
Lecture 6. Division with remainder; Gröbner bases

Proposition 4.6. (Division with remainder) *Let $f, f_1, \dots, f_s \in k[X_1, \dots, X_n]$ be non-zero polynomials. Then there exist polynomials $h_1, \dots, h_s, r \in k[X_1, \dots, X_n]$ such that*

$$f = h_1 f_1 + h_2 f_2 + \dots + h_s f_s + r$$

with the following properties:

- $LT(h_i f_i) \leq LT(f)$ for all i with $h_i \neq 0$;
- either $r = 0$, or no term of r is divisible by any of $LT(f_1), \dots, LT(f_s)$ and $LT(r) \leq LT(f)$.

Proof. We argue by induction on $LM(f)$: by Lemma 4.5 there is no infinite strictly decreasing sequence of monomials, so we may assume that the statement holds for every non-zero polynomial whose leading monomial is smaller than $LM(f)$.

Suppose first that there exists an i such that $LT(f_i) | LT(f)$, and let $i \in \{1, \dots, s\}$ be the smallest such index. Let

$$\tilde{f} = f - \frac{LT(f)}{LT(f_i)} f_i.$$

If $\tilde{f} = 0$, we stop, setting $h_i = LT(f)/LT(f_i)$, $h_j = 0$ for $j \neq i$ and $r = 0$. Otherwise, we have $LT(\tilde{f}) < LT(f)$, so by induction we can write

$$\tilde{f} = \tilde{h}_1 f_1 + \dots + \tilde{h}_s f_s + r$$

with the required conditions. Then

$$f = h_1 f_1 + \dots + h_s f_s + r$$

where $h_j = \tilde{h}_j$ for $j \neq i$ and $h_i = \tilde{h}_i + \frac{LT(f)}{LT(f_i)}$. The conditions on r are inherited from $\tilde{f}$, and $LT(h_j f_j) \leq LT(f)$ for all j because $LT(\tilde{h}_j f_j) \leq LT(\tilde{f}) < LT(f)$ and $LT(\frac{LT(f)}{LT(f_i)} f_i) = LT(f)$.

Suppose now that no $LT(f_i)$ divides $LT(f)$, and let $\tilde{f} = f - LT(f)$. If $\tilde{f} = 0$, we stop, setting all $h_i = 0$ and $r = f$. Otherwise, by induction we can write $\tilde{f} = h_1 f_1 + \dots + h_s f_s + \tilde{r}$ with the required conditions, and we set

$$f = h_1 f_1 + \dots + h_s f_s + r$$

where $r = \tilde{r} + LT(f)$. The term $LT(f)$ is divisible by no $LT(f_i)$ by assumption, and $LT(r) = LT(f)$ since every term of $\tilde{r}$ is at most $LT(\tilde{r}) \leq LT(\tilde{f}) < LT(f)$. $\square$

Example. Let $f = XY^2 - X$, $f_1 = XY + 1$, $f_2 = Y^2 - 1$, and use the lex order with $X > Y$. The leading terms are XY^2, XY, Y^2 respectively. Since $XY \mid XY^2$, we can write $\tilde{f} = f - Yf_1 = -X - Y$. Neither X nor Y is divisible by XY or Y^2 , hence

$$f = Yf_1 + 0f_2 + (-X - Y).$$

Another possibility is to use that $Y^2 \mid XY^2$; then $\tilde{f} = f - Xf_2 = 0$, so we get

$$f = 0f_1 + Xf_2 + 0.$$

Hence the remainder r is not unique: it depends on the order in which $f_1, f_2, \dots, f_s$ are listed.

We can implement the division with remainder algorithm in Macaulay2 as follows.

```
div = (f,G) -> (
R := ring f; p := f; r := 0_R; s := #G; Q := new MutableHashTable;
for j from 0 to s-1 do Q#j = 0_R;
while p != 0 do (
  i := 0;
  while i < s and leadTerm(p) % leadTerm(G#i) != 0 do i = i+1;
  if i < s then (
    Q#i = Q#i + (leadTerm(p) // leadTerm(G#i));
    p = p - (leadTerm(p) // leadTerm(G#i)*G#i)
  else (
    r = r + leadTerm(p);
    p = p - leadTerm(p));
L := apply(s, j -> Q#j);
return (r,L));
```

