Lecture 4: Roots and reducibility (4.4)

Assume R commutative ring, F field

Def: A polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ induces a function $f: R \to R$ defined by

$$f(r) = a_n r^n + a_{n-1} r^{n-1} + \cdots + a_1 r + a_0, \quad r \in R$$

Ex: Let $R = \mathbb{Z}_3$. The polynomial $x^4 + x + 1 \in \mathbb{Z}_3[x]$ induces $f(r) = r^4 + r + 1$, $r \in \mathbb{Z}_3$.

We have $f(0) = 1$, $f(1) = 0$, $f(2) = 1$.

On the other hand $x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$ induces $g(r) = r^3 + r^2 + 1$, $r \in \mathbb{Z}_3$, with $g(0) = 1, g(1) = 0, g(2) = 1$

Note: Different polynomials can give rise to same function $f = g$.

Convention: We will use the same notation, $f(x)$, both for the polynomial and the corresponding function.

Def: We say that $a \in R$ is a root of $f(x) \in R[x]$ if $f(a) = 0_R$.

Theorem: The remainder of $f(x) \in F[x]$ when divided by $x - a$ ($a \in F$) is the constant $f(a)$.

Proof: Div. alg $\Rightarrow$ $f(x) = (x-a)g(x) + r(x)$, where $\deg r(x) < \deg(x-a) = 1$ or $r(x) = 0$.

$\Rightarrow$ $\deg r(x) = 0$ or $r(x) = 0$

$\Rightarrow$ $r(x) = C$ for some $C \in F$. Let $x = a$. We get

$$f(a) = \underbrace{(a-a)}_{=0} g(a) + C = C \quad \Rightarrow r(x) = f(a) \qquad \square$$

Theorem (Factor theorem):

$a \in F$ root of $f(x) \in F[x]$ $\Leftrightarrow$ $x - a \mid f(x)$.

Proof: a root $\Leftrightarrow f(a) = 0 \Leftrightarrow r(x) = 0 \Leftrightarrow x - a \mid f(x)$ $\square$

Repetition: A polynomial $p(x) \in F[x]$ ($\deg p(x) \geq 1$) is irreducible if $p(x) = f(x)g(x) \Rightarrow f(x) \in F$ or $g(x) \in F$.

Ex: Determine all irreducible polynomials in $\mathbb{Z}_2[x]$ (← field) up to degree 3.

deg 1: x and $x+1$ are irr.

deg 2: $f(x)$ reducible $\Leftrightarrow$ $f(x)$ has a factor of degree 1

$\Leftrightarrow$ $f(x)$ has root 0 or 1

We get $f(x) = a_2 x^2 + a_1 x + a_0$, $a_2 \neq 0$

$f(0) = 0 \Leftrightarrow a_0 = 0$

$f(1) = 0 \Leftrightarrow a_2 + a_1 + a_0 = 0$ and so

$f(x)$ irreducible $\Leftrightarrow$ $a_0 \neq 0$ and $a_2 + a_1 + a_0 \neq 0$

Only possibility $f(x) = x^2 + x + 1$

(Note for example that $x^2 + 1 = (x+1)^2$.)

deg 3: $f(x)$ reducible $\Leftrightarrow$ $f(x)$ has factor of degree 1

$\Leftrightarrow$ $f(x)$ has root 0 or 1

We get $f(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$, $a_3 \neq 0$

$f(0) = 0 \Leftrightarrow a_0 = 0$

$f(1) = 0 \Leftrightarrow a_3 + a_2 + a_1 + a_0 = 0$, so

$f(x)$ irreducible $\Leftrightarrow$ $a_0 \neq 0$ and $a_3 + a_2 + a_1 + a_0 \neq 0$

Only possibilities $f(x) = x^3 + x^2 + 1$ and $f(x) = x^3 + x + 1$

Note: For deg 4 we have not

$f(x)$ reducible $\Leftrightarrow$ $f(x)$ has root 0 or 1.

E.g. $f(x) = (x^2 + x + 1)^2$ reducible but has no root.

Corollary: A polynomial $f(x) \in F[x]$ has at most the same number of roots as its degree.

"Proof": Combine Factor theorem and induction.

Note: Not true if pol. ring not over a field, e.g.

$2x - 2 \in \mathbb{Z}_6[x]$ has two roots, $x = 1$ and $x = 4$

Corollary: Let F be an infinite field and let $f(x), g(x) \in F[x]$

Then

$f(x) = g(x)$ as polynomials $\Leftrightarrow$ $f(x) = g(x)$ as functions.

