Groups & Rings: Lecture #17

Prime & maximal ideals (§16.3)

- Prime ideals (Ex: $\mathbb{Z}$)
- Properties of ideals vs quotients

Polynomial rings (§17.1)

- Definitions, integral domain
- Evaluation homomorphisms

Prime & maximal ideals

Def: $I = R$ is the improper ideal.

Def: $I \subset R$ is maximal if maximal among proper ideals.

Def: $I \subset R$ is prime if

(i) proper $(I \neq R)$, and

(ii) $x, y \in R$, $xy \in I \Rightarrow$ either $x \in I$ or $y \in I$

$(x \notin I, y \notin I \Rightarrow xy \notin I)$

Rmk: The trivial ideal $(0) \subset R$ is prime $\Leftrightarrow$ R integral domain.

(i) $0 \neq 1$

(ii) $xy = 0 \Rightarrow x = 0$ or $y = 0$

Ex: $\mathbb{Z}/12\mathbb{Z}$

$\{\text{ideals of } \mathbb{Z}/12\mathbb{Z}\}$

$\|$ corr thm

$\{\text{ideals } (12) \subseteq I \leq \mathbb{Z}\}$

(1) ← improper ideal

$\cup \quad \cup$

$(2) \quad (3)$ ← max ideals = prime ideals

$\cup \quad \cup \quad \cup$

$(4) \quad (6)$ ← proper ideals

$\cup \quad \cup$

$(0) = (12)$ ← trivial ideal

(0) not prime b/c $3 \cdot 4 = 0 \in (0)$ but $3 \notin (0)$ and $4 \notin (0)$

Ex: $\mathbb{Z}$. Every ideal is principal $I = (n)$:

can assume that n non-negative integer b/c $(5) = (-5)$

(i) $n = \pm p$, p prime $\Rightarrow$ $I = (n)$ maximal (and prime)

(ii) $n = 0$, $I = (0)$ prime (but not maximal)

pf: (n) prime $\Leftrightarrow n \neq \pm 1$ and $xy \in (n) \Rightarrow x \in (n)$ or $y \in (n)$

$\Leftrightarrow n \neq \pm 1$ and $n \mid xy \Rightarrow n \mid x$ or $n \mid y$

$\Leftrightarrow n = \pm p$ or $n = 0$

Properties of ideal vs quotient

Theorem: $I \subseteq R$ ideal, (R commutative).

(i) I maximal $\overset{\text{Thm 16.35}}{\iff}$ R/I field

(ii) I prime $\overset{\text{Prop 16.38}}{\iff}$ R/I integral domain

(Exam 2019-08-12 4a, 2019-06-03 4b)

Rmk: (field $\Rightarrow$ int. dom) $\Rightarrow$ (maximal $\Rightarrow$ prime)

Ex: $\mathbb{Z}/n\mathbb{Z}$ integral domain $\iff$ $n=0$ or $n=\pm p$.

$\mathbb{Z}/p\mathbb{Z}$ field w/ p elements (char p)

$\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ int. domain, not field (char 0)

pf of (ii): I improper $(I=R) \iff R/I = (0) \iff 1=0$ in R/I $\overset{\text{(def)}}{\Rightarrow}$ R/I not int. domain

($\Rightarrow$): Suppose I prime. Then I proper $\Rightarrow 1 \neq 0$ in R/I.

Have to show that 0 is the only zero-divisor in R/I.

Suppose $\exists x, y \in R/I$, $xy = 0$

Then $x = a+I$, $y = b+I$, $xy = ab + I = 0 + I$

$\iff \exists a, b \in R$ s.th. $\underbrace{ab \in I}$

$ab = 0 + i$, $i \in I$

$\overset{I \text{ prime}}{\iff}$ $a \in I$ or $b \in I$

$\iff x = 0$ or $y = 0$

Thus, R/I has no zero-divisors (except for 0).

$(\Leftarrow)$ Suppose R/I integral domain. Then $0 \neq 1$ in R/I
$\Rightarrow I$ proper. Let $a, b \in R$, $ab \in I$.
Then $0 + I = ab + I = (a+I)(b+I)$
Since R/I integral domain $\Rightarrow a + I = 0 + I$
or $b + I = 0 + I$
$\Leftrightarrow a \in I$ or $\in I$. Thus, I prime. $\square$

Pf of (i): Corr. thm $\{\text{ideals of } R/I\} \overset{\text{bij.}}{\longleftrightarrow} \{I \subseteq \underset{\text{ideal}}{J} \subseteq R\}$
I maximal $\overset{\text{def}}{\Leftrightarrow}$ $I \neq R$ and $(J = I$ or $J = R)$
$\overset{\text{corr}}{\Leftrightarrow}$ R/I has precisely two ideals: $\underset{\text{trivial}}{(0)}$, $\underset{\text{improper}}{R/I}$
so (i) follows from (ii) of the following lemma.

