16. The division algorithm

Note that if $f(x) = g(x)h(x)$ then α is a zero of $f(x)$ if and only if α is a zero of one of $g(x)$ or $h(x)$. It is very useful therefore to write $f(x)$ as a product of polynomials.

What we need to understand is how to divide polynomials:

Theorem 16.1 (Division Algorithm)**.** *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum a_i x^i$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum b_i x^i$$

be two polynomials over a field F of degrees n and $m > 0$.

Then there are unique polynomials $q(x)$ and $r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof. We proceed by induction on the degree n of $f(x)$. If the degree n of $f(x)$ is less than the degree m of $g(x)$, there is nothing to prove, take $q(x) = 0$ and $r(x) = f(x)$. Suppose the result holds for all degrees less than the degree n of $f(x)$.

Put $q_0(x) = cx^{n-m}$, where $c = a_n/b_m$. Let $f_1(x) = f(x) - q_1(x)g(x)$.

Then $f_1(x)$ has degree less than g. By induction then,

$$f_1(x) = q_1(x)g(x) + r(x),$$

where $r(x)$ has degree less than $g(x)$. It follows that

$$\begin{aligned} f(x) &= f_1(x) + q_0(x)f(x) \\ &= (q_0(x) + q_1(x))f(x) + r(x) \\ &= q(x)f(x) + r(x), \end{aligned}$$

where $q(x) = q_0(x) + q_1(x)$. □

Note that this is the usual algortihm. Attack the leading terms first, get some sort of approximation to the quotient, find the difference and keep going. As usual, we will call $q(x)$ the quotient and $r(x)$ the remainder.

Example 16.2. *Let's find the quotient and the remainder when we divide $f(x) = x^7 + 2x^6 + 3x^5 + 4x^4 + x^3 + 4x + 3$ by $g(x) = x^3 + 2x + 1$, where we consider these polynomials inside the polynomial ring $\mathbb{Z}_5[x]$.*

We present this the usual way:

So the remainder is x^2+x+1 and the quotient is $x^4+2x^3+x^2+4x+2$,

$$x^7+2x^6+3x^5+4x^4+x^3+4x+3 = (x^4+2x^3+x^2+4x+2)(x^3+2x+1)+(x^2+x+1).$$

Corollary 16.3. *$\alpha \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - \alpha$ is a factor of $f(x)$.*

Proof. Suppose that $x - \alpha$ is a factor of $f(x)$. Then we may find $g(x) \in F[x]$ such that $f(x) = (x-\alpha)g(x)$. If we apply the function ϕ_α, evaluation at α, then we get

$$\begin{aligned}\phi_\alpha(f(x)) &= \phi_\alpha((x-a)g(x)) \\ &= \phi_\alpha(x-a)\phi_\alpha(g(x)) \\ &= (\alpha-\alpha)\phi_\alpha(g(x)) \\ &= 0\phi_\alpha(g(x)) \\ &= 0.\end{aligned}$$

Conversely suppose that α is a zero of $f(x)$. By the division algortihm we may find $q(x)$ and $r(x)$ such that

$$f(x) = q(x)(x-a) + r(x),$$

where either $r(x)$ is zero or its degree is zero. Thus $r(x) = r_0$ is a constant, possibly zero. If we apply the function ϕ_α, evaluation at α, then we get

$$\begin{aligned}\phi_\alpha(f(x)) &= \phi_\alpha(q(x)(x-a) + r(x)) \\ &= \phi_\alpha(x-a)\phi_\alpha(q(x)) + \phi_\alpha(r(x)) \\ &= r_0 \\ &= 0.\end{aligned}$$

