21MAB143 Rings and Polynomials: Week 3

1 Greatest Common Divisor and the Euclidean Algorithm

This week we will see how to compute the Greatest Common Divisor (GCD) of two polynomials, using the Euclidean algorithm. If you have seen the Euclidean algorithm used to compute the GCD of two integers, you will notice how similar this version is. We will also see an application to finding common roots of two given polynomials, and multiple roots of a single polynomial.

We start by introducing the necessary terminology.

Definition 1.1. *A nonzero polynomial* $f \in K[x]$ *is* **monic** *if the leading coefficient (meaning the coefficient of the highest power of* x*) equals 1.*

For a nonzero polynomial $f \in K[x]$ *with leading coefficient* a*, the monic polynomial* $\frac{1}{a}f$ *is called the* **monic form** *of* f*, and denoted by* $\widehat{f}$*.*

Examples In $\mathbf{Q}[x]$ the polynomial

$$f = x^3 - 17x^2 + 59$$

is monic. The polynomial

$$g = 2x^5 - x + 1$$

is not monic. Its leading coefficient is 2, therefore its monic form is

$$\begin{aligned}\widehat{g} &= \frac{1}{2}g \\ &= x^5 - \frac{1}{2}x + \frac{1}{2}.\end{aligned}$$

Definition 1.2 (Greatest Common Divisor)**.** *Let* $f, g \in K[x]$ *be two polynomials. A polynomial* $d \in K[x]$ *is called the* **greatest common divisor** *(GCD) of* f *and* g *if it satisfies the following conditions:*

1. d *is monic*
2. $d \mid f$ *and* $d \mid g$
3. *if* $\delta \in K[x]$ *is any other polynomial such that* $\delta \mid f$ *and* $\delta \mid g$*, then* $\delta \mid d$ *also.*

We write $d = \gcd(f, g)$ *to denote that* d *is the greatest common divisor of* f *and* g*.*

You will show on Problem Sheet 3 that if f and g are not both zero, then they have a **unique** GCD.

1.1 Euclidean algorithm

A key fact about the GCD is that there is an efficient algorithm to calculate it. This is called the **Euclidean algorithm.** Let's see how it works.

Input: Two polynomials $f, g \in K[x]$, not both zero.

Output: The greatest common divisor $d = \gcd(f, g)$.

Steps: Rename the polynomials if necessary so that $\deg(f) \geq \deg(g)$.
If $g = 0$, then $d = \gcd(f, g) = f$, and we can write $d = 1 \cdot f + 0 \cdot g$. So let's assume $g \neq 0$.
By the Division Theorem, we can write

$$f = q_1 g + r_1$$

for some q_1, r_1, with $\deg r_1 < \deg g$. Now the idea is to repeat this process: divide g by r_1 to get

$$\begin{aligned} g &= q_2 r_1 + r_2 \quad \text{and then} \\ r_1 &= q_3 r_2 + r_3 \quad \text{and so on...} \end{aligned}$$

The Division Theorem tells us that the degree of the remainder goes down each time: $\deg r_1 > \deg r_2 > \deg r_3 > \cdots$. So eventually we must end up with zero remainder: that is, after some number n of steps we must get the following situation:

$$\begin{aligned} r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} && \text{(Step } n-2\text{)} \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} && \text{(Step } n-1\text{)} \\ r_{n-2} &= q_n r_{n-1} && \text{(Step } n\text{).} \end{aligned}$$

At Step n we obtained zero remainder. At this point we **STOP**.

Claim: The GCD $\gcd(f, g)$ is equal to $\widehat{r}_{n-1}$, the monic form of the last nonzero remainder.

To prove this, first let us show that we can write r_{n-1} in the form

$$r_{n-1} = af + bg$$

for some polynomials a and b. From Step $n-1$ above we can write

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}.$$

But now Step $n-2$ allows us to write

$$r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}.$$

Substituting that into the previous equation gives

$$r_{n-1} = (1 + q_{n-1}q_{n-2})r_{n-3} - q_{n-1}r_{n-4}.$$

Working backwards like this, we eventually end up with an expression $r_{n-1} = af + bg$, as required.

To see that $\widehat{r}_{n-1}$ actually is the GCD of f and g, we use the Steps above to show $r_{n-1} \mid r_{n-2}$, then $r_{n-1} \mid r_{n-3}$, and so on, eventually obtaining $r_{n-1} \mid f$ and $r_{n-1} \mid g$. On the other hand, since we have that $r_{n-1} = af + bg$, for any polynomial d such that $d \mid f$ and $d \mid g$ we must have $d \mid r_{n-1}$ too. Taking the monic form shows that $\widehat{r}_{n-1}$ is indeed the GCD of f and g. □

We will record part of the above argument as a separate result for later use:

Corollary 1.3 (Bézout's identity for polynomials)**.** *Let* $f, g \in K[x]$ *and let* $d = \gcd(f, g)$*. Then there exist polynomials* $a, b \in K[x]$ *such that*

$$d = af + bg.$$

We can state essentially the same information in terms of ideals. We know by Week 2 Theorem 2.5 that the ideal generated by f and g can also be generated by a single element, and unsurprisingly the GCD is the polynomial that does the job:

