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

$$f(x) = (x^2 + bx + b)(x^2 + cx + d)$$ (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 $f(x) = a_n x^n + .. + a_1 x + a_0 \in \mathbb{Z}[x]$ with:

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

(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 (*).

2019(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.

3.2 cont: Factorisation of polynomials

Here is a nice application of Eisenstein's criterion

Example The polynomial $\Phi_p(x) = \frac{x^p-1}{x-1} = 1+x+x^2\ldots+x^{p-1}$ is irreducible over $\mathbb{Q}$ for any prime p

Gauss's Lemma & its corollaries tell us that it is enough to show that $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$.

Once again, we use the "trick" of first looking for factorisations after substituting the indeterminate with a new one: call $\Psi_p(x) := \Phi_p(x+1)$ which means substitute $x+1$ for x in the polynomial $\Phi_p(x)$.

So $\Psi_p(x) = \frac{(x+1)^p-1}{x+1-1} = \frac{?}{x}$ (*) recall $(a+b)^n = a^n b^0 + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b + \ldots + \binom{n}{1}a^0 b^n$

where $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ is the binomial coefficient

so in the numerator of $\Psi_p(x)$ we will find coefficients of the form $\binom{p}{k}$ which are divisible by p for all k between 1 and $p-1$ (p is prime!)

$$(*) = \frac{x^p + x^{p-1}\cdot\binom{p}{p-1} + \ldots + \binom{p}{1}x + 1 - 1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \binom{p}{p-2}x^{p-3} \ldots + \binom{p}{1}\cdot 1 \quad (= p)$$

$$= x^{p-1} + \underbrace{\qquad}_{\text{intermediate summands w/ coeffs all divisible by } p} + p$$

The polynomial $\Psi_p(x)$ satisfies the Eisenstein criterion

$\Rightarrow \Psi_p(x)$ is irreducible over $\mathbb{Q}$.

How do we conclude that $\Phi_p(x)$ is then irreducible?

Suppose $\Phi_p(x) = f(x)\,g(x)$ were a proper factorisation of $\Phi_p(x)$ in $\mathbb{Z}[x]$ Then also

$\Psi_p(x) = \Phi_p(x+1) = f(x+1)\,g(x+1)$ would be a factorisation of $\Psi_p(x)$ in $\mathbb{Z}[x]$,

which we just proved does not exist $\Rightarrow \Phi_p(x)$ is irreducible for all p prime (over $\mathbb{Q}$)

Rmk $\Phi_p(x)$ is called the p-th cyclotomic polynomial.

3.3 Field extensions

We have seen that if a polynomial is irreducible over $\mathbb{Q}$ it might be reducible over $\mathbb{R}$, and it is (if degree >1) reducible over $\mathbb{C}$.

Intuitively, $\mathbb{C}$ is obtained from $\mathbb{R}$ by introducing "i" and taking all numbers of the form $a+bi$ for $a,b\in\mathbb{R}$. i is defined as the root of the polynomial x^2+1.

We won't mention how $\mathbb{R}$ is "obtained" from $\mathbb{Q}$, but it is a lot bigger than it's needed to get reducibility for one irreducible (over $\mathbb{Q}$) polynomial. In fact, one can mimic what done to get $\mathbb{C}$ from $\mathbb{R}$ in order to get fields that contain $\mathbb{Q}$ and over which a given polynomial becomes reducible.

The typical example is x^2-2. We know that over $\mathbb{R}$ this reduces to $(x-\sqrt{2})(x+\sqrt{2})$.

Is it the case that taking all numbers of the form $a+b\sqrt{2}$ for $a,b \in \mathbb{Q}$ we get a field over which x^2-2 is reducible? Yes (cf Problem 30)

This field is a "simple extension" of $\mathbb{Q}$, also denoted $\mathbb{Q}(\sqrt{2})$

In a field such as this one, multiplication and addition are the familiar ones. To compute the inverse of an element we can use a method very similar to that we use to find the inverse of a complex number.

For instance, in $\mathbb{Q}(\sqrt{5})$ the inverse of $3-\sqrt{5}$ is:

$$(3-\sqrt{5})^{-1} = \frac{1}{3-\sqrt{5}} = \frac{3+\sqrt{5}}{(3-\sqrt{5})(3+\sqrt{5})} = \frac{3+\sqrt{5}}{4} = \frac{3}{4}+\frac{1}{4}\sqrt{5}$$

which as we claimed is again of the form $a+b\sqrt{5}$ for some $a,b \in \mathbb{Q}$.