Lecture notes of Algebra. Week 4

12. The Remainder Theorem and the Factor Theorem

Let $f(x) \in F[x]$, and $\alpha \in F$. We say that α is a *root* (or a *zero*) of $f(x)$ if $f(\alpha) = 0$. In other words, if we obtain zero after substituting α for x in $f(x) = a_n x^n + \cdots + a_1 x + a_0$, that is, computing $f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$.

We say that a polynomial $g(x)$ divides $f(x)$ if there is another polynomial $h(x)$ such that $f(x) = g(x) \cdot h(x)$. This occurs exactly when dividing $f(x)$ by $g(x)$ we obtain zero as the remainder.

LEMMA 22 (The Remainder Theorem and the Factor Theorem). *Let F be a field, $0 \neq f(x) \in F[x]$, $\alpha \in F$. Then*

(1) *$f(\alpha)$ equals the remainder of the division of $f(x)$ by $x - \alpha$;*
(2) *α is a root of $f(x)$ if, and only if, $x - \alpha$ divides $f(x)$.*

PROOF. Dividing $f(x)$ by $(x - \alpha)$ we obtain $f(x) = (x - \alpha) \cdot q(x) + r$, where r is either zero or a polynomial of degree less than 1, hence a constant $r \in F$ in both cases. Evaluating on α we find $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r = r$, which proves the remainder theorem.

The Factor Theorem is an immediate consequence: the equality $f(x) = (x-\alpha)\cdot q(x)+r$ shows that $x - \alpha$ divides $f(x)$ (exactly) if, and only if, $r = 0$; but $r = f(\alpha)$ according to the remainder theorem. □

A nice application of the Factor Theorem arises when $f(x) = x^n \pm a^n$, where $a \neq 0$ is a constant. Because $f(a) = a^n \pm a^n$ and $f(-a) = (-1)^n a^n \pm a^n$ the Factor Theorem implies:

- $x^n - a^n$ is always divisible by $x - a$;
- $x^n - a^n$ is divisible by $x + a$ exactly when n is even;
- $x^n + a^n$ is divisible by $x + a$ exactly when n is odd;
- $x^n + a^n$ is never divisible by $x - a$.

For example,

$$x^2 - a^2 = (x - a)(x + a)$$
$$x^3 - a^3 = (x - a)(x^2 + ax + a^2)$$
$$x^3 + a^3 = (x + a)(x^2 - ax + a^2)$$
$$x^4 - a^4 = (x - a)(x^3 + ax^2 + a^2 x + a^3) = (x + a)(x^3 - ax^2 + a^2 x - a^3)$$

Note, however, that if we had to factorise $x^4 - a^4$ it would be smarter to think of it as $(x^2)^2 - (a^2)^2$, and so

$$x^4 - a^4 = (x^2 - a^2)(x^2 + a^2) = (x - a)(x + a)(x^2 + a^2).$$

Note also that, if $a \in \mathbb{R}$ and we work over the real numbers, $x^2 + a^2$ cannot be further factorised, again because of the Factor Theorem, since it cannot have any real roots: whatever real value we assign to x will make $x^2 + a^2$ a positive number, hence never zero. Over the complex numbers, however, we have

$$x^4 - a^4 = (x - a)(x + a)(x - ai)(x + ai),$$

as ai and $-ai$ are the square roots of $-a^2$. (Every polynomial in $\mathbb{C}[x]$ can be factorised into a product of factors of degree 1, this is called *the Fundamental Theorem of Algebra*.)

Similarly, if we have to factorise $x^6 - a^6$, we best proceed as follows:

$$\begin{aligned} x^6 - a^6 &= (x^3)^2 - (a^3)^2 \\ &= (x^3 - a^3)(x^3 + a^3) \\ &= (x - a)(x^2 + ax + a^2)(x + a)(x^2 - ax + a^2). \end{aligned}$$

Over the real numbers the two quadratic factors cannot be further factorised, because they have negative discriminant $a^2 - 4a^2 = -3a^2$. Starting, instead, with

$$\begin{aligned} x^6 - a^6 &= (x^2)^3 - (a^2)^3 \\ &= (x^2 - a^2)(x^4 + a^2x^2 + a^4) \\ &= (x - a)(x + a)(x^4 + a^2x^2 + a^4), \end{aligned}$$

would not have been as good, because none of the above rules applies directly to further factorise the factor of degree four. However, there is another trick which can be very useful in certain situations, namely,

$$\begin{aligned} x^4 + a^2x^2 + a^4 &= (x^4 + 2a^2x^2 + a^4) - a^2x^2 \\ &= (x^2 + a^2)^2 - (ax)^2 \\ &= (x^2 - ax + a^2)(x^2 + ax + a^2), \end{aligned}$$

