mathbb{N}_0$

$$X^i \leq X^j : \iff i \leq j.$$

**Question:** Can we use above order and extend it to monomials in  $\mathbb{F}[X_1, \dots, X_n]$  by setting

$$X_1^{i_1} \dots X_n^{i_n} \leq X_1^{j_1} \dots X_n^{j_n} : \iff \forall 1 \leq k \leq n : i_k \leq j_k?$$

## “Let There Be Order”: Total Order I

**Answer:** No, not quite. But the approach is not completely pointless.

**Example:** Let's say, we wanted to compare and order monomials in  $\mathbb{F}[X, Y]$  according to the suggested order above. Then, e.g., how would we relate the monomials  $X^2Y^2$  and  $X^3Y$ ?

**Conclusion:** We need to think a bit more about what we mean by an “order”.

## “Let There Be Order”: Total Order II

As it turns out, there is an order relation available that is useful for our purposes.

### Definition (Total Order)

Let  $M$  be a set and  $\leq$  a (binary) relation on  $M$  satisfying the following properties

- $a \leq b$  or  $b \leq a$  (Comparability),
- $a \leq b$  and  $b \leq c$  implies  $a \leq c$  (Transitivity),
- $a \leq b$  and  $b \leq a$  implies  $a = b$  (Antisymmetry),

for all  $a, b, c \in M$ . Then  $\leq$  is called a **total order on  $M$** .

## “Let There Be Order”: Monomial Order in $\mathbb{F}[X_1, \dots, X_n]$

**Notation:** We use the abbreviating notation  $X^\alpha := X_1^{\alpha_1} \dots X_n^{\alpha_n}$  for a monomial in  $\mathbb{F}[X_1, \dots, X_n]$  with exponent vector  $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ .

Our previous observations about order in multivariate polynomial rings are reflected in the following

### Definition

A **monomial order**  $\leq$  on  $\mathbb{F}[X_1, \dots, X_n]$  is a (binary) relation on the set of monomials in  $\mathbb{F}[X_1, \dots, X_n]$  satisfying the following properties

- $\leq$  is a total order,
- $X^\alpha \leq X^\beta \Rightarrow X^\alpha \cdot X^\gamma \leq X^\beta \cdot X^\gamma$

for every monomial  $X^\alpha, X^\beta, X^\gamma$  in  $\mathbb{F}[X_1, \dots, X_n]$ .

## Examples of Monomial Orders I

**Remark:** Of course the polynomial ring  $\mathbb{F}[X_1, \dots, X_n]$  is the same as, e.g., the polynomial ring  $\mathbb{F}[X_n, \dots, X_1]$ . For simplicity, we fix the following succession  $(X_1, X_2, \dots, X_n)$  when writing down the exponent vector  $\alpha = (\alpha_1, \dots, \alpha_n)$  of  $X^\alpha$ .

Some commonly used monomial orders:

- **Lexicographic Order** (“lex”)  
→ Emphasises the **first place** of variables in their succession, then **higher univariate** degree, then 1
- **Graded Lex Order** (“deglex” or “glex”)  
→ Emphasises **higher multivariate** degree, then **first place** in succession, then **higher univariate** degree, then 1
- **Graded Reverse Lex Order** (“degrevlex” or “grevlex”)  
→ Emphasises **higher multivariate** degree, then **last place** in succession, then **lower univariate** degree, then 1



## Examples of Monomial Orders II

Let's discuss some examples in  $\mathbb{Q}[X, Y, Z]$ , with the variables arranged in the following succession  $(X, Y, Z)$ .

<b>lex</b>	first in succ.	higher uni.	
<b>deglex</b>	higher multi.	first in succ.	higher uni.
<b>degrevlex</b>	higher multi.	last in suc.	lower uni.

**Example:** What is the arrangement of the monomials  $X^2, XY^2Z^2, Y^4Z$  in descending order with respect to lex, deglex and degrevlex?