Lemma: S commutative ring w/ identity.
(i) $I \subseteq S$ improper $\Leftrightarrow$ I contains a unit.
(ii) S field $\Leftrightarrow$ S has exactly 2 ideals: trivial + improper

proof:
(i) $(\Rightarrow)$ $I = S \Rightarrow 1 \in I$
$(\Leftarrow)$ $u \in I$, $\exists u^{-1} \in R : uu^{-1} = 1 \Rightarrow 1 = uu^{-1} \in I$
$\Rightarrow 1 \cdot s \in I \ \forall s \in S \Leftrightarrow I = S$

(ii) $(\Rightarrow)$ S field, $I \neq (0) = \{0\}$, then $\exists s \in I \setminus \{0\}$
$\Rightarrow s$ unit $\overset{\text{by (i)}}{\Rightarrow}$ $I = S$. ($1 \neq 0 \Leftrightarrow$ trivial $\neq$ improper)
$(\Leftarrow)$ If $s \in I \setminus \{0\}$, then $(s) \neq (0) \Rightarrow (s) = S$
$\Rightarrow 1 \in (s) \Leftrightarrow 1 = st \Leftrightarrow s$ unit. So S field. $\square$

A slightly different perspective on the Theorem:

Rmk: If $R \xrightarrow{\phi} S$ surjective ring homo. $\overset{1^{st} \text{ iso}}{\Longrightarrow}$ $S \cong R/\ker\phi$

($\twoheadrightarrow$ denotes a surj map)

Cor: There are 1–1 correspondences

(i) max. ideals $I \subset R$ and
surjective ring homo $R \twoheadrightarrow S$ where S a field

(ii) prime ideals $I \subset R$ and
surjective ring homo $R \twoheadrightarrow S$ where S an ID

Correspondences given by

$$I \longmapsto (R \twoheadrightarrow R/I)$$

$$\ker\phi \longleftarrow\!\!\!\shortmid \; R \overset{\phi}{\twoheadrightarrow} S \cong R/\ker\phi$$

Polynomial rings

Previously: polynomials as certain functions $\mathbb{R} \to \mathbb{R}$

$$\mathrm{Pol}(\mathbb{R}) \subset C(\mathbb{R}, \mathbb{R}) \qquad \begin{pmatrix} \text{or } \mathbb{C} \to \mathbb{C} \\ \text{or } \mathbb{Q} \to \mathbb{Q} \end{pmatrix}$$

ring by pointwise add. and mult.

Def: Let R be a commutative ring w/ identity.
$R[x]$ ring of polynomials w/ coefficients in R.

polynomial = formal expression $p(x) = \sum_{d=0}^{n} a_d x^d$
for some $n \in \mathbb{N}$, $a_d \in R$.

coefficients

x indeterminate

degree = largest d s.th $\boxed{a_d} \neq 0$
(or $-\infty$ if all $a_d = 0$)

monic = leading coeff is 1.

$\left(= \sum_{d=0}^{\infty} a_d x^d \text{ where almost all } a_d \text{ are zero} \right)$

Let $p(x) = \sum a_d x^d$, $q(x) = \sum b_d x^d$

- $p(x) = q(x) \iff a_d = b_d \;\; \forall d$
- $p(x) + q(x) = \sum (a_d + b_d) x^d$
- $p(x) q(x) = \sum_d \left(\sum_{e+f=d} a_e b_f \right) x^d$

Ex: $R = \mathbb{Z}/p\mathbb{Z}$, $p(x) = x$, $q(x) = x^p$

$p(x) \neq q(x)$ as polynomials but equal as functions.

Fermat's little theorem $a^p \equiv a \pmod p$

Aside (derivatives of pol's)

Also possible to define $\frac{d}{dx} p(x)$ by rule $\frac{d}{dx} x^a = a x^{a-1}$

(equivalently: impose Leibniz rule)

In example: $\frac{d}{dx}(x^p) = p x^{p-1} = 0 x^{p-1} = 0$

(only happens in char $p > 0$)

Theorem 17.3: $R[x]$ commutative ring w/ identity

pf: • Abelian group (zero, add inverse, commutative, ass.)

$p(x) = 0$ $\quad -p(x) = \Sigma(-a_d)x^d$

follows from R being an abelian group.