Using the above division function, you can do division in Macaulay2 as follows.

```
R = QQ[X,Y, MonomialOrder => Lex]
f= X*Y^2 - X
f1 = X*Y +1
f2 = Y^2 - 1
G = {f1,f2}
div(f,G)
G = {f2,f1}
div(f,G)
```

Definition 4.7. (Buchberger) Let $I \subset k[X_1, \dots, X_n]$ be a non-zero ideal. The **initial ideal** of I is the monomial ideal

$$\text{in}(I) := (LT(f) : 0 \neq f \in I).$$

A finite subset $G \subset I \setminus \{0\}$ is called a **Gröbner basis** of I (with respect to the fixed monomial ordering) if the leading terms of its elements generate the initial ideal, that is, $\text{in}(I) = (LT(g) : g \in G)$.

► Every non-zero ideal I has a Gröbner basis. Indeed, $\text{in}(I)$ is finitely generated by the Hilbert basis theorem, and each of its finitely many generators is a combination of finitely many of the $LT(f)$ with $0 \neq f \in I$. Hence $\text{in}(I) = (LT(g_1), \dots, LT(g_s))$ for some $g_1, \dots, g_s \in I \setminus \{0\}$.

► If $I = (f_1, f_2, \dots, f_s)$, then $\text{in}(I)$ need not equal $(LT(f_1), \dots, LT(f_s))$.

◁ Take $I = (f_1, f_2)$ with $f_1 = X^3 - 2XY$ and $f_2 = X^2Y - 2Y^2 + X$ and use $\leq_{\text{grlex}}$. Show that $(LT(f_1), LT(f_2))$ is strictly contained in $\text{in}(I)$.

If you want to check your calculations, you can ask Macaulay2 for help as follows:

```
R = QQ[x,y, MonomialOrder=> GLex];
I = ideal (x^3-2*x*y, x^2*y-2*y^2+x);
inI = ideal leadTerm I
```

Note that the initial ideal depends on the monomial order you choose.

```
R = QQ[x,y, MonomialOrder=> Lex];
I = ideal (x^3-2*x*y, x^2*y-2*y^2+x);
inI = ideal leadTerm I
```

Theorem 4.8. (Buchberger) Let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of a non-zero ideal $I \subset k[X_1, \dots, X_n]$.

1. For a non-zero $f \in k[X_1, \dots, X_n]$, use division with remainder to write

$$f = h_1g_1 + h_2g_2 + \dots + h_sg_s + r.$$

Then $r = 0$ if and only if $f \in I$. Moreover, r does not depend on the order in which $g_1, g_2, \dots, g_s$ are listed. It also follows that $I = (G)$.

2. Let $C(I) := \{\alpha \in \mathbb{N}^n : LT(g_i) \nmid X^\alpha \text{ for all } i\}$. Then $\{X^\alpha + I : \alpha \in C(I)\}$ is a basis of $k[X_1, \dots, X_n]/I$ as a k -vector space.

Proof. (1) Suppose $f \in I$ and $r \neq 0$. Then $r = f - \sum_{i=1}^s h_i g_i \in I$, and since G is a Gröbner basis,

$$LT(r) \in \text{in}(I) = (LT(g_1), LT(g_2), \dots, LT(g_s)).$$

By Lemma 4.4, there exists i such that $LT(g_i) \mid LT(r)$. This contradicts the properties of the division with remainder. Hence $r = 0$. Conversely, if $r = 0$ then $f = \sum_{i=1}^s h_i g_i \in (G) \subset I$. It also follows that $I = (G)$, since every $f \in I$ is of the form $\sum_{i=1}^s h_i g_i$.

Suppose $f = \sum_{i=1}^s h_i g_i + r = \sum_{i=1}^s k_i g_i + \tilde{r}$ are two expressions obtained by division with remainder, with the g_i listed in different orders. Then $\sum_{i=1}^s (h_i - k_i) g_i = \tilde{r} - r \in I$. If $\tilde{r} \neq r$, then $LT(\tilde{r} - r) \in \text{in}(I) = (LT(g) : g \in G)$, hence there exists i such that $LT(g_i) \mid LT(\tilde{r} - r)$. But every term of $\tilde{r} - r$ is, up to a scalar, a term of r or of $\tilde{r}$, and none of these is divisible by any $LT(g_i)$. This is a contradiction, hence $r = \tilde{r}$.