**Question:** What distinguishes one monomial order from another one?

**Short Answer:** Different monomial orders have different arithmetic and/or algorithmic properties (e.g. number of steps in the division algorithm).

# Leading Monomials and Leading Terms

## Definition

Let  $\leq$  be a monomial order on the monomials in  $\mathbb{F}[X_1, \dots, X_n]$  and  $f \in \mathbb{F}[X_1, \dots, X_n]$  a polynomial denoted as

$$f(X_1, \dots, X_n) = \sum_{\alpha=(\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n} c_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n} = \sum_{\alpha=(\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n} c_\alpha X^\alpha.$$

The **leading monomial of  $f$**  (with respect to  $\leq$ ) is the monomial given by

$$\text{LM}(f) := \text{LM}_{\leq}(f) := \max_{\leq} \{X^\alpha : c_\alpha \neq 0\},$$

whereas the **leading term of  $f$**  (with respect to  $\leq$ ) is the product of the leading monomial with its corresponding coefficient, i.e.

$$\text{LT}(f) := \text{LT}_{\leq}(f) := c_\alpha X^\alpha, \text{ for } X^\alpha = \text{LM}(f).$$

## Long Division on Polynomials in Several Variables I

**Key ingredients for multivariate long division:** A monomial ordering in  $\mathbb{F}[X_1, \dots, X_n]$  and the requirement of multiple divisors.

**Outline:** With these key ingredients at hand, we sketch the multivariate division algorithm in  $\mathbb{F}[X_1, \dots, X_n]$ .<sup>1</sup>

	Univariate	Multivariate
Dividend	$f = f(X)$	$f = f(X_1, \dots, X_n)$
Divisor	$g$	$f_1, \dots, f_k$
Result	$f = q \cdot g + r$	$f = q_1 \cdot f_1 + \dots + f_k \cdot g_k + r$

<sup>1</sup>For a formal treatment see e.g. Cox, Little, O’Shea: “Ideals, Varieties and Algorithms”, 4th ed., p. 64

## Long Division on Polynomials in Several Variables II

**Input:** Dividend  $f$ , divisors  $f_1, \dots, f_k$ , monomial order  $\leq$

**Output:** Factors  $q_1, \dots, q_k$  and remainder  $r$  such that  $f = q_1 f_1 + \dots + q_k f_k + r$

$q_1 := 0; \dots; q_k := 0; \quad r := 0; \quad p := f$

**while**  $p \neq 0$  **do**

$i := 1;$

**while**  $i \leq k$  **do**

**if**  $\text{LT}(f_i)$  divides  $\text{LT}(p)$  **then**

$q_i := q_i + \text{LT}(p)/\text{LT}(f_i); \quad p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$

$i := 1$

**else**

$i := i + 1$

$r := r + \text{LT}(p); \quad p := p - \text{LT}(p)$

**return**  $q_1, \dots, q_k, r$

**Algorithm 1:** Multivariate Division

## Long Division on Polynomials in Several Variables III

### Theorem (Long Division with Multivariate Polynomials)

Let  $\mathbb{F}$  be a field and  $\{f_1, \dots, f_k\} \subseteq \mathbb{F}[X_1, \dots, X_n]$  be a set of non-zero polynomials. Then every polynomial  $f \in \mathbb{F}[X_1, \dots, X_n]$  can be written as

$$f = q_1 f_1 + \dots + q_k f_k + r,$$

where  $q_1, \dots, q_k, r \in \mathbb{F}[X_1, \dots, X_n]$ , and either  $r = 0$  or no monomial of  $r$  is divisible by any of  $\text{LT}(f_1), \dots, \text{LT}(f_k)$ .

**Remark:** Multivariate division doesn't guarantee uniqueness of factors and remainder.

## Example I

**Example:** Let us divide  $f = X^2Y + XY^2 + Y^2$  by  $f_1 = Y^2 - 1$  and  $f_2 = XY - 1$  with respect to the lex order.