Corollary 1.4. *Let* $f,\ g \in K[x]$ *and let* $d = \gcd(f, g)$*. Then*

$$\langle f, g\rangle = \langle d\rangle\,.$$

Proof. By definition of the GCD we know that $d \mid f$ and $d \mid g$. So there are polynomials $r,\ s \in K[x]$ such that $f = rd$ and $g = sd$. But that means that both f and g belong to the ideal $\langle d\rangle$. Since $\langle f, g\rangle$ is the smallest ideal containing both f and g, we must have

$$\langle f, g\rangle \subset \langle d\rangle\,.$$

Conversely Bézout's Identity tells us that there are polynomials $a,\ b \in K[x]$ such that

$$d = af + bg.$$

According to Week 2 Proposition 2.4, the polynomial on the right hand side is an element of $\langle f, g\rangle$, and therefore $d \in \langle f, g\rangle$. Again, since $\langle d\rangle$ is the smallest ideal containing d, this shows

$$\langle d\rangle \subset \langle f, g\rangle\,.$$

Putting together these two inclusions of ideals we get the result. □

1.2 Example

Consider the following polynomials in $\mathbf{Q}[x]$:

$$f = x^4 - 2x^2 + 1$$
$$g = x^3 + 1$$

Let's use the Euclidean algorithm to calculate $d = \gcd(f, g)$ and find a, b such that $d = af + bg$.

Step 1: Divide f by g to get

$$f = q_1 g + r_1 \quad \text{where}$$
$$q_1 = x$$
$$r_1 = -2x^2 - x + 1$$

Step 2: Divide g by r_1 to get

$$g = q_2 r_1 + r_2 \quad \text{where}$$
$$q_2 = -\frac{1}{2}x + \frac{1}{4}$$
$$r_2 = \frac{3}{4}x + \frac{3}{4}$$

Step 3: Divide r_1 by r_2 to get

$$r_1 = q_3 r_2 \quad \text{where}$$
$$q_3 = -\frac{8}{3}x + \frac{4}{3}$$

At this stage there is no remainder: $r_3 = 0$. So we **STOP**.

The GCD is the monic form of the last nonzero remainder:

$$\gcd(f, g) = \widehat{r_2} = x + 1.$$

To find a, $b \in \mathbf{Q}[x]$ such that $\gcd(f, g) = af + bg$ we reverse the steps above.

Rearranging Step 2 above we have

$$r_2 = g - q_2 r_1 \qquad (*)$$

Rearranging Step 1 we have

$$r_1 = f - q_1 g \qquad (**)$$

and substituting $(**)$ into $(*)$ we get

$$\begin{aligned} r_2 &= g - q_2(f - q_1 g) \\ &= -q_2 f + (1 + q_1 q_2) g \end{aligned}$$

Finally $\gcd(f, g) = \widehat{r_2} = \frac{4}{3} r_2$ so we have

$$\gcd(f, g) = \left(-\frac{4}{3} q_2\right) f + \frac{4}{3} (1 + q_1 q_2)\, g$$

So the polynomials we are looking for are

$$\begin{aligned} a &= \left(-\frac{4}{3} q_2\right) = \frac{2}{3} x - \frac{1}{2} \\ b &= \frac{4}{3} (1 + q_1 q_2) = -\frac{2}{3} x^2 + \frac{1}{3} x + \frac{4}{3}. \end{aligned}$$

2 Common roots and multiple roots

In this section we will see that the greaest common divisor allows us to determine whether two polynomials have a common root, **without** first finding all the roots of the two polynomials.

Proposition 2.1. *Let* $f,\ g \in K[x]$ *be two polynomials, and let* $d = \gcd(f, g)$. *If* k *is any element of* K*, then*

$$d(k) = 0 \Leftrightarrow f(k) = g(k) = 0.$$

In other words, the roots of the polynomial d are exactly the common roots of f and g.

Proof. By definition we know $d \mid f$ and $d \mid g$, which means that there are polynomials r and s such that

$$f = rd, \quad g = sd.$$

If $d(k) = 0$, then these equations show that $f(k) = g(k) = 0$ too. Conversely, Bézout's Identity (Corollary 1.3) shows that there exist polynomials $a,\ b \in K[x]$ such that

$$d = af + bg.$$

If $f(k) = g(k) = 0$, this equation shows that $d(k) = 0$. □

We can apply this to say something very useful about common roots in $\mathbf{C}$ of two complex polynomials:

Corollary 2.2. *If* $f,\ g \in \mathbf{C}[x]$*, then* f *and* g *have a common root in* $\mathbf{C}$ *if and only if* $d = \gcd(f, g)$ *is nonconstant.*

Proof. By the Proposition, f and g have a common root if and only if d has a root. A nonzero polynomial in $\mathbf{C}[x]$ has a root if and only if it is nonconstant, by the so-called *Fundamental Theorem of Algebra* [1]. □

Note that in the Corollary, we really need to consider **complex** roots of $\mathbf{C}$, even if for example f and g both have real coefficients.

