Groups & Rings: Lecture #19

Ideals in $F[x]$ (§17.3)

- Principal ideals
- Maximal ideals
- Euclidean domains (§18.2)

Fraction field / ring of fractions (§18.1)

- Fraction field of an int domain
- More general construction ($S^{-1}R$)
- Universal property (notes on webpage)

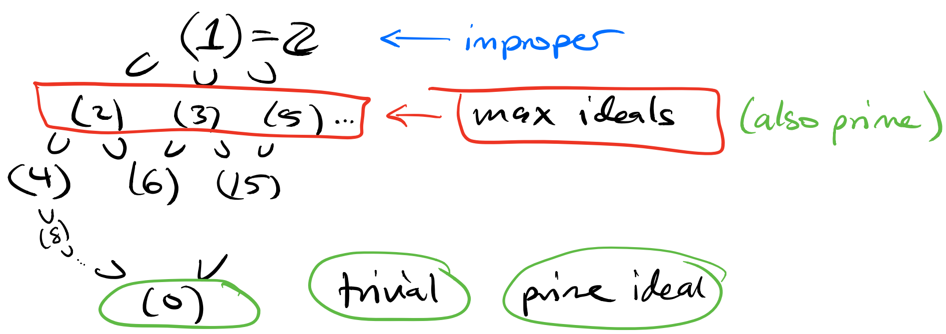
Ideals in $\mathbb{Z}$ and $F[x]$

Recall $\mathbb{Z}$:

(1) Every ideal is principal (n) ($\mathbb{Z}$ is a principal ideal domain)

(2) Maximal ideals are (p) p prime.

(3) Prime ideals are (0) and (p) p prime.



Today: $F[x]$, F field.

Thm 17.20: $F[x]$ is a PID = principal ideal domain

that is, every ideal is principal.

pf: Let $I \subseteq F[x]$ be a non-trivial ideal $(I \neq 0)$.

Pick $f(x) \in I$ nonzero, of minimal degree $d = \deg f$ $(d \geq 0)$

Claim: $I = (f)$.

Pick any $g(x) \in I$. Use division algorithm $(f \neq 0)$

$$\underbrace{g(x)}_{\in I} = \underbrace{f(x)}_{\in I} q(x) + r(x) \qquad \deg r(x) < d$$

$\Rightarrow$ $r(x) \in I$.

Since $\deg r(x) < d \Rightarrow r(x) = 0 \Rightarrow g(x) \in (f)$

$\Rightarrow I = (f)$

(If I trivial, then $I = (0)$.) $\square$

<u>Rmk</u>: Proofs for $\mathbb{Z}$ and $F[x]$ formally the same.

Notion of <u>Euclidean domains</u> where we have <u>div algo</u> $\Rightarrow$ PID.

<u>Def</u>: A domain D is a Euclidean domain if there exist a Euclidean fcn $v : D \setminus \{0\} \to \mathbb{N}$ s.th

(EF1) $\forall a, b \in D, b \neq 0 \ \exists q, r \in D$ s.th $a = q \cdot b + r$ and either $r = 0$ or $v(r) < v(b)$

<u>Ex</u>:
- $\mathbb{Z}$, $v = |\cdot|$ (abs. value)
- $F[x]$, $v = \deg$ (degree)

are Euclidean domains.

<u>Fact</u> Eucl. domain $\Rightarrow$ PID. ("same" proof as $\mathbb{Z}/F[x]$)

<u>Ex</u>: $R = F[x,y]$ is not a PID

Ideal $(x,y) = \{ f(x,y) = x g(x,y) + y h(x,y) \}$ not principal.

No common divisor of x and y except 1.

quotient

<u>No div algo</u>:
- $x = 0 \cdot y + x$ "$\deg(x)$" < "$\deg(y)$"
- $y = 0 \cdot x + y$ "$\deg(y)$" < "$\deg(x)$"

remainder

$\mathrm{mdeg}(x) = (1,0)$

$\mathrm{mdeg}(y) = (0,1)$

Maximal ideals in $F[x]$

Theorem 17.22: A principal ideal $(p(x)) \subseteq F[x]$ is maximal $\iff$ $p(x)$ irreducible.

Recall: • R ring, $r \in R$ irreducible if non-zero, non-unit and not product of 2 non-units.

Ex: • $R = \mathbb{Z}$, $n \in \mathbb{Z}$ irreducible $\iff$ $n = \pm p$ p prime.