(2) Let $f \in k[X_1, \dots, X_n]$ be non-zero. After division with remainder, none of the terms of r is divisible by any $LT(g_i)$, so r is a k -linear combination of monomials X^α with $\alpha \in C(I)$. Since $f + I = r + I$, the quotient $k[X_1, \dots, X_n]/I$ is spanned by $\{X^\alpha + I : \alpha \in C(I)\}$.

Suppose that $\sum_{i=1}^m a_i X^{\alpha_i} \in I$ for distinct $\alpha_1, \dots, \alpha_m \in C(I)$ and $a_i \in k$. If this polynomial is non-zero, dividing it by $g_1, \dots, g_s$ gives

$$\sum_{i=1}^m a_i X^{\alpha_i} = 0 \cdot g_1 + 0 \cdot g_2 + \dots + 0 \cdot g_s + r$$

with $r = \sum_{i=1}^m a_i X^{\alpha_i}$, since no term of it is divisible by any $LT(g_i)$. By part (1), $r = 0$, a contradiction. Hence all $a_i = 0$, and the $X^\alpha + I$ for $\alpha \in C(I)$ are linearly independent. $\square$

► Although $C(I)$ is defined using G , it depends only on I and the monomial ordering: by Lemma 4.4, $\alpha \in C(I)$ if and only if $X^\alpha \notin \text{in}(I)$. The monomials X^α with $\alpha \in C(I)$ are called the **standard monomials** of I .

Corollary 4.9. *The variety $\mathcal{V}(I) \subset k^n$ defined by I has finitely many points if $C(I)$ is finite.*

Proof. By the theorem, if $C(I)$ is finite then the ring $k[X_1, \dots, X_n]/I$ is finite-dimensional as a k -vector space. Now fix i and consider the monomials $1, X_i, X_i^2, \dots$. Their images in $k[X_1, \dots, X_n]/I$ are linearly dependent, so there exist m and $c_0, c_1, \dots, c_m \in k$, not all zero, such that

$$c_0 + c_1 X_i + c_2 X_i^2 + \dots + c_m X_i^m \in I.$$

This polynomial vanishes on $\mathcal{V}(I)$, but a non-zero polynomial in one variable has at most finitely many roots. It follows that the i -th co-ordinates of the points of $\mathcal{V}(I)$ take only finitely many values. The same is true for every i , hence $\mathcal{V}(I)$ is finite. $\square$

Theorem 4.8 gives an algorithm for solving the ideal membership problem provided that we know a Gröbner basis for the ideal.

Problem: How to construct a Gröbner basis?

Definition 4.10. *Let $f, g \in k[X_1, \dots, X_n]$ be non-zero polynomials. Let $X^\alpha = LM(f)$ with $\alpha = (\alpha_1, \dots, \alpha_n)$ and $X^\beta = LM(g)$ with $\beta = (\beta_1, \dots, \beta_n)$. Define $\gamma = (\gamma_1, \dots, \gamma_n)$ with $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all i , i.e. $X^\gamma = \text{lcm}(LM(f), LM(g))$. The S -polynomial of f and g is defined to be*

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

Example. Let $f = 4X^2Z - 7Y^2$ and $g = XYZ^2 + 3XZ^4$. Using the $\leq_{lex}$ order with $X > Y > Z$, we see that $\text{lcm}(LM(f), LM(g)) = X^2YZ^2$, and

$$S(f, g) = \frac{X^2YZ^2}{4X^2Z} f - \frac{X^2YZ^2}{XYZ^2} g = (1/4)YZf - Xg = -3X^2Z^4 - (7/4)Y^3Z$$

Here is how you may do this in Macaulay2:

```

R = QQ[x,y,z, MonomialOrder => Lex];
f = 4*x^2*z-7*y^2;
g = x*y*z^2 + 3*x*z^4;
Spoly = (f,g) -> (
    m := lcm(leadMonomial f, leadMonomial g);
    (m // leadTerm f) * f - (m // leadTerm g) * g);
Spoly(f,g)

```

► If $S(f, g) \neq 0$, then $LM(S(f, g)) < \text{lcm}(LM(f), LM(g))$. In this sense, we can say that the S -polynomial is designed to produce cancellation of leading terms.

The name S -polynomial is short for “syzygy polynomial”. You can blame Sylvester if you don’t know how to pronounce the word syzygy. In general, syzygy is a kind of linear relation. Here it is a linear relation between polynomials in several variables with polynomial coefficients. In astronomy, a syzygy is an alignment of three celestial bodies, such as the Sun, the Earth and the Moon during an eclipse.