Recall:

Thm (The division algorithm)

Let F be a field and take $f(x), g(x) \in F[x]$, with $g(x) \neq 0$.

Then there exist unique polynomials $q(x), r(x) \in F[x]$ s.t.

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

with $\deg r(x) < \deg g(x)$.

Cor Let F be a field. Then $a \in F$ is a zero of $p(x) \in F[x]$ iff $x - a \in F[x]$ is a factor of $p(x)$ in $F[x]$.

Cor If F is a field, then a polynomial in $F[x]$ of degree n has at most n distinct roots in F.

(Proof.) If $x - \alpha$ is a factor of $p(x)$, then

$$p(x) = (x - \alpha)\, q(x),$$

for some $q(x) \in F[x]$. Then

$$\phi_\alpha(p(x)) = \phi_\alpha(x - \alpha) \cdot \phi_\alpha(q(x))$$
$$= 0 \cdot \phi_\alpha(q(x)) = 0,$$

So $p(x) \in \ker \phi_\alpha \Rightarrow \alpha$ is a zero of $p(x)$.

OTOH, $\forall\ \alpha$ is a zero of $p(x)$. i.e., $\phi_\alpha(p(x)) = 0$.

Division algorithm: $p(x) = (x-\alpha)q(x) + r(x)$,

for some $q(x), r(x) \in F[x]$ with

$$\deg r(x) = 0.$$

$\therefore r(x) = a \in F$ ← some fixed elt of the field

Then $0 = \phi_\alpha(p(x))$

$= \phi_\alpha((x-\alpha)q(x) + r(x))$

$= \phi_\alpha(x-\alpha) \cdot \phi_\alpha(q(x)) + \phi_\alpha(r(x))$

$= 0 \cdot \phi_\alpha(q(x)) + a$

$= a.$

So $r(x) = 0$, and $p(x) = (x-\alpha)q(x)$. ∎

Def. Let F be a field and fix $p(x), q(x) \in F[x]$.

Call a monic polynomial $d(x)$ a **greatest common divisor** for $p(x), q(x)$ if

1. $d(x) \mid p(x)$ and $d(x) \mid q(x)$;
2. for any $f(x) \in F[x]$ s.t. $f(x) \mid p(x)$ & $f(x) \mid q(x)$, we have $d(x) \mid f(x)$.

Call $p(x)$ & $q(x)$ **relatively prime** if $1 \in F[x]$ is a gcd for them.

Prop. Let F be a field, pick $p(x), q(x) \in F[x]$. Then there is a unique gcd $d(x)$ of $p(x)$ & $q(x)$ and there exist polynomials $r(x), s(x) \in F[x]$ s.t.

$$d(x) = r(x)p(x) + s(x)q(x).$$

Proof is very similar to version for $\mathbb{Z}$.

Irreducible polynomials

Def. Let F be a field. Call $p(x) \in F[x]$ **irreducible** if, for any factorization $p(x) = a(x)b(x)$, with $a(x), b(x) \in F[x]$, either $a(x)$ or $b(x)$ has degree 0.

Ex. ① degree 1 polynomials are always irreducible.

② $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible

As an element of $\mathbb{R}[x]$:

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

Similarly, $x^2 + 1$ is irreducible over $\mathbb{R}$, but not over $\mathbb{C}$.

(3) Consider $p(x) = x^3 + x^2 + 1 \in \mathbb{Z}_5[x]$.

$0+3$ ✓
$1+2$
$2+1$
$3+0$ ✓

$\deg p(x) = 3 \Rightarrow$ either has a linear factor or is irred.

If $p(x)$ has a linear factor in $\mathbb{Z}_5[x]$, then it has a root in $\mathbb{Z}_5$.

But

α	0	1	2	3	4
$p(\alpha)$	1	3	3	2	1

.

No zeros $\Rightarrow$ No linear factors $\Rightarrow$ irreducible.

[cubics
¡ quadratics.

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

No linear factors, but still reducible.

Think of irreducibles as polynomials whose zeros we can't see (unless they're linear).

We want to

(1) detect irreducibility;

(2) enhance our field so that we can see the zeros.