• $R = F[x]$ $p(x) \in F[x]$ irreducible $\iff$ $\deg p(x) \geq 1$ and $\nexists\ p(x) = q(x)r(x)$ with $\deg q(x), \deg r(x) \geq 1$.

pf: ($\Rightarrow$) Suppose $p(x)$ not irreducible.

If $p(x) = 0 \Rightarrow (p(x)) = 0$ trivial, not maximal

If $p(x)$ unit $\Rightarrow (p(x)) = F[x]$ improper, not maximal

If $p(x) = \underbrace{q(x)}_{\deg \geq 1}\underbrace{r(x)}_{\deg \geq 1} \Rightarrow (p(x)) \subsetneq (q(x)) \subsetneq F[x] \Rightarrow (p(x))$ not max.

$\Rightarrow$ q not mult. of p

q not unit

($\Leftarrow$) Suppose $(p(x))$ not maximal. Then $\exists$

$$(p(x)) \subsetneq (q(x)) \subsetneq F[x]$$

$p(x) = q(x)r(x)$

$\Downarrow$ q not mult of p

$\Downarrow$ q not unit

$\Downarrow$ r not unit

$\Rightarrow p$ not irreducible. $\square$

Consequences / examples

$\mathbb{R}[x]$:

$\ker(ev_a) = (x-a)$

$$\begin{tikzcd} \mathbb{R}[x] \arrow[d] \arrow[dr, "ev_a"] & \\ \mathbb{R}[x]/(x-a) \arrow[r, phantom, "\cong"] & \mathbb{R} \end{tikzcd}$$

- $x-a$ irreducible ($a \in \mathbb{R}$) $\iff$ $(x-a)$ maximal $\Rightarrow$ $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$ field
  ($\cong$: 1st iso thm)
- x^2+1 irreducible $\iff$ (x^2+1) maximal
  $\Rightarrow E = \mathbb{R}[x]/(x^2+1)$ field w/ $\bar{x} = x + (x^2+1) \in E$, $\bar{x}^2 = -1$
  $(\bar{x}^2 = x^2 + (x^2+1) = -1 + (x^2+1))$

$$\begin{tikzcd} \mathbb{R}[x] \arrow[d] \arrow[dr, "ev_i"] & \\ E = \mathbb{R}[x]/(x^2+1) \arrow[r, phantom, "\cong"] & \mathbb{C} \end{tikzcd}$$

($\cong$: 1st iso thm)

- $\ker(ev_i) = (x^2+1)$
- ev_i surjective because
  $ev_i(a+bx) = a+bi \quad \forall a,b \in \mathbb{R}$

$\mathbb{Q}[x]$:

- $x-a$ irr $\iff$ $(x-a)$ max $\Rightarrow$ $\mathbb{Q}[x]/(x-a) \cong \mathbb{Q}$
- x^3-2 irr $\iff$ (x^3-2) max $\Rightarrow$ field $E = \mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$

$$\bar{x} = x + (x^3-2), \quad \boxed{\bar{x}^3 = 2}$$

$$E = \{a + b\bar{x} + c\bar{x}^2 : a,b,c \in \mathbb{Q}\}$$
$$= \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$$

<u>Exc</u>: The abelian group $(E,+)$ is a $\mathbb{Q}$-vector space with basis $1, \bar{x}, \bar{x}^2$.

Fraction fields

Recall: $\mathbb{Z} \subset \mathbb{Q} = \{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \}$

$= \{ (a,b) : a, b \in \mathbb{Z},\ b \neq 0 \} / \sim$ = equiv classes $[a,b]$ of $\sim$

$$(a,b) \sim (c,d) \overset{\text{def}}{\iff} ad = bc$$

$$\frac{a}{b} = \frac{c}{d}$$

Compare: R ring, $I \subseteq R$, $R/I = \{ r + I \}$

$= R/\sim = \{ \bar{r} \} = \{ [r] \}$

$$r \sim s \iff r - s \in I$$

Def: Let D be an integral domain. The fraction field of D is $\mathrm{Frac}(D) = \{ (a,b) : a, b \in D,\ b \neq 0 \} / \sim$ where $(a,b) \sim (c,d) \iff ad = bc$.

Lemma 18.1: $\sim$ is an equivalence relation.

pf: (i) reflexive: $(a,b) \sim (a,b) \iff ab = ab$ ✓

(ii) symmetric: $(a,b) \sim (c,d) \overset{?}{\iff} (c,d) \sim (a,b)$ ✓

$\Updownarrow$ def $\qquad\qquad \Updownarrow$ def

$$ad = bc \iff cb = da$$

(iii) transitive: $(a,b) \sim (c,d),\ (c,d) \sim (e,f) \implies (a,b) \sim (e,f)$

(uses D int domain)

$\Updownarrow \qquad\qquad \Updownarrow \qquad\qquad \Updownarrow$

$ad = bc \qquad cf = de \qquad af = be$

$\Updownarrow f \neq 0 \qquad\qquad d \neq 0$

$$a\cancel{d}f = bcf = b\cancel{d}e$$

□

Def: $\frac{a}{b} = [a,b]$ equiv class of (a,b).

