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

A natural question is now the following: what are the irreducibles over the various fields?

- Over $\mathbb{C}$, a polynomial is irreducible if and only if it has degree 1 (the fundamental theorem of algebra tells us that over $\mathbb{C}$ a polynomial of deg n has exactly n roots)
- Over $\mathbb{R}$ the degree of an irreducible polynomial is either 1 or 2. The irreducibles of degree 2 are those polynomials $ax^2 + bx + c$ with $b^2 - 4ac < 0$.
- Over $\mathbb{Q}$?

Lecture 18

3.2 Factorisation of Polynomials over a field.

We have seen in an example that when a polynomial f over a field F has low degree, the remainder (or factor) theorem tells us that to detect irreducibility is enough to check for the existence of roots.

Theorem Let $f \in F[X]$ be of degree 2 or 3. Then $f(x)$ is irreducible over F if and only if it has a zero in F.

As we have seen, this is easy to show as a factorisation of a polynomial of degree 2 or 3 must involve a factor of degree one.

Irreducibility over $\mathbb{Q}$ of polynomials in $\mathbb{Q}[X]$ is harder to detect. It is related to irreducibility in $\mathbb{Z}[X]$ by the following results.

As we discussed, over a field a polynomial belongs to a "family" of associates (i.e. polynomials obtained by multiplying by a non zero field element), and a polynomial is irreducible if and only if its associates are.

A polynomial over $\mathbb{Q}$ has in particular associates in $\mathbb{Z}[X]$.

Surprisingly, a polynomial $f(x) \in \mathbb{Z}[X]$ turns out to have a proper factorisation in $\mathbb{Q}[X]$ if and only if it has a proper factorisation (with factors of the same degree) in $\mathbb{Z}[X]$.

The latter is easier to detect.

Def A polynomial in $\mathbb{Z}[X]$ is called primitive if the gcd of all its coefficients is 1.

Example $2x^3 - 3x + 1$ is primitive

$2x^2 + 4x + 2$ is not

Theorem (Gauss's Lemma) Let $f(x)$ and $g(x)$ be primitive polynomials in $\mathbb{Z}[X]$. Then their product is again primitive.

With a lot of work, this can be used to show the result we announced:

Thm Suppose $f(x)$ is a polynomial of degree ≥ 2 in $\mathbb{Z}[X]$. Then $f(x)$ has a proper factorisation in $\mathbb{Q}[X]$ if and only if it has a proper factorisation in $\mathbb{Z}[X]$, with factors of the same degrees.

Slogan: we can forget about denominators!

Corollary If $f(x) = x^n + a_{n-1}x^{n-1} \ldots + a_0 \in \mathbb{Z}[X]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $\mathbb{Q}$ then $f(x)$ has a zero $m \in \mathbb{Z}$, and m divides a_0.

Indeed, if $f(x)$ has a zero $\alpha \in \mathbb{Q}$ (that is $f(\alpha) = 0$) then $x - \alpha$ divides $f(x)$, or better $x - \alpha$ appears as a factor of $f(x)$ over $\mathbb{Q}$. But by the results above $x - m$, for some $m \in \mathbb{Z}$, appears as a linear factor of $f(x)$ over $\mathbb{Z}$:

$$f(x) = (x - m)\left(x^{n-1} + \ldots + \frac{a_0}{m}\right)$$ but this is a factorisation over $\mathbb{Z}$

$$\Rightarrow \frac{a_0}{m} \in \mathbb{Z} \quad \text{so } m \text{ divides } a_0.$$

Example Decide whether $f(x) = x^4 - 2x^2 + 8x + 1$ as element of $\mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

By our thm above, if $f(x)$ has a linear factor over $\mathbb{Q}$ then it has one over $\mathbb{Z}$, which by the corollary must be a divisor (over $\mathbb{Z}$) of the constant term 1. The only possibilities are 1 and -1 but

$$f(1) = 1 - 2 + 8 + 1 \neq 0$$
$$f(-1) = 1 - 2 - 8 + 1 \neq 0$$

$\Rightarrow$ f doesn't have linear factors. A factorisation, if it exists, should therefore be of the form

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$ (we can do this directly in $\mathbb{Z}$ thanks to our thm!)

This leads to

$$x^4 + x^3(c+a) + x^2(ac+b+d) + x(ad+bc) + bd \overset{!}{=} f(x)$$

equating the coefficients:

$$\begin{cases} (1)\ a + c = 0 \\ (2)\ ac + b + d = -2 \\ (3)\ ad + bc = 8 \\ (4)\ bd = 1 \end{cases}$$ with $a, b, c, d \in \mathbb{Z}$!

So $bd = 1$ already tells us: $b = d = 1$ or $b = d = -1$

also, substituting $b = d$ in (3) we get $d(a+c) = 8$ which is incompatible with $a + c = 0$ (over $\mathbb{Z}$)

$\Rightarrow$ f is irreducible over $\mathbb{Q}$. ____ 11.11.19

For polynomials of higher degree, and under certain hypotheses, we can use the following.

Thm (Eisenstein Criterion) Let $p \in \mathbb{Z}$ be a prime.
Let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ with:

(*)
- $a_n \not\equiv 0 \mod p$
- $a_i \equiv 0 \mod p$ for $i = 0, \dots n-1$
- $a_0 \not\equiv 0 \mod p^2$

(that is: a_n is not divisible by p, all other coefficients are but a_0 is not divisible by p^2)

Then $f(x)$ is irreducible over $\mathbb{Q}$

Example. $2x^4 - 3x^3 + 6x + 12$ is irreducible over $\mathbb{Q}$. In fact, 3 divides a_3, a_1, a_0, doesn't divide a_4 and 9 doesn't divide 12.

(!) Nothing can be said (using this criterion) for polynomials in $\mathbb{Z}[x]$ for which no prime satisfies the requirements (*).

2018/19
- $x^4 - 8x^3 + 4x^2 - 6x - 2$ is irreducible over $\mathbb{Q}$: The prime 2 divides a_3, a_2, a_1, a_0 does not divide a_4 and 4 does not divide a_0.