Section 23 - Factorisation of polynomials

Let F be a field $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p)$, $f(x) = a_n x^n + \cdots + a_0 \in F[x]$.

General question: When is $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$?

If such equation holds, then

$f(x) = 0 \iff g(x) = 0$ or $h(x) = 0$,

$\{\text{zeros of } f\} = \{\text{zeros of } g\} \cup \{\text{zeros of } h\}$.

Division algorithm: Let $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_0$, $\in F[x]$ $m > 0$. There are unique $q(x), r(x) \in F[x]$ such that

(1) $f(x) = g(x)q(x) + r(x)$

(2) $\deg r(x) < \deg g(x)$, or $r(x) = 0$.

Example: Take $f(x) = x^4 + 1$, $g(x) = x^2 + 1 \in \mathbb{Z}_3[x]$.

$$x^4 + 1 : x^2 + 1 = x^2 - 1$$
$$x^4 + x^2$$
$$-x^2 + 1$$
$$-x^2 - 1$$
$$2$$

$q(x) = x^2 - 1$, $r(x) = 2$.

$$x^4 + 1 = (x^2 - 1)(x^2 + 1) + 2.$$

Thm If $r(x) = 0$, then $f(x) = q(x)g(x)$, & say $g(x)$ is a factor of $f(x)$.

Thm Let $f(x) \in F[x]$, $a \in F$. Then

a is a zero of $f(x) \iff x-a$ is a factor of $f(x)$.

Proof $\Leftarrow$: $f(x) = (x-a)q(x)$

$\Downarrow$

$f(a) = (a-a)q(a) = 0\,q(a) = 0.$

$\Rightarrow$ Assume $f(a)=0$. Write $f(x) = (x-a)q(x) + r(x)$, with $\deg r(x) < \deg x-a = 1$ or $r(x)=0$

Want to prove $r(x)=0$.

$\deg r(x) < 1 \Rightarrow r(x) = c, \quad c \in F.$

Then $0 = f(a) = (a-a)q(a) + r(a) = 0\,q(a) + c = c.$

$0 = c$

$0 = r(x).$

□

Example $f(x) = x^2+x+4 \in \mathbb{Z}_5[x]$. $f(2) = 2^2+2+4 = 4+2+4 = 0$,

so $x-2$ is a factor of $f(x)$.

Check

$$\begin{array}{r} x^2+x+4 : x-2 = x+3 \\ \underline{x^2-2x} \\ 3x+4 \\ \underline{3x-(2)(3)} \\ 0 \end{array}$$

$3x-(2)(3) = 3x-1 = 3x+4$

$x^2+x+4 = (x-2)(x+3) = (x-2)^2.$

Thm Let $f(x) \in F[x]$ have degree $n \geq 0$. Then $f(x)$ has at most n zeros in F.

Proof: Let $a_1, \ldots, a_r \in F$ be the zeros of $f(x)$. Then $x-a_1$ is a factor of $f(x)$, so

$f(x) = (x-a_1)\,q_1(x)$, $\deg q_1(x) = n-1$.

a $f(a_2)=0 \Rightarrow (a_2-a_1)\,q_1(a_2)=0 \overset{(a_2-a_1\neq 0)}{\Rightarrow} q_1(a_2)=0 \Rightarrow x-a_2$ is a factor of $q_1(x)$.

$f(x) = (x-a_1)(x-a_2)\,q_2(x)$, $\deg q_2(x) = n-2$.

Repeat! $f(x) = (x-a_1)\dots(x-a_r)\,q_r(x)$, $\deg q_r(x) = n-r$

$\deg q_r(x) \geq 0$

$n - r \geq 0$

$n \geq r$.

□

Corollary: Let p be a prime. The group $\mathbb{Z}_p^*$ with multiplication is cyclic.

Proof $\mathbb{Z}_p^*$ is abelian and finite.

Fundamental thm. of finite abelian groups $\Rightarrow$

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_n^{e_n}}, \qquad p_i \text{ primes}, \; e_i \neq 0 \in \mathbb{Z}^+$$

where $p_1^{e_1} \cdots p_n^{e_n} = |\mathbb{Z}_p^*| = p-1$.

Let $m = \operatorname{lcm}(p_1^{e_1}, \dots, p_n^{e_n})$. Then for each $a \in \mathbb{Z}_{p_i^{e_i}}$

$$ma = k\{p_i^{e_i} a = k0 = 0.$$

It follows, for each $(a_1, \dots, a_n) \in \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_n^{e_n}}$, $m(a_1, \dots, a_n) = (0, \dots, 0)$.

Hence, for each $a \in \mathbb{Z}_p^*$, $a^m = 1$.

Polynomial $x^m - 1$ has $p-1$ zeros; $\{1, 2, \dots, p-1\} = \mathbb{Z}_p^*$,

hence $m \geq p-1$.