Lemma. Pick $p(x) \in \mathbb{Q}[x]$. There are integers

$$r, s, a_0, a_1, \ldots, a_n$$

s.t. ① $\gcd(r,s) = 1$;

② $\gcd(a_0, a_1, \ldots, a_n) = 1$;

③ $p(x) = \frac{r}{s}(\underbrace{a_0 + a_1 x + \cdots + a_n x^n}_{\in \mathbb{Z}[x]})$.

primitive

Thm (Gauss's lemma)

Suppose $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ both have positive degree and $\alpha(x)\beta(x) \in \mathbb{Z}[x]$ is monic. Then there are monic polynomials $a(x), b(x) \in \mathbb{Z}[x]$ s.t.

① $a(x)b(x) = \alpha(x)\beta(x)$;

② $\deg a(x) = \deg \alpha(x)$;

③ $\deg b(x) = \deg \beta(x)$.

Informally: Non-constant polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$ iff it's irreducible over $\mathbb{Q}$ and primitive in $\mathbb{Z}$.

(Proof.) By lemma,

$$\alpha(x) = \frac{c_1}{d_1}\alpha_1(x) \quad \& \quad \beta(x) = \frac{c_2}{d_2}\beta_1(x),$$

with $\gcd(c_i, d_i) = 1$ and $\alpha_1(x), \beta_1(x) \in \mathbb{Z}[x]$ are primitive.

Then $$\alpha(x)\beta(x) = \left(\frac{c_1}{d_1}\alpha_1(x)\right)\left(\frac{c_2}{d_2}\beta_1(x)\right)$$

$$= \frac{c}{d}\alpha_1(x)\beta_1(x),$$

with $\gcd(c,d) = 1$.

If $d = 1$ & $c = 1$, then $\alpha(x)\beta(x) = \alpha_1(x)\beta_1(x)$,

so the leading coefficient is given by

$$1 = a_m b_n.$$

$\therefore$ either $a_m = b_n = 1 \Rightarrow a(x) = \alpha_1(x)$, $b(x) = \beta_1(x)$

or $a_m = b_n = -1 \Rightarrow a(x) = -\alpha_1(x)$, $b(x) = -\beta_1(x)$.

$d = 1$ & $c = -1$ is similar.

If $d \neq 1$, pick p prime s.t. $p \mid d$ & $p \nmid c$.

B/c $\alpha_1(x)$ & $\beta_1(x)$ are primitive, each has

at least one coefficient not divisible by p.

So $\alpha_1(x) \xrightarrow{\text{reduce mod } p} \alpha_1'(x)$, $\beta_1(x) \rightsquigarrow \beta_1'(x)$ $\in \mathbb{Z}_p[x]$ nonzero.

But then we'd have

$$c\,\alpha_1'(x)\beta_1'(x) \equiv d\,\alpha(x)\beta(x) \equiv 0 \in \mathbb{Z}_p[x].$$

Since $\mathbb{Z}_p[x]$ is an I.D., this is a contradiction. ∎

Cor Let $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$, with $a_0 \neq 0$. If $p(x)$ has a zero in $\mathbb{Q}$, then $p(x)$ has a zero $\alpha \in \mathbb{Z}$, and α divides a_0.

(Proof.) $\S$ $a \in \mathbb{Q}$ is a zero of $p(x)$.

Then $x - a$ divides $p(x)$ in $\mathbb{Q}[x]$.

If $\deg p(x) = 1$, then $p(x) = x - a$.
$\therefore a \in \mathbb{Z}$ and we're done.

Otherwise, $p(x) = (x-a)\beta(x)$, for $\beta(x) \in \mathbb{Q}[x]$ with $\deg \beta(x) \geq 1$.

Gauss's lemma: $p(x) = \underbrace{(x-\alpha)(x^{n-1} + \cdots + b_1x + b_0)}_{\in \mathbb{Z}[x]}$.

So $\alpha \in \mathbb{Z}$ is a zero of $p(x)$.

Also, $-\alpha b_0 = a_0 \Rightarrow \alpha \mid a_0$. ∎

Exercise. Use the Thm & Corollary to show that $p(x) = x^4 - 2x^3 + x + 1$ is irreducible over $\mathbb{Q}$.

Thm. (Eisenstein's criterion)

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ and p is a prime s.t.

1. $p \mid a_i$, for $0 \le i \le n-1$;
2. $p \nmid a_n$;
3. $p^2 \nmid a_0$;

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