Day 23 July 9, 2024

Recall:

The division algorithm

Thm. Let F be a field and let $f(x), g(x) \in F[x]$, with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that
$$f(x) = g(x)q(x) + r(x),$$
where $\deg r(x) < \deg g(x)$.

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

(Proof.) Exercise using induction. $\blacksquare$

Def. Let F be a field and fix $p(x), q(x) \in F[x]$. We call a monic polynomial $d(x) \in F[x]$ a greatest common divisor of $p(x)$ and $q(x)$ if

- $d(x)$ divides $p(x)$ and $q(x)$ in $F[x]$;
- any polynomial in $F[x]$ which divides both $p(x)$ and $q(x)$ also divides $d(x)$.

We call $p(x)$ & $q(x)$ relatively prime if 1 is a greatest common divisor for $p(x)$ & $q(x)$.

Prop. Consider $p(x), q(x) \in F[x]$, with F a field. Then a unique greatest common divisor $d(x)$ for $p(x)$ & $q(x)$ exists, and there exist $r(x), s(x) \in F[x]$ s.t.
$$d(x) = r(x)p(x) + s(x)q(x).$$

Irreducibility

Def. Let F be a field. Then $p(x) \in F[x]$ is called 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 $x^2 - 2$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{R}$

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

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

Either $p(x)$ is $\underbrace{\text{irred. or it has a linear factor.}}_{\text{b/c } \deg p(x) = 3}$

linear factor $\longleftrightarrow$ root in $\mathbb{Z}_5$

$p(0) = 1$

$p(1) = 3$

$p(2) = 8 + 4 + 1 = 3$

$p(3) = 27 + 9 + 1 = 2$

$p(4) = 64 + 16 + 1 = 1$

No roots $\Rightarrow$ No linear factors $\Rightarrow$ irred.

Lemma. Pick $p(x) \in \mathbb{Q}[x]$. There exist integers $r, s, a_0, \ldots, a_n$ with $\gcd(r,s) = 1$ & $\gcd(a_0, \ldots, a_n) = 1$ such that

$$p(x) = \frac{r}{s}(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n).$$

We call a polynomial $a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ **primitive** if $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Thm. [Gauss's lemma]
Suppose $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ each have positive degree and $\alpha(x)\beta(x)$ has integer coefficients and 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. $\deg b(x) = \deg \beta(x)$.

(Proof.) By previous lemma,

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

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

$$\alpha(x)\beta(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x).$$

If $d = 1$, then $\alpha(x)\beta(x) = c\,\alpha_1(x)\beta_1(x)$, so the leading coeff. of the product is

$$1 = c\, a_m b_n.$$

So $c = \pm 1$.

If $c=1$, then either

$a_m = b_n = 1 \Rightarrow$ set $a(x) = \alpha_1(x)$ & $b(x) = \beta_1(x)$

OR $a_m = b_n = -1 \Rightarrow$ set $a(x) = -\alpha_1(x)$ & $b(x) = -\beta_1(x)$.

The case $c=-1$ is similar, but $\alpha_1(x)$ & $\beta_1(x)$ have opp. signs.

Finally we claim $d \neq 1$ is impossible.
If $d \neq 1$, pick a prime p which divides d, but does not divide c (since $\gcd(c,d)=1$).

$\alpha_1(x)$ & $\beta_1(x)$ primitive $\Rightarrow$ each has at least one coeff. not divisible by p.

Reduce everything mod p:

$$\alpha_1(x) \rightsquigarrow \tilde{\alpha}_1(x) \not\equiv 0 \pmod p$$
$$\beta_1(x) \rightsquigarrow \tilde{\beta}_1(x) \not\equiv 0 \pmod p$$

$$c\,\alpha_1(x)\,\beta_1(x) = d\,\alpha(x)\,\beta(x) \quad \text{in } \mathbb{Z}[x]$$

$$c\,\tilde{\alpha}_1(x)\,\tilde{\beta}_1(x) = d\,\alpha(x)\,\beta(x) \quad \text{in } \mathbb{Z}_p[x]$$
$$= 0, \text{ since } p \mid d.$$

This contradiction tells us that $d=1$. $\blacksquare$

Cor. Let $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ be a monic polynomial 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.)

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

Then

$$p(x) = (x-a)\,\beta(x),$$

for some $\beta(x) \in \mathbb{Q}[x]$ with $\deg \beta(x) \geq 1$.

By Gauss's lemma,

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

with $\alpha \in \mathbb{Z}$ and $b(x) \in \mathbb{Z}[x]$. The constant term is

$$a_0 = -\alpha \cdot b_0,$$

so α divides a_0. $\blacksquare$

Ex. Consider $p(x) = x^4 - 2x^3 + x + 1 \in \mathbb{Q}[x]$.

If $p(x)$ has a linear factor, it has a root in $\mathbb{Q}$. By prev. Corollary, it would have a root $\alpha \in \mathbb{Z}$ with $\alpha \mid 1$. i.e., $\alpha = \pm 1$.

But

$$p(1) = 1 \quad \& \quad p(-1) = 3,$$

so $p(x)$ has no rational roots, hence no linear factors in $\mathbb{Q}[x]$.

So either $p(x)$ is irreducible or it's the product of two quadratic factors.

Gauss:

$$p(x) = (x^2 + ax + b)(x^2 + cx + d),$$

with $a, b, c, d \in \mathbb{Z}$.

i.e.,

$$p(x) = x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.$$

Check: Matching this with $p(x)$ gives a system with no integer sol'ns.

So $p(x)$ is irreducible.

Thm. [Eisenstein's criterion]

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ admits a prime p such that

1. p divides a_i for $0 \leq i \leq n-1$;
2. p does not divide a_n;
3. p^2 does not divide a_0;

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

Ex. We can build an irreducible polynomial degree 6: Pick a prime — say $p = 3$ — and ensure that the conditions are satisfied.

$$15 + 81x - 18x^2 + 9x^3 - 27x^4 + 3x^5 + 4x^6$$

is irreducible over $\mathbb{Q}$.