Then $m = \operatorname{lcm}(p_1^{e_1}, \dots, p_n^{e_n}) = p-1$

$\Rightarrow \operatorname{lcm}(p_1^{e_1}, \dots, p_n^{e_n}) = p_1^{e_1} \cdots p_n^{e_n}$

$\Rightarrow$ the p_i are distinct $\Rightarrow \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_n^{e_n}}$ is cyclic.

This is used in public key encryption! (Diffie-Hellman)

Take enormous prime p, pick generator $a \in \mathbb{Z}_p^*$.

$$\phi : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p^* \qquad \text{"discrete exponentiation"}$$
$$\phi(b) = a^b$$
$$\phi^{-1} : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_{p-1} \qquad \text{"discrete logarithm"}$$

ϕ easy to compute, ϕ^{-1} very hard.

Irreducible polynomials Let $f(x) \in F[x]$. Say $f(x)$ is irreducible over F if we can not write

$$f(x) = g(x)\,h(x)$$

with $g(x), h(x) \in F[x]$, both of lower degree than $f(x)$.

$f(x)$ not irreducible $\Leftrightarrow$ $f(x)$ reducible.

Example x^2-2 is irreducible over $\mathbb{Q}$, since

$$x^2-2 = (a_0 + a_1 x)(b_0 + b_1 x) \qquad a_0, a_1, b_0, b_1 \in \mathbb{Q}.$$
$$\Downarrow$$
$$\left(-\frac{a_0}{a_1}\right)^2 = \left(-\frac{b_0}{b_1}\right)^2 = 2$$

x^2-2 is reducible over $\mathbb{R}$, since $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

Thm Let $f(x) \in F[x]$ such that $\deg f(x) = 2$ or 3. Then

$f(x)$ reducible over $F \iff f(x)$ has a zero in F

Proof $\Leftarrow$ Let $a \in F$, $f(a) = 0$. Then $x-a$ is a factor of $f(x)$, so $f(x) = (x-a)\,q(x) \Rightarrow f(x)$ reducible.

$\Rightarrow$ Write $f(x) = g(x)h(x)$. Since $\deg f(x) = 2$ or 3 either $g(x)$ or $h(x)$ has degree 1.

Assume $g(x) = (a_1 x + a_0)$.

Then
$$f(x) = (a_1 x + a_0) h(x) = a_1 \left(x + \frac{a_0}{a_1} \right) h(x)$$

$\Rightarrow -\frac{a_0}{a_1}$ is a zero of $f(x)$.

Example $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$, since

$$f(0) = 0^2 + 0 + 1 = 1$$
$$f(1) = 1^2 + 1 + 1 = 1.$$

Irreducibility over $\mathbb{Q}$

Gauss' lemma: Let $f(x) \in \mathbb{Z}[x]$, Assume that $g(x), h(x) \in \mathbb{Q}[x]$ are such that
$$f(x) = g(x) h(x).$$
Then there exist $G(x), H(x) \in \mathbb{Z}[x]$ such that $\deg g(x) = \deg G(x)$, $\deg h(x) = \deg H(x)$, &
$$f(x) = G(x) H(x).$$

Example $x^2 - 3x + 2 = \left(\frac{3x}{2} - \frac{3}{2} \right) \left(\frac{2x}{3} - \frac{2}{3} \right)$

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

Corollary Let $f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $a_i \in \mathbb{Z}$.
If $f(x)$ has a zero in $\mathbb{Q}$, it has a zero in in $\mathbb{Z}$, and in divides a_0.

Proof $a \in \mathbb{Q}$ $f(a) = 0 \Rightarrow f(x) = (x - a)(x^{n-1} + b_{n-1} x^{n-2} + \cdots + b_0)$ $b_i \in \mathbb{Q}$

Gauss lemma $\Rightarrow f(x) = (c_1 x + c_0)(d_{n-1} x^{n-1} + \cdots + d_0)$ $c_i, d_i \in \mathbb{Z}$

$c_1 d_{n-1} = 1 \Rightarrow c_1 = \pm 1 \Rightarrow -\frac{c_0}{c_1} \in \mathbb{Z}$, and $-\frac{c_0}{c_1}$ is a zero of $f(x)$.

~~$c_1 d_0 = a_0$~~

Example $f(x) = x^2 - 2$ irreducible over $\mathbb{Q}$, since

$f(x)$ reducible of deg 2 $\Rightarrow$ $f(x)$ has 0 in $\mathbb{Q}$

$\Rightarrow$ $f(x)$ has 0 in $\mathbb{Z}$, which is false.

Example $f(x) = x^3 + 4x^2 - 7x + 1$ is irreducible over $\mathbb{Q}$.

$f(x)$ reducible of deg. 3 $\Rightarrow$ $f(x)$ has a zero in $\mathbb{Q}$ $\Rightarrow$ $f(x)$ has zero m in $\mathbb{Z}$ m divides 1.

If m divides 1, then $m = 1$ or $m = -1$

$f(1) = 1 + 4 - 7 + 1 = -1$ $\quad$ $f(-1) = -1 + 4 + 7 + 1 = 11$.