Proof: $\Rightarrow$) obvious

$\Leftarrow$) Assume $f(x) = g(x)$ as functions, i.e. $f(a) = g(a)$ for all $a \in F$. This means that $f(a) - g(a) = 0$ for all $a \in F$ $\Rightarrow$ $f(x) - g(x)$ has infinite number of roots

Cor. above $\Rightarrow$ $f(x) - g(x) = 0$ (zero pol.) $\Rightarrow$ $f(x) = g(x)$ as polynomials. $\square$

Factorization in $\mathbb{Q}[x]$ (4.5):

Theorem (Rational root test):

If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$ has the rational root $\frac{r}{s} \in \mathbb{Q}$, $(r,s) = 1$, then

$r \mid a_0$ and $s \mid a_n$.

Proof: $f\left(\frac{r}{s}\right) = a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1 \cdot \frac{r}{s} + a_0 = 0$

Mult. by s^n $\Rightarrow$ $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$

$\Rightarrow$ $a_0 s^n = -r\left(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}\right)$

$\Rightarrow$ $r \mid a_0 s^n$ $\Rightarrow$ $r \mid a_0$ ($(r,s) = 1$)

Similar argument for $s \mid a_n$. $\square$

Theorem: Let $f(x) \in \mathbb{Z}[x]$. Then

$f(x)$ reducible in $\mathbb{Z}[x] \iff f(x)$ reducible in $\mathbb{Q}[x]$

Proof $\Rightarrow$) Assume $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $\deg g(x), \deg h(x) \geq 1$

Then $f(x) = g(x)h(x)$ is also a factorization in $\mathbb{Q}[x]$.

$\Leftarrow$) We need the following lemma first:

Lemma: Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$.

If p (prime) divides all coeff. of $f(x)$, then p divides all coeff. of $g(x)$ or all coeff. of $h(x)$.

Proof: Let $g(x) = b_n x^n + \dots + b_0$, $h(x) = c_m x^m + \dots + c_0$

Assume the contrary. Then for some r, t we have

$$\begin{cases} p \mid b_i \text{ when } i<r, \text{ but } p \nmid b_r \\ p \mid c_j \text{ when } j<t, \text{ but } p \nmid c_t \end{cases}$$

Consider coeff. a_{r+t} in $f(x)$:

$$a_{r+t} = \underbrace{b_0 c_{r+t} + \dots + b_{r-1} c_{t+1}}_{=A} + b_r c_t + \underbrace{b_{r+1} c_{t-1} + \dots + b_{r+t} c_0}_{=B}$$

$p \mid a_{r+t}$, $p \mid A$, $p \mid B$ $\Rightarrow$ $p \mid b_r c_t$ $\Rightarrow$

$\Rightarrow p \mid b_r$ or $p \mid c_t$ contradiction! $\square$

$\Leftarrow$) (Cont.) Assume

$f(x) = g(x)h(x)$ $\quad g(x), h(x) \in \mathbb{Q}[x]$, $\deg g(x), \deg h(x) \geq 1$

Let $c, d \in \mathbb{Z}$ such that $cg(x), dh(x) \in \mathbb{Z}[x]$

$(*)$ $\Rightarrow$ $cd f(x) = (cg(x))(dh(x))$ a factorization in $\mathbb{Z}[x]$

($cg(x) \in \mathbb{Z}[x]$, $dh(x) \in \mathbb{Z}[x]$)

Let p be a prime factor in cd. Then p divides all coeff. in $cdf(x)$ $\overset{\text{lemma}}{\Rightarrow}$ p divides all coeff. in $cg(x)$ or all coeff. in $dh(x)$.

Cancel p on both sides in $(*)$. We then still have a factorization in $\mathbb{Z}[x]$.

Repeat for all prime factors in cd. Finally we get a factorization of $f(x)$ in $\mathbb{Z}[x]$. $\square$

Cor. Let $f(x) \in \mathbb{Q}[x]$ and let c be an integer such that $cf(x) \in \mathbb{Z}[x]$. Then

$f(x)$ reducible in $\mathbb{Q}[x] \iff cf(x)$ reducible in $\mathbb{Z}[x]$

Proof: $f(x)$ reducible in $\mathbb{Q}[x] \iff cf(x)$ reducible in $\mathbb{Q}[x]$ (trivial)

$\overset{\text{Th. above}}{\iff}$ $cf(x)$ reducible in $\mathbb{Z}[x]$. $\square$

~~Ex: Show that $f(x) = x^4 - 5x^2 + 1$ irreducible in $\mathbb{Q}[x]$.~~

Note: We have even proved a stronger statement.

For $f(x) \in \mathbb{Z}[x]$ we have

$f(x) = G(x)H(x)$ $\iff$ $f(x) = g(x)h(x)$

where $G(x), H(x) \in \mathbb{Z}[x]$ and $\deg G(x) = m$, $\deg H(x) = n$ $\quad$ where $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg g(x) = m$, $\deg h(x) = n$

↖ degrees equal! ↗

Ex: Show that $f(x) = x^4 - 5x^2 + 1$ irreducible in $\mathbb{Q}[x]$.