Thus $r(x) = 0$ and so $x - \alpha$ is a factor of $f(x)$. □

Example 16.4. *Let's look at*

$$x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x].$$

First note that 1 is a zero of this polynomial. So by (16.3), we may write

$$x^4 + 3x^3 + 2x + 4 = (x-1)f_1(x).$$

Let's find $f_1(x)$ using the division algortihm:

$$x^4 + 3x^3 + 2x + 4 = (x-1)(x^3 + 4x^2 + 4x + 1).$$

Note that 1 is again a zero of $x^3 + 4x^2 + 4x + 1$. So by (16.3), we may write

$$x^3 + 4x^2 + 4x + 1 = (x-1)f_2(x).$$

Let's find $f_2(x)$ using the division algortihm:

$$x^3 + 4x^2 + 4x + 1 = (x-1)(x^2+4).$$

Note that 1 is yet again a zero of x^2+4. So by (16.3), we may write

$$x^2 + 4 = (x-1)f_3(x).$$

Let's find $f_3(x)$ using the division algortihm:

$$x^2 + 4 = (x-1)(x+1).$$

Putting all of this together, it follows that

$$x^4 + 3x^3 + 2x + 4 = (x-1)^3(x+1).$$

Corollary 16.5. *A non-zero polynomial $f(x) \in F[x]$ of degree n has at most n zeroes in F.*

Proof. By induction on the degree of $f(x)$. If $f(x)$ has degree zero then $f(x)$ is a non-zero constant and so $f(x)$ has no zeroes.

Otherwise if α is a zero of $f(x)$ then (16.3) implies that $x - \alpha$ is a factor of $f(x)$. So we can write

$$f(x) = (x-\alpha)g(x),$$

where $g(x)$ has degree $n-1$. By induction $g(x)$ has at most $n-1$ zeroes and so $f(x)$ has at most n zeroes, the zeroes of $g(x)$ plus one more for α if it is not a zero of $g(x)$. □

Corollary 16.6. *If G is a finite subgroup of the multiplicative group F^* of non-zero elements of F then G is cyclic.*

Proof. By the Fundamental theorem of finitely generated abelian groups, G is isomorphic to a product of cyclic groups, of order a power of a prime,

$$G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}.$$

We will use multiplicative notation for the both the LHS and the RHS.

Let m be the least common multiple of $d_1, d_2, \ldots, d_r$. Then

$$m \leq d_1 d_2 \ldots d_r.$$

If $a_i \in \mathbb{Z}_{d_i}$ then $a^{d_i} = 1$ and so

$$a^m = 1$$

as d_i divides m.

Thus

$$\alpha^m = 1,$$

for all $\alpha \in G$. But then every element α of G is a zero of $x^m - 1$. As G has $d_1 d_2 \ldots d_r$ elements and a polynomial of degree m has at most m zeroes it follows that $m = d_1 d_2 \ldots d_r$. But this can only happen if

$d_1, d_2, \ldots, d_r$ are powers of distinct primes, in which case G is cyclic of order m. □

It might help to understand this argument by going through a concrete example:

Example 16.7. *Consider the non-zero elements G of $\mathbb{Z}_{181}$.*

Note that 181 is a prime, so that $\mathbb{Z}_{181}$ is a field. G is the set of all units which is a finite group. G has $180 = 181 - 1$ elements. The prime factorisation of

$$180 = 2^2 \cdot 3^2 \cdot 5.$$

G is a finite abelian group. So it is isomorphic to one of

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
(3) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
(4) $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

The last group is cyclic. We have to eliminate the other three cases. In the first case every element of G has order dividing $2 \cdot 3 \cdot 5 = 30$. In the second case every element has dividing $2 \cdot 9 \cdot 5 = 90$ and in the third case every element has order dividing $4 \cdot 3 \cdot 5 = 60$.

But if α has order dividing 30 it is a zero of $x^{30} - 1$; if α has order dividing 90 it is a zero of $x^{90} - 1$; and if α has order dividing 60 it is a zero of $x^{60} - 1$. As G has order 180 and a polynomial of degree 30, 90 and 60 has at most 30, 90 or 60 zeroes, it follows that the first three cases cannot happen.

Thus the fourth case happens and G is cyclic.