So $f(x)$ has no zero in $\mathbb{Z}$, hence is irreducible over $\mathbb{Q}$.

Eisenstein criterion: Let p be a prime. Let $f(x) = a_n x^n + \cdots + a_0$, with $a_i \in \mathbb{Z}$, such that

- $a_n \not\equiv 0 \pmod{p}$
- $a_k \equiv 0 \pmod{p}$ for all $k < n$
- $a_0 \not\equiv 0 \pmod{p^2}$

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

Example $f(x) = 14x^3 + 9x^2 + 18x + 3$ is irreducible over $\mathbb{Q}$, by Eisenstein criterion with $p = 3$. $14 \not\equiv 0 \pmod 3$, $9 \equiv 18 \equiv 3 \equiv 0 \pmod 3$, $3 \not\equiv 0 \pmod 9$.

Example: Let $\phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$, the pth cyclotomic polynomial.

This is irreducible over $\mathbb{Q}$: Consider $\phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1}$

$$= \frac{\left(x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x + 1\right) - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}.$$

This satisfies Eisenstein's criterion: $1 \not\equiv 0 \pmod p$

$\binom{p}{k} \equiv 0 \pmod p$ for $1 \le k \le p-1$

$\binom{p}{1} = p \not\equiv 0 \pmod{p^2}$.

over $\mathbb{Q}$

So $\phi_p(x+1)$ is irreducible, hence $\phi_p(x)$ is irreducible over $\mathbb{Q}$

(If $\phi_p(x) = g(x)h(x)$, then $\phi_p(x+1) = g(x+1)\,h(x+1)$.)

Factoring into irreducible polynomials. Let F be a field

Slogan: Irreducible polynomials behave in $F[x]$ as primes do in $\mathbb{Z}$.

Let $f(x), g(x) \in F[x]$. Say $f(x)$ divides $g(x)$, write $f(x) \mid g(x)$, if there is a $q(x) \in F[x]$ such that

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

(remainder $r(x) = 0$ in polynomial division).

Thm Let $f(x) \in F[x]$ be irreducible, let $g(x), h(x) \in F[x]$, and assume $f(x) \mid g(x)\,h(x)$. Then either $f(x) \mid g(x)$ or $f(x) \mid h(x)$.

Proof in Section 27.

Thm Let $f(x) \in F[x]$ be irreducible, let $g_1(x), g_2(x), \dots, g_n(x) \in F[x]$
If $f(x) \mid g_1(x) \cdots g_n(x)$, then $\exists\, i \in \{1, \dots, n\}$ s.t. $f(x) \mid g_i(x)$.

Proof: By induction from previous theorem.

Thm Let $f(x) \in F[x]$. Then we can write

$$f(x) = p_1(x) \cdots p_n(x),$$

with $p_i(x) \in F[x]$ irreducible. The $p_i(x)$ are uniquely determined by $f(x)$ up to reordering and multiplication by constants in F.

Example (uniqueness) $x^2 - 3x + 2 = (x-1)(x-2) = (x-2)(x-1)$

$= (2x-2)\left(\frac{x}{2} - \frac{2}{2}\right) = (3x-3)\left(\frac{x}{3} - \frac{2}{3}\right) \dots$

Proof If $f(x)$ is reducible, write $f(x) = g(x)h(x)$, $\deg g(x), \deg h(x) < \deg f(x)$.

If $g(x)$ & $h(x)$ irreducible, done.

Else factor $g(x) = i(x)j(x)$, and so on, eventually get

$$f(x) = p_1(x) \cdots p_n(x), \quad p_i(x) \text{ irreducible}$$

Uniqueness: Suppose $f(x) = r_1(x) \cdots r_m(x)$ $\quad r_i(x)$ irreducible.

Then $p_1(x) \mid f(x) \Rightarrow \exists\, j_1$ s.t. $p_1(x) \mid r_{j_1}(x)$.
$\quad\quad p_1(x)$ irr.

But $r_j(x)$ irreducible, so $\deg p_1(x) = \deg r_{j_1}(x)$, hence $r_{j_1}(x) = p_1(x)\, c_1$, $c_1 \in F$.

Cancelling gives

$$p_2(x) \cdots p_n(x) = c_1 r_1(x) \cdots r_{j_1-1}(x)\, r_{j_1+1}(x) \cdots r_m(x)$$

$p_2(x) \mid f(x) \Rightarrow \exists\, j_2$ s.t. $r_{j_2}(x) = p_2(x)\, c_2$

$$\Rightarrow \quad p_3(x) \cdots p_n(x) = c_1 c_2\, r_1(x) \cdots r_{j_2-1}(x)\, r_{j_2+1}(x) \cdots r_{j_1-1}(x)\, r_{j_1+1}(x) \cdots r_m(x).$$

Repeating this n times shows that the $p_i(x)$ match the $r_i(x)$ up to scalar factors.