In this case enough to show that $f(x)$ has no factor of degree 1 or 2.

- **Degree 1:** Assume $f(x)$ has a linear factor $x - \frac{a}{b}$ where $(a,b) = 1$. (We may assume factor monic. Why?)

  This means $\frac{a}{b}$ root of $f(x)$ and by the rational root test we must have $a \mid 1$ and $b \mid 1$ $\Rightarrow$ $a, b = \pm 1$ $\Rightarrow$ $\frac{a}{b} = \pm 1$.

  But ± 1 are not roots (check!). Contradiction!

- **Degree 2:** By theorem + note above we may check factors in $\mathbb{Z}[x]$.

  Assume $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $\deg g(x) = \deg h(x) = 2$ and $g(x), h(x)$ monic

  Then

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

  $\iff$ $x^4 - 5x^2 + 1 = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (bc+ad)x + bd$

  $$\iff \begin{cases} a + c = 0 & \Rightarrow c = -a \\ b + d + ac = -5 & \Rightarrow a^2 = 5 + b + d \\ bc + ad = 0 \\ bd = 1 \end{cases} \Rightarrow \begin{cases} \text{①} \ b = d = 1 & \Rightarrow a^2 = 7 \\ \text{②} \ b = d = -1 & \Rightarrow a^2 = 3 \end{cases}$$

  ① impossible! ② contradiction!

Theorem (Eisenstein):

Let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$.

If there exists a prime p such that

$$p \mid a_0, p \mid a_1, p \mid a_2, \dots, p \mid a_{n-1}$$

but $p \nmid a_n$, $p^2 \nmid a_0$, then

$f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Assume the contrary, i.e.

$$f(x) = (b_r x^r + \dots + b_1 x + b_0)(c_s x^s + \dots + c_1 x + c_0).$$

$a_0 = b_0 c_0$ and $p \mid a_0$ $\Rightarrow$ $p \mid b_0$ or $p \mid c_0$, let's say $p \mid b_0$

$p^2 \nmid a_0 = b_0 c_0$ $\Rightarrow$ $p \nmid c_0$

Now since $p \nmid a_n = b_r c_s$ $\Rightarrow$ $p \nmid b_r$, we have for some integer k that $p \mid b_i$ when $i<k$ but $p \nmid b_k$.

Consider $a_k = \underbrace{b_0 c_k + b_1 c_{k-1} + \dots + b_{k-1} c_1}_{=A} + b_k c_0$

$p \mid a_k$, $p \mid A$ $\Rightarrow$ $p \mid b_k c_0$ $\Rightarrow$ $p \mid b_k$ or $p \mid c_0$

contradiction! $\square$

Ex: $x^n + 7$ irr. in $\mathbb{Q}[x]$ for all n $\quad (p = 7)$

Ex: $2x^4 - 5x^3 + 25x^2 - 10x + 35$ irr. in $\mathbb{Q}[x]$ $\quad (p = 5)$

Theorem: $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and p prime such that $p \nmid a_n$.

Then $\bar{f}(x) = [a_n]x^n + \cdots + [a_0]$ irreducible in $\mathbb{Z}_p[x]$

$\Rightarrow$ $f(x)$ irreducible in $\mathbb{Q}[x]$.

"Proof": factorization of $f(x)$ in $\mathbb{Q}[x]$ $\overset{\text{theorem}}{\Rightarrow}$ factoriz. of $f(x)$ in $\mathbb{Z}[x]$

$\Rightarrow$ factorization of $f(x)$ in $\mathbb{Z}_p[x]$. □

Ex: Show that $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ irr. in $\mathbb{Q}[x]$.

$\mathbb{Z}_2[x]$: $\bar{f}(x) = x^5 + x^2 + 1$

- $\bar{f}(0) \neq 0$ and $\bar{f}(1) \neq 0$ $\Rightarrow$ no linear factor
- Only irr. pol. of degree 2 in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$ (not a factor in $\bar{f}(x)$, since by pol. div.

$$\bar{f}(x) = (x^3 + x^2)(x^2 + x + 1) + \underline{1}$$)

$\Rightarrow$ $\bar{f}(x)$ irreducible in $\mathbb{Z}_2[x]$

$\Rightarrow$ $f(x)$ irreducible in $\mathbb{Q}[x]$.

Note: The converse of the theorem above is not true.

E.g. $f(x) = x^2 + 1 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$

but $\bar{f}(x) = x^2 + 1$ is reducible in $\mathbb{Z}_2[x]$ since

$$x^2 + 1 = (x+1)^2$$

- Chapter 4.6, factorization in $\mathbb{R}[x]$ and $\mathbb{C}[x]$, is covered in "endim. analys". Study yourself.