Def: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ $\qquad$ $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Lemma 18.2: $+$ and $\cdot$ give welldefined operations on Frac D.

Lemma 18.3: $(\mathrm{Frac}\,D, +, \cdot)$ is a field

Outline of pf of 18.3: Frac D is an abelian group:

- zero: $\frac{0}{1} = \frac{0}{b}$ $\quad b \in D \setminus 0$ $\qquad$ **denoted** 0
- ass of $+$
- comm of $+$
- add. inverses $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$

Frac D is a commutative ring w/ mult identity:

- ass of $\cdot$
- dist of $\cdot$ over $+$
- comm of $\cdot$
- one: $1 = \frac{1}{1} = \frac{b}{b}$ $\quad b \in D \setminus 0$

Frac D is a field:

- inverse of $\frac{a}{b}$: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ exists when $a \neq 0$. $\square$

Ex: $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

Ex: $\mathrm{Frac}(F[x]) = F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F[x],\ q(x) \neq 0 \right\}$

"rational functions".

More general fraction rings

<u>Def</u>: Let R be a ring with 1. A subset $S \subseteq R$ is **multiplicative** if

- $1 \in S$
- $s, t \in S \Rightarrow st \in S$.

<u>Def</u>: The **localization of R w.r.t. S** is $S^{-1}R = \left\{ \frac{r}{s} : r \in R, s \in S \right\}$
(fraction ring)

$$= \{(r,s) : r \in R, s \in S\} / \sim$$

makes $\sim$ transitive
when R not domain

where $(r,s) \sim (r',s')$ if $trs' = tr's$ for some $t \in S$

$\left(\Leftrightarrow rs' = r's \text{ if } R \text{ domain and } 0 \notin S \right)$

<u>Theorem</u>: $S^{-1}R$ is a ring (not nec. a field).

<u>Ex</u>: $S = \{1\}$, $S^{-1}R = R$

<u>Ex</u>: D domain, $S = D \setminus \{0\}$, $S^{-1}D = \mathrm{Frac}(D)$

<u>Ex</u>: $S^{-1}R = R$ if elements in S are invertible
$\mathrm{Frac}(F) = F$ if F field.

Universal properties

Motivation: Inverse of a matrix A:

Construction: $A^{-1} = \frac{1}{\det A} A^{adj}$ $\quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Property: $AA^{-1} = A^{-1}A = I$

$\Downarrow$

A^{-1} unique

Universal property of quotient of groups

$H \trianglelefteq G$ normal subgroup $\quad \pi : G \longrightarrow \underbrace{G/H = \{g+H\}}_{\text{construction}}$

Universal property: $G \xrightarrow{\varphi} G'$ group homomorphism such that $\varphi(H) = e$, that is, $H \subseteq \ker \varphi$.

Then $\exists !\, q : G/H \to G'$ such that the diagram

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, dashed, "q"'] & \end{tikzcd}$$

commutes: $\varphi = q \circ \pi$

If $\pi' : G \longrightarrow Q$ another map w/ same property, then Q and G/H are isomorphic and π and π' are identified.

<u>Universal property of fraction field</u>

<u>Thm 18.4</u>: The map $D \xrightarrow{\phi} \mathrm{Frac}\, D$, $\phi(a) = a/1$ is an injective ring homomorphism. If F is a field and $\varphi : D \longrightarrow F$ is an injective ring homomorphism, then $\exists ! \, \psi : \mathrm{Frac}\, D \longrightarrow F$ such that $\varphi = \phi \circ \psi$. That is,

$$\begin{tikzcd} D \arrow[rr, "\varphi"] \arrow[dr, "\phi"'] & & F \\ & \mathrm{Frac}\, D \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

commutes.

<u>SLOGAN</u>: "Frac D is the smallest field containing D"

Similarly, $R \xrightarrow{\phi} S^{-1}R$ is the universal ring homomorphism such that $\phi(s)$ invertible for all $s \in S$. <u>NB</u>! ϕ <u>not</u> injective if S contains zero-divisors.

<u>Do on your own / tutorial</u>:

<u>Exc</u>: 18.10 / Cor 18.6–18.7 On <u>prime field</u>.