2.1 Application: detecting multiple roots

In many practical situations, multiple roots of functions cause big problems when trying to do numerical computations. A simple example is **Newton's method** for iteratively finding roots of a one-variable function $f(x)$. This method works as follows: start with any value x_0, and then define a sequence (x_n) of better and better approximations to a root by setting

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

In well-behaved cases, the sequence (x_n) will then quickly converge to a limit x such that $f(x) = 0$, and we have found our root. (In practice we will have to stop after a finite number of steps, but we can determine how accurate the resulting approximation is.)

But what happens if x is a **multiple** root of f? At a multiple root, we have $f(x) = f'(x) = 0$, so as we approach x, both the numerator and denominator of the above fraction approach zero. As a result, the sequence (x_n) can then become unstable, and convergence to the root is much slower.

The moral of the story is that in situations where accurately finding roots is important, it is a good idea to stick to functions without multiple roots! And the results above give a quick way to check this condition for polynomials.

Definition 2.3. *Let $f \in \mathbf{C}[x]$. We say that f has a* multiple root *at $z \in \mathbf{C}$ if*

$$f(z) = f'(z) = 0.$$

Applying Corollary 2.2 with $g = f'$, we then get our check for multiple roots:

Corollary 2.4. *Let $f \in \mathbf{C}[x]$ be a polynomial with derivative f'. Then the multiple roots of f are exactly the roots of $\gcd(f, f')$. In particular, f has a multiple root if and only if $\gcd(f, f')$ is nonconstant.*

2.2 Examples

Common Roots

Let's find the common roots (if any) of the two polynomials

$$f = x^5 - 6x + 3$$
$$g = x^4 - x - 6$$

Importantly, we can do this without first finding the roots of f and g!

Recall that if $d = \gcd(f, g)$, then the roots of d are exactly the common roots of f and g. Let's find d by using the Euclidean algorithm.

Step 1: Divide f by g to get

$$f = q_1 g + r_1 \quad \text{where}$$
$$q_1 = x$$
$$r_1 = x^2 + 3$$

Step 2: Divide g by r_1 to get

$$g = q_2 r_1 + r_2 \quad \text{where}$$
$$q_2 = x^2 - 3$$
$$r_1 = -x + 3$$

Step 3: Divide r_1 by r_2 to get

$$\begin{aligned} r_1 &= q_3 r_2 + r_3 \quad \text{where} \\ q_3 &= -x - 3 \\ r_3 &= 12 \end{aligned}$$

Step 4: Divide r_2 by r_3 to get

$$r_2 = \left(\frac{1}{12} r_2\right) r_3$$

So $r_4 = 0$ and we **STOP**.

We have $\gcd(f, g) = \widehat{r_3} = 1$. Since this is a nonzero constant polynomial, it has no roots. So f and g have no common roots.

Remark: In fact, there is no "algebraic" formula for the roots of $f = x^5 - 6x + 3$: this follows from a famous theorem of Galois.

Multiple Roots

Consider the polynomial

$$f = x^4 - 4x^3 + 5x^2 - 2x$$

Let's use Corollary 2.4 to find the multiple roots of f, or show it has none. (Again, we don't need to find all the roots of f to do this!) Corollary 2.4 tells us that multiple roots of f are exactly the common roots of f and its derivative

$$f' = 4x^3 - 12x^2 + 10x - 2.$$

Let's compute $d = \gcd(f, g)$ using the Euclidean algorithm.

Step 1: Divide f by f' to get

$$\begin{aligned} f &= q_1 f' + r_1 \quad \text{where} \\ q_1 &= \frac{1}{4}x - \frac{1}{4} \\ r_1 &= -\frac{1}{2}x^2 + x - \frac{1}{2} \end{aligned}$$

Step 2: Divide f' by r_1 to get

$$\begin{aligned} f' &= q_2 r_1 + r_2 \quad \text{where} \\ q_2 &= -8x + 8 \\ r_2 &= -2x + 2 \end{aligned}$$

Step 3: Divide r_1 by r_2 to get

$$\begin{aligned} r_1 &= q_3 r_2 \quad \text{where} \\ q_3 &= \frac{1}{4}x - \frac{1}{4} \end{aligned}$$

At this stage we find $r_3 = 0$ so we **STOP.** We have

$$\begin{aligned} \gcd(f, f') &= \widehat{r_2} \\ &= -\frac{1}{2}(-2x + 2) \\ &= x - 1. \end{aligned}$$

So the multiple roots of f are exactly the roots of $x - 1$, namely, $x = 1$.

We can check this: indeed

$$\begin{aligned} f &= x^4 - 4x^3 + 5x^2 - 2x \\ &= x(x-1)^2(x-2). \end{aligned}$$

This shows that $x = 1$ is indeed a double root of f and there are no other multiple roots.

References

[1] "Fundamental Theorem of Algebra". `https://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra`