Lecture 17

(*) Corollary A nonzero polynomial $f(x) \in F[x]$ of degree n has at most n roots in a field F

3.1 Factorisation, gcd

Recall that if $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then $f(x)$ is divisible by $g(x)$ over F if $f(x) = g(x)q(x)$ for some $q(x) \in F[x]$. That is, $f(x)$ is divisible by $g(x)$ if the remainder in the division of $f(x)$ by $g(x)$ is zero. (*) If $f(x)$ is divisible by $g(x)$ (over F) then we also say that $g(x)$ is a factor of $f(x)$ (over F). We can formulate the following familiar corollary to the remainder theorem.

Factor Theorem If $f(x) \in F[x]$ and $c \in F$ then $(x-c)$ is a factor of $f(x)$ if and only if $f(c) = 0$.

A field element c such that $f(c) = 0$ is called a root or a zero of the polynomial $f(x)$ over F.

We now continue our study of "similarities" between the ring of integers and a polynomial ring $F[x]$. We have seen that over $\mathbb{Z}$ we can perform the Euclidean algorithm to find the greatest common divisor of two integers. We can give an analogous definition & result for polynomials over a field.

Theorem (Existence and uniqueness of gcd in $F[x]$)

If $a(x)$ and $b(x)$ are polynomials over a field F, not both zero, then there is a unique monic polynomial $d(x)$ over F such that

1. $d(x) \mid a(x)$ and $d(x) \mid b(x)$, and
2. if $c(x)$ is a polynomial such that $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$

In analogy with $\mathbb{Z}$, the polynomial $d(x)$ is called the gcd of $a(x)$ and $b(x)$. Let's see in an example how the polynomial version of the Euclidean algorithm works:

Example $a(x) = x^4 - x^3 - x^2 + 1$ and $b(x) = x^3 - 1$ in $\mathbb{Q}[x]$

As usual, we will repeatedly write expressions of the form given by the division algorithm, changing the roles of the various polynomials at each step.

Step 1. $a(x) = b(x)q(x) + r_1(x)$ with $\deg r_1(x) < \deg b(x)$

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

Step 2. $$x^3 - 1 = (-x^2 + x)(-x - 1) + (x - 1) \quad (2)$$

$$\vdots \quad -x^2 + x = (x - 1)(-x) \quad (3)$$

As the remainder here is 0, $(x-1)$ is the desired gcd.

In the same way as for the gcd of two integers, one can use the Euclidean algorithm backwards to write the gcd as combination of the two polynomials:

Theorem If $a(x)$ and $b(x)$ are as before and $d(x) = \gcd(a(x), b(x))$ then there exist $u(x), v(x) \in F[x]$ such that

$$d(x) = a(x)u(x) + b(x)v(x)$$

We illustrate how it works using the steps from the example above.

Rewrite ① to get

$$-x^2+x \overset{(*)}{=} x^4-x^3\ x^2+1\ -(x^3-1)(x-1)$$

use this in ② where we "solved" for $x-1$

$$\begin{aligned} x-1 &= x^3-1-(-x^2+x)(-x-1) \\ &\overset{(*)}{=} (x^3-1)-\left[(x^4-x^3-x^2+1)-(x^3-1)(x-1)\right](-x-1) \\ &= (x^4-x^3-x^2+1)(x+1)+(x^3-1)\left[1-(x-1)(x+1)\right] \\ &= (x^4-x^3-x^2+1)(x+1)+(x^3-1)(-x^2+2) \end{aligned}$$

In the ring of integers a special role is played by prime numbers. We will soon define their natural analogues in this setting. Before that, we need the following definition.

Def Two polynomials $f(x)$ and $g(x)$ over a field are said to be associates if $f(x)=c\cdot g(x)$ for some nonzero element $c\in F[x]$.

Example • $2x^2-1$, $6x^2-3$ and $x^2-\frac{1}{2}$ are associates over $\mathbb{Q}$.

• $2x^2+1$ and x^2+3 are associates over $\mathbb{Z}_5$

The fact that for a field element there exists exactly one inverse tells us that each nonzero polynomial has exactly one monic associate.

If $f(x)\in F[x]$ then all its associates divide it, and so do all polynomials of degree 0.

The analogues of primes in $F[x]$ are exactly those polynomials which admit only these divisors:

Definition (Irreducible Polynomial) A nonconstant polynomial $f(x)\in F[x]$ is irreducible over F (or an irreducible polynomial in $F[x]$) if $f(x)$ cannot be expressed as product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)\in F[x]$ both of lower degree than the degree of $f(x)$.

If $f(x)\in F[x]$ is a nonconstant polynomial that is not irreducible over F then $f(x)$ is said to be reducible over F.

⚠ Both notions depend on the field. A polynomial can be irreducible over F but reducible over a bigger field.

Example x^2-2 is irreducible over $\mathbb{Q}$. It is, however, reducible over $\mathbb{R}$:

$$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$$

Example The polynomial $f(x)=x^3+3x+2\in\mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$.

To show this, note that if it were reducible there would be at least one linear (= of degree 1) factor. By the (corollary of the) remainder thm, this would imply that there exists $c\in\mathbb{Z}_5$ such that $f(c)=0$. By direct calculation:

$f(0)=2$, $f(1)=1$, $f(2)=1$, $f(3)=3$, $f(4)=3$. Therefore no polynomial of degree 1 divides $f(x)$ in $\mathbb{Z}_5[x]$, and thus $f(x)$ is irreducible over $\mathbb{Z}_5$

As we mentioned the irred polynomials over a field play the role of the primes in the ring of integers. For instance, the following holds.

Fact If F is a field and $a(x), b(x), p(x) \in F[x]$ with $p(x)$ irreducible over F and $p(x)$ divides $a(x) \cdot b(x)$ then $p(x)$ divides $a(x)$ or $p(x)$ divides $b(x)$.

which leads to the following analogue of the fundamental theorem of arithmetic:

Unique Factorisation Theorem Each polynomial of degree at least one over a field F can be written as an element of F times a product of monic irreducible polynomials over F. This factorisation is unique up to the order.

Example Consider the polynomial $f(x) = 3x^4 - 3x^2 - 6$ over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

over $\mathbb{Q}$: $f(x) = 3(x^4 - x^2 - 2) = 3(x^2 - 2)(x^2 + 1)$ and the factors on the RHS are all irreducible over $\mathbb{Q}$.

over $\mathbb{R}$ $x^2 - 2$ splits, so $f(x) = 3(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$ " " over $\mathbb{R}$

Finally, over $\mathbb{C}$ $f(x) = 3(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$