and so we would recover the complete (or full) factorisation of $x^6 - a^6$ as before. This trick also allows us to factorise $x^6 + a^6$, where writing it as $(x^3)^2 + (a^3)^2$ would have been a dead end:

$$x^6 + a^6 = (x^2 + a^2)(x^4 - a^2x^2 + a^4).$$

One could show that this is a complete factorisation over the rational numbers (if a is rational), but over the real numbers the same trick factorises the factor of degree four:

$$\begin{aligned} x^4 - a^2x^2 + a^4 &= (x^4 + 2a^2x^2 + a^4) - 3a^2x^2 \\ &= (x^2 + a^2)^2 - (\sqrt{3}ax)^2 \\ &= (x^2 - a\sqrt{3}x + a^2)(x^2 + a\sqrt{3}x + a^2). \end{aligned}$$

13. Ruffini's rule

Because of the Factor Theorem, the very special case of polynomial division where we divide by a binomial of the form $x - a$, for some constant a, is important. In this case the ordinary division algorithm is very sparse, and all the numbers involved can be arranged in a more compact notation, which we illustrate by an example: to divide $f(x) = x^4 + 3x^3 - 5x - 10$ by $x - 2$ we write

$$\begin{array}{c|cccc|c} & 1 & 3 & 0 & -5 & -10 \\ 2 & & 2 & 10 & 20 & 30 \\ \hline & 1 & 5 & 10 & 15 & 20 \end{array}$$

and conclude that $x^4 + 3x^3 - 5x - 10 = (x^3 + 5x^2 + 10x + 15)(x - 2) + 20$. This method of performing the division is called *Ruffini's method* (or *Ruffini's rule*). (An extension of it exists, called *synthetic division,* which allows division by any monic polynomial rather than a special binomial $x - a$.)

According to the Factor Theorem, the remainder 20 of the division equals $f(2)$, and so this algorithm can also be used to *evaluate* a polynomial $f(x)$ on a number a (that is, to compute $f(a)$). This algorithm (called *Horner scheme,* but equivalent to Ruffini's rule), which really amounts to rewriting $x^4 + 3x^3 - 5x - 10$ as

$$((((x + 3)x + 0)x - 5)x - 10,$$

is more efficient than the obvious one (computing the various powers of 2, multiplying them by the corresponding coefficients, and then adding up the results), as it requires the same number of addition, but about half as many multiplications. Not a drastic saving, but significant.

Exercise. For a generic polynomial $f(x)$ of degree n (that is, avoiding special cases where some coefficient is zero), exactly how many additions and how many multiplications are required to compute $f(a)$ by the two methods?

Example. Continuing with a previous example, we already know that $f(x) = x^n - a^n$ is divisible by $x - a$. In fact, dividing by means of Ruffini's rule we find remainder zero:

$$\begin{array}{c|ccccc|c} & 1 & 0 & 0 & \cdots & 0 & -a^n \\ a & & a & a^2 & \cdots & a^{n-1} & a^n \\ \hline & 1 & a & a^2 & \cdots & a^{n-1} & 0 \end{array}$$

But Ruffini's rule also gives us the quotient, and so we find

$$x^n - a^n = (x - a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}).$$

Of course this identity could be easily verified directly by executing the multiplication on the RHS, but the point is that Ruffini's rule produces the quotient very quickly. When

n is odd (and only then) a similar identity

$$x^n + a^n = (x + a)(x^{n-1} - ax^{n-2} + \cdots - a^{n-2}x + a^{n-1})$$

can be obtained by applying Ruffini's rule to divide $f(x) = x^n + a^n$ by $x + a$, but it is quicker to deduce the identity by replacing a with $-a$ in the previous identity.

14. Expansion of a polynomial in terms of $x - a$

The following example illustrates how iterating Ruffini's rule we can expand a polynomial in x into powers of $x - a$, that is, if we like, into *a polynomial in* $x - a$. Say we want to expand $f(x) = x^3 + 2x^2 - x - 3$ into powers of $x - 2$. Then we do the following: we divide $f(x)$ by $x - 2$, then we divide the resulting quotient by $x - 2$, then we divide the resulting quotient by $x - 2$, and so on until the quotient is zero.