## Example II

**Example:** Let us divide  $f = X^2Y + XY^2 + Y^2$  (same dividend) by  $f_1 = XY - 1$  and  $f_2 = Y^2 - 1$  (same divisors, but in reversed order) with respect to the lex order.

## Side Effects of Multivariate Division

**Observation:** We have

$$\begin{aligned}X^2Y + XY^2 + Y^2 &= (X + 1)(Y^2 - 1) + X(XY - 1) + (2X + 1) \\ &= (Y^2 - 1) + (X + Y)(XY - 1) + (X + Y + 1).\end{aligned}$$

**In other words:** The outcome of multivariate division is not unique and depends on the order of the divisors!

**Bottom line:** When testing a polynomial  $f$  for membership in the ideal  $\text{Id}(f_1, \dots, f_k)$  we only know

$$\text{Zero remainder after dividing } f \text{ by } f_1, \dots, f_k \implies f \in \text{Id}(f_1, \dots, f_k).$$

But, we desire to have equivalence between these two statements.

**Resolution:** The notion of Gröbner bases!





# Gröbner Bases I

Let's recall the definition from the beginning, this time slightly refined.

## Definition

Let  $\leq$  be a monomial order. A Gröbner basis for a polynomial ideal  $I$  in  $\mathbb{F}[X_1, \dots, X_n]$  is a finite set of generators  $\{g_1, \dots, g_k\}$  for  $I$  such that the ideal generated by the leading terms of  $g_1, \dots, g_k$  is equal to the ideal generated by all the leading terms of polynomials in  $I$ , i.e., such that for  $\text{LT}(I) := \{\text{LT}(i) : i \in I\}$  it holds

$$\text{Id}(\text{LT}(g_1), \dots, \text{LT}(g_k)) = \text{Id}(\text{LT}(I)).$$

**Observation:** The crucial property here is

$$\text{LT}(I) \subseteq \text{Id}(\text{LT}(g_1), \dots, \text{LT}(g_k)),$$

or in other words: “The leading term  $\text{LT}(i)$  of every element  $i \in I$  is a linear combination of the leading terms  $\text{LT}(g_1), \dots, \text{LT}(g_k)$  with coefficients in  $\mathbb{F}[X_1, \dots, X_n]$ .”

## Gröbner Bases II

**Question:** The crucial property of Gröbner bases reads as

$$\text{LT}(i) = p_1 \text{LT}(g_1) + \cdots + p_k \text{LT}(g_k),$$

for every  $i \in I$  and certain  $q_1, \dots, p_k \in \mathbb{F}[X_1, \dots, X_n]$ . But why is this important?

**Intuitive Answer:** Let's divide some polynomial  $f$  by  $g_1, \dots, g_k$ . We possibly get

$$f = \underbrace{q_1 g_1 + \cdots + q_k g_k}_{=:q} + r = \underbrace{q'_1 g_1 + \cdots + q'_k g_k}_{=:q'} + r'.$$

Suppose  $r \neq r'$ , then  $\text{LT}(r - r') = \text{LT}(q' - q) \in \text{LT}(I) \stackrel{!}{\subseteq} \text{Id}(\text{LT}(g_1), \dots, \text{LT}(g_k))$ , and therefore

$$\text{LT}(r - r') = p_1 \text{LT}(g_1) + \cdots + p_k \text{LT}(g_k).$$

After expanding the RHS, we conclude that  $\text{LT}(g_i) \mid \text{LT}(r - r')$  for at least one  $i$ . ⚡