• Comm ring w/ unity (one, ass mult, dist mult, comm)

(some work)

Prop 17.4: R int. domain $\Rightarrow$ $R[x]$ int. domain.

pf: $(\underbrace{a_n}_{\neq 0} x^n + a_{n-1}x^{n-1} + \cdots + a_0)(\underbrace{b_m}_{\neq 0} x^m + \cdots + b_0)$ non-zero

$= a_n b_m x^{n+m} + \cdots + a_0 b_0$ $\underset{R \text{ ID}}{\Longrightarrow}$ $a_n b_m \neq 0$

Evaluation homomorphism

Thm 17.5: Let $\alpha \in R$. There $\exists$ a ring homo the evaluation homomorphism at α:

$$\begin{aligned} \phi_\alpha : R[x] &\longrightarrow R \\ p(x) &\longmapsto p(\alpha) \\ \sum a_d x^d &\longmapsto \sum a_d \alpha^d \end{aligned}$$

$\boxed{\begin{array}{l} \phi_\alpha \text{ characterized by:} \\ \bullet\ \phi_\alpha(r) = r \quad \forall r \in R \\ \bullet\ \phi_\alpha(x) = \alpha \end{array}}$

That is: Add/mult in $R[x]$ compatible w/ pointwise add/mult.

Rmk: ϕ_α always surjective $\left(\phi_\alpha(r) = r\right)$

constant polynomial

Fact: (Factor thm) $\ker \phi_\alpha = (x - \alpha)$

that is, $p(\alpha) = 0 \iff p(x) = (x-\alpha)q(x)$.

Read more about evaluation homomorphisms in supplementary notes (§4).

Examples:

Ex: $\mathbb{C}[x] \xrightarrow{\phi_\alpha} \mathbb{C}$ $\qquad$ $\mathbb{C}[x] \xrightarrow{\phi_i} \mathbb{C}$

$p(x) \longmapsto p(\alpha)$ $\qquad$ $p(x) \longmapsto p(i)$

Ex: $\mathbb{R}[x] \xrightarrow{\phi_i} \mathbb{C}$

$p(x) \longmapsto p(i)$

$\ker \phi_i = (x^2+1)$

$p(i) = p(-i) = 0$

(extended version of eval. homo $R[x] \xrightarrow{\phi_\alpha} S$ using $R \xrightarrow{f} S$, $\alpha \in S$. $\phi_\alpha(r) = f(r)$, $\phi_\alpha(x) = \alpha$)

1^{st} isom thm: $\mathbb{R}[x] / \ker \phi_i \cong \operatorname{im} \phi_i$

$$\boxed{\mathbb{R}[x] / (x^2+1) \cong \mathbb{C}}$$

$\Rightarrow (x^2+1) \subset \mathbb{R}[x]$ maximal ideal. (x^2+1 irreducible)

cannot be factored

Ex: $\phi_\alpha : \mathbb{R}[x] \longrightarrow \mathbb{R}$ $\qquad$ $\alpha \in \mathbb{R}$

$\mathbb{R}[x] / (x-\alpha) \cong \mathbb{R}$

$\Rightarrow (x-\alpha) \subset \mathbb{R}[x]$ maximal ideal $\qquad$ ($x-\alpha$ irr.)

A glimpse of algebraic geometry

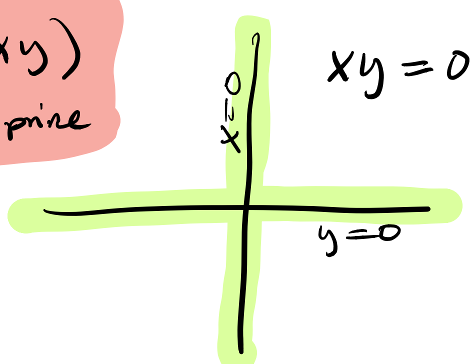
$R = \mathbb{C}[x,y]$ polynomials in x and y

Algebra vs Geometry

- max ideals of $\mathbb{C}[x,y]$ / fields $\longleftrightarrow$ points of $\mathbb{C}^2$
- prime ideals of $\mathbb{C}[x,y]$ / integral domains $\longleftrightarrow$ "irreducible subsets" of $\mathbb{C}^2$

Examples:

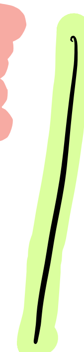
1. (xy) not prime



$xy = 0$

reducible

2. (x) prime



$x = 0$

irreducible

3. (x, y) maximal ideal

$\bullet$ $x=y=0$

point

4. $(x-3,\ y-\sqrt{2})$ maximal ideal

$\bullet$ $(3, \sqrt{2})$

point