	1	2	−1	−3
2		2	8	14
	1	4	7	**11**
2		2	12	
	1	6	**19**	
2		2		
	1	**8**		
2				
	1			

The final result of this calculation is that

$$x^3 + 2x^2 - x - 3 = 1(x - 2)^3 + 8(x - 2)^2 + 19(x - 2) + 11.$$

The reason why it works is that the term 11 can be obtained as the remainder of dividing the polynomial by $x - 2$, which is done via Ruffini's rule. The quotient $x^2 + 4x + 7$ of this division is eventually going to be written as $1(x - 2)^2 + 8(x - 2) + 19$, and hence 19 can be obtained as the quotient of dividing it by $x - 2$. And so on.

Of course an alternative way of expanding a polynomial into powers of $x - a$ is substituting $x = y + a$ into it, then expanding the various powers of $y + a$ involved, thus converting it into a polynomial in y after the appropriate simplifications, and finally set $y = x - a$. This procedure, however, involves more operations and hence is computationally less efficient.[5]

[5]The way described of expanding a polynomial in terms of $x - a$ is analogous to the efficient way to convert an integer from decimal to another base b, which was described earlier in the notes.

15. Divisibility, GCD, and the Euclidean algorithm for polynomials

Divisibility, GCD and lcm, and the Euclidean algorithm, work for polynomials with coefficients in a field F very much the same as they do for integers, with only small adjustments. To begin with, divisibility, divisors, etc., are defined in the same way:

DEFINITION 23 (Divisibility for polynomials). Let $f(x)$ and $g(x)$ be polynomials with coefficients in a field F. We say that $g(x)$ divides $f(x)$, and we write $g(x) \mid f(x)$, if there is a polynomial $h(x) \in F[x]$ such that $f(x) = g(x) \cdot h(x)$.

With polynomials, if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $g(x) = c \cdot f(x)$ for some nonzero constant c. In fact, the nonzero constants play the same role in $F[x]$ as ± 1 play in $\mathbb{Z}$: they are exactly the elements which are *invertible,* that is, which have an *inverse* (belonging to the same set). This means that the only polynomials $c(x)$ such that there is a polynomial $d(x)$ with $c(x) \cdot d(x) = 1$, are exactly the nonzero constant polynomials $c(x)$ (which, being constants, we may simply write as c). To show this rigorously, taking the degrees in the equality $c(x) \cdot d(x) = 1$ gives us $\deg\big(c(x)\big) + \deg\big(d(x)\big) = 0$, which can only happen if $\deg\big(c(x)\big) = \deg\big(d(x)\big) = 0$, that is, $c(x)$ is a nonzero constant polynomial (and so is $d(x)$).

The greatest common divisor of two polynomials $f(x)$ and $g(x)$ is defined in the same way as for the integers:

DEFINITION 24 (Greatest common divisor). Let $f(x)$ and $g(x)$ be polynomials with coefficients in a field F (hence $f(x), g(x) \in F[x]$, in a formula). A polynomial $d(x) \in F[x]$ is called *a greatest common divisor* of $f(x)$ and $g(x)$ if

(1) $d(x)$ divides $f(x)$ and $g(x)$, and
(2) if $c(x) \in F[x]$ is any polynomial which divides both $f(x)$ and $g(x)$, then $c(x)$ divides $d(x)$.

REMARK. Beware that this is different from the definition given in Part II, Chapter 2, of the recommended book by Childs. The definition given there is more in the style of a 'school' definition, but the one we give here has the advantage of being (essentially) the same for integers, for polynomials, and for other contexts: whenever you have a concept of divisibility, there is a concept of *a* greatest common divisor (which need not be precisely unique).

A greatest common divisor of $f(x)$ and $g(x)$, denoted by $\big(f(x), g(x)\big)$, is only unique up to multiplying it by a nonzero constant. Hence saying that the GCD of two polynomials is $x+3$ is equivalent to saying that it is $2x+6$, or $\frac{1}{3}x+1$, etc. Among all those equivalent GCD's one usually chooses the one which is monic. (This is similar to choosing the positive greatest common divisors of two integers, rather than its opposite.) As we do

for integers, if two polynomials $f(x)$ and $g(x)$ have greatest common divisor 1 then we say that they are *coprime*.