## Recap

- When trying to solve a system of polynomial equations, represented by the polynomials  $f_1, \dots, f_k$ , it is convenient to switch to the **generated ideal**  $\text{Id}(f_1, \dots, f_k)$
- **Another generating set** for  $\text{Id}(f_1, \dots, f_k)$  may be more practical for determining the solutions  $x_1, \dots, x_n \in \mathbb{F}$  of  $f_1(x_1, \dots, x_n) = \dots = f_k(x_1, \dots, x_n) = 0$
- A **Gröbner basis**  $\{g_1, \dots, g_k\}$  is a special kind of generating set
- The crucial property of a Gröbner basis is the relation

$$\text{LT}(i) = p_1 \text{LT}(g_1) + \dots + p_k \text{LT}(g_k),$$

for every  $i \in I$  and certain  $p_1, \dots, p_k \in \mathbb{F}[X_1, \dots, X_n]$ . It allows us to “control” the division algorithm such that we have a **unique remainder** when dividing by  $g_1, \dots, g_k$ .

## Computing Gröbner Bases: The Buchberger Criterion

**Remark:** Our definition of a Gröbner basis is of little help for checking if a set  $\{g_1, \dots, g_l\}$  is a Gröbner basis for the ideal  $I := \text{Id}(g_1, \dots, g_l)$ . We need a more practical criterion.

The “main theorem” of Gröbner basis theory is the following criterion, introduced by Bruno Buchberger in his Phd thesis (1965).

### Theorem (Buchberger's criterion)

Let  $G := \{g_1, \dots, g_k\}$  be a set of generators for the ideal  $I := \text{Id}(g_1, \dots, g_k)$ . Then  $G$  is a Gröbner basis of  $I$  if and only if for all pairs  $i \neq j$  the remainder of

$$s(g_i, g_j) := \frac{u}{\text{LT}(g_i)}g_i - \frac{u}{\text{LT}(g_j)}g_j,$$

with  $u(g_i, g_j) := \text{lcm}(\text{LT}(g_i), \text{LT}(g_j))$ , after division by  $G$  (in some order) is zero.

## Computing Gröbner Bases: The Buchberger Algorithm in $\mathbb{F}[X_1, \dots, X_n]$

**Input:** A set of polynomials  $F := \{f_1, \dots, f_k\}$

**Output:** A Gröbner basis  $G := \{g_1, \dots, g_l\}$  for the ideal  $\text{Id}(f_1, \dots, f_k)$

$G := F$

**while**  $G \neq H$  **do**

$H := G$

**foreach**  $p, q \in G, p \neq q$  **do**

$u := \text{lcm}(\text{LM}(p), \text{LM}(q))$

$s := \frac{u}{\text{LT}(p)}p - \frac{u}{\text{LT}(q)}q$

$r :=$  remainder of  $S$  after division by  $H$

**if**  $r \neq 0$  **then**

$G := G \cup \{r\}$

**return**  $G$

**Algorithm 2:** Buchberger

## Computing Gröbner Bases: Efficiency Considerations

**Observation:** In Buchberger's Algorithm, only polynomials  $s$  which have **non-zero remainder** after division by elements in the intermediate set  $H$  contribute to the final Gröbner basis.

**Basic strategy for improvements:** Reduce the number of polynomials  $s$  that need to be considered. That means, finding other criteria that tell us **in advance** when a given polynomial  $s$  has zero remainder.

### Approaches

- Preprocessing the input ( $\longrightarrow$  homogeneous polynomials)
- Batch processing of several  $s$ -polynomials at once ( $\longrightarrow$  linear-algebra-based algorithms,  $F_4$ )
- Exploit certain relations between the input elements ( $\longrightarrow$  "signature"-based algorithms,  $F_5$ )

Questions?



## Questions for Self-Control

1. What is the fundamental difference of ideals in univariate and multivariate polynomial rings (with coefficients in a field) and how does this difference influence multivariate polynomial long division?
2. What is a monomial ordering and why is it important for polynomial long division?
3. Explain the similarities/differences of univariate and multivariate polynomial long division.
4. What is a Gröbner basis? Discuss the underlying idea and the connection to multivariate long division.
5. Discuss Buchberger's Algorithm and identify the most expensive steps. Highlight the main idea for improvements.