The Euclidean algorithm and the extended Euclidean algorithm work for polynomials in the same way as for the integers. Hence, given two polynomials $f(x)$ and $g(x)$, with $\deg\big(f(x)\big) \geq \deg\big(g(x)\big)$ (otherwise we just swap the two polynomials), we start the algorithm by dividing the first polynomials by the second:

$$f(x) = g(x)q_1(x) + r_1(x), \qquad \text{with } \deg\big(r_1(x)\big) < \deg\big(g(x)\big).$$

Then we divide $g(x)$ by the first remainder $r_1(x)$,

$$g(x) = r_1(x)q_2(x) + r_2(x), \qquad \text{with } \deg\big(r_2(x)\big) < \deg\big(r_1(x)\big),$$

and repeat the procedure until some remainder is zero. The last nonzero remainder is then the GCD of the two polynomials. As in the case of integers, this is justified by noting the following basic fact: if $f(x) = g(x)q(x)+r(x)$ then $\mathrm{GCD}\big(f(x), g(x)\big) = \mathrm{GCD}\big(g(x), r(x)\big)$. Hence if $r_i(x)$ is the last nonzero remainder, then $\mathrm{GCD}\big(f(x), g(x)\big) = \mathrm{GCD}\big(g(x), r_1(x)\big) = \mathrm{GCD}\big(r_1(x), r_2(x)\big) = \cdots = \mathrm{GCD}\big(r_i(x), 0\big) = r_i(x)$.

The number of divisions required by the Euclidean algorithm on polynomials is at most the lower of the degrees of the two polynomials. This is easy to see as the degree of each remainder is less than the degree of the previous remainder.

Example. We compute the GCD of the polynomials $x^3 + 2x^2 + x$ and $x^2 + x - 1$ using the Euclidean algorithm:

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

The remainder of the second division is -1, so there is no point in doing a third division, as dividing by -1 (or by 1, or $2/3$, or any nonzero rational number) would give remainder zero. Hence the last nonzero remainder is -1, and so GCD of x^3+2x^2+x and x^2+x-1 is 1. In words, those polynomials are coprime.

Example. We compute the GCD of the polynomials $x^{3n} - 1$ and $x^{2n} - 1$, where n is any positive integer. The Euclidean algorithm reads:

$$\begin{aligned} x^{3n} - 1 &= (x^{2n} - 1) \cdot x^n + (x^n - 1) \\ x^{2n} - 1 &= (x^n - 1) \cdot (x^n + 1). \end{aligned}$$

Hence the last nonzero remainder is $x^n - 1$, and so GCD of $x^{3n} - 1$ and $x^{2n} - 1$ is $x^n - 1$.

We should have known from the start that $x^n - 1$ divides both polynomials. In fact $x^{3n} - 1 = (x^n - 1)(x^{2n} + x^n + 1)$ follow from the general identity $x^3 - a^n = (x - a)(x^2 + ax+a^2)$. Similarly, we should have known that $x^{2n}-1 = (x^n-1)(x^n+1)$. Knowing these factorisations, another way to prove that $x^2 - 1$ is actually the *greatest* common divisor

of $x^{3n}-1$ and $x^{2n}-1$ (rather than just *a* common divisor) would then be showing that $x^{2n}+x^n+1$ and x^n+1 are coprime. Of course we can do that by applying the Euclidean algorithm, which in this case consists of a single division: $x^{2n}+x^n+1=(x^n+1)\cdot x^n+1$. This tells us that their GCD is 1, and so the GCD of $x^{3n}-1$ and $x^{2n}-1$ is x^n-1.

REMARK. One can actually prove that for any positive integers m and n the greatest common divisor of x^m-1 and x^n-1 is $x^{(m,n)}-1$ (where the exponent (m,n) means the GCD of m and n, as usual).

The conclusion of the extended Euclidean algorithm can be formally stated as Bézout's Lemma for polynomials:

LEMMA 25 (Bézout's Lemma for polynomials). *Let $f(x), g(x) \in F[x]$, where F is a field, and let $d(x) = \big(f(x), g(x)\big)$ be their greatest common divisor. Then there exist polynomials $u(x), v(x) \in F[x]$ such that*

$$f(x)\,u(x) + g(x)\,v(x) = d(x).$$

It is not difficult to show that if neither $f(x)$ or $g(x)$ is the zero polynomial then the polynomials $u(x)$ and $v(x)$ produced by the extended Euclidean algorithm satisfy

$$\deg\big(u(x)\big) < \deg\big(g(x)\big) \qquad \text{and} \qquad \deg\big(v(x)\big) < \deg\big(f(x)\big).$$

EXAMPLE. Reading the divisions in the previous example backwards we find:

$$\begin{aligned}
1 &= -(x^2+x-1) + (x+1)\cdot x \\
&= -(x^2+x-1) + [(x^3+2x^2+x) - (x^2+x-1)\cdot(x+1)]\cdot x \\
&= (x^3+2x^2+x)\cdot x + (x^2+x-1)\cdot[-1-(x+1)x] \\
&= (x^3+2x^2+x)\cdot x + (x^2+x-1)\cdot(-x^2-x-1).
\end{aligned}$$

So we have found find two polynomials $u(x)$ and $v(x)$ such that

$$(x^3+2x^2+x)\cdot u(x) + (x^2+x-1)\cdot v(x) = 1,$$

namely,

$$u(x) = x, \quad \text{and} \quad v(x) = -x^2-x-1.$$

Note that these polynomials satisfy

$$\frac{1}{(x^3+2x^2+x)(x^2+x-1)} = \frac{u(x)}{x^2+x-1} + \frac{v(x)}{x^3+2x^2+x}.$$

Hence the extended Euclidean algorithm has allowed us to write the fraction on the LHS as a sum of the two 'simpler' fractions on the RHS. Note that in each of the two fractions on the RHS the numerator has degree strictly less than the denominator. This is a particular instance of the general fact on the degrees of $u(x)$ and $v(x)$ mentioned before the example.

EXAMPLE. We compute the *monic* greatest common divisor $d(x)$ of $x^3 - x^2 + x - 6$ and $x^3 + x - 10$:

$$\begin{aligned} x^3 - x^2 + x - 6 &= (x^3 + x - 10) \cdot 1 + (-x^2 + 4) \\ x^3 + x - 10 &= (x^2 - 4) \cdot x + (5x - 10) \\ x^2 - 4 &= (x - 2)(x + 2). \end{aligned}$$

The last nonzero remainder is $5x - 10 = 5(x - 2)$, and so the *monic* GCD is $d(x) = (x^3 - x^2 + x - 6, x^3 + x - 10) = x - 2$. Of course it would also be correct to say that a GCD is $5x - 10$, as much as $\frac{1}{2}x - 2$, or $-\frac{2}{3}x + \frac{4}{3}$, etc., but as a standard way of choosing one we have asked for the *monic* GCD, which is $x - 2$.

Now we carry out the extended part of the Euclidean algorithm, by reading those divisions backwards, and we find

$$\begin{aligned} 5x - 10 &= (x^3 + x - 10) - (x^2 - 4) \cdot x \\ &= (x^3 + x - 10) + [(x^3 - x^2 + x - 6) - (x^3 + x - 10) \cdot 1] \cdot x \\ &= (x^3 + x - 10) \cdot x - (x^3 + x - 10) \cdot (x - 1) \end{aligned}$$

So we have found polynomials $u(x)$ and $v(x)$ whose existence is stated in Bézout's Lemma: $u(x) = \frac{1}{5}x$ and $v(x) = -\frac{1}{5}(x - 1)$ satisfy

$$(x^3 - x^2 + x - 6) \cdot u(x) + (x^3 + x - 10) \cdot v(x) = d(x) = x - 2.$$

EXAMPLE. When the GCD of two polynomials is not 1, as in the previous example, there is an alternative way to proceed with the extended Euclidean algorithm in order to have simpler calculations: once we have found that $(x^3 - x^2 + x - 6, x^3 + x - 10) = x - 2$, we may divide both polynomials by their GCD $x - 2$ and factorise them as follows:

$$\begin{aligned} x^3 - x^2 + x - 6 &= (x - 2)(x^2 + x + 3) \\ x^3 + x - 10 &= (x - 2)(x^2 + 2x + 5). \end{aligned}$$

We see from these factorisations that there was nothing special about the 5 coefficients in the GCD $5x - 10$ which we found using the Euclidean algorithm on the original polynomial, as there is no trace of that in the factorisations.

Now we carry out the extended Euclidean algorithm using the quotients by $x - 2$ instead of our original polynomials:

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

Hence the GCD of those polynomials is 1 (or 5, or 2/3 if you like, they all mean the same in this polynomial context, because all nonzero constants are invertible in $\mathbb{Q}[x]$). Reading

the divisions backwards we find:

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

So we have found the same $u(x) = \frac{1}{5}x$ and $v(x) = -\frac{1}{5}(x-1)$ as before. In fact, those polynomials satisfy

$$(x^2+x+3)\cdot u(x) + (x^2+2x+5)\cdot v(x) = 1,$$

and if we multiply both sides of this equality by $x-2$ we recover

$$(x^3-x^2+x-6)\cdot u(x) + (x^3+x-10)\cdot v(x) = x-2,$$

which we obtained the first time.

Note that *it would not be possible* to find polynomials $s(x)$ and $t(x)$ such that

$$(x^3-x^2+x-6)\cdot s(x) + (x^3+x-10)\cdot t(x) = 1,$$

because x^3-x^2+x-6 and x^3+x-10 are not coprime. In fact, each of them is a multiple of $x-2$, so the left-hand side is as well, but the right-hand side 1 is not, so that is impossible.