Lecture XL: Characteristic of a ring ; Prime and Maximal Ideals

§40.1 Summary of results so far:

Assume R is a commutative ring.

- $I \subseteq R$ is an ideal if it is a subgroup such that $R \cdot I \subseteq I$.
- $x \in R$ is a zero-divisor if $\exists\, y \in R \setminus \{0\}$ s.t. $x \cdot y = 0$.
- $a \in R$ is a unit (or "a is invertible") if $\exists\, b \in R$ s.t. $ab = 1$

  $R^\times$ = set of units in R (group under multiplication)

Definition: We say R is an integral domain if ($x \in R$ is a zero-divisor $\Rightarrow x = 0$)

We say R is a principal ideal ring if every ideal of R is principal, i.e., of the form $(a) = \{ra : r \in R\} = Ra$ for some $a \in R$.

Combining both properties we get principal ideal domain (P.I.D. for short) = integral domain that is also a principal ideal ring.

Examples: ① $\mathbb{Z}$, K any field

② $K[x]$ = polynomials in one-variable with coefficients from a field K.

③ $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$

(These were discussed in Lecture 38)

④ $\mathbb{Z}[x]$, $K[x,y]$ are integral domains but NOT PID's.

Lemma: Every field is an integral domain.

Proof: R is a field if it is commutative and $R^\times = R \setminus \{0\}$.

Since $R^\times \cap \text{ZeroDivisors}(R) = \emptyset$, we conclude that R is an integral domain. $\square$

§40.2 The Characteristic of a ring:

Let R be a commutative ring (recall $0_R \neq 1_R$). We automatically get a ring homomorphism

$$\mathbb{Z} \xrightarrow{\ \phi\ } R$$

$$n \longmapsto \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} & \text{if } n \geq 0 \\ -(\underbrace{1_R + \cdots + 1_R}_{-n \text{ times}}) & \text{if } n < 0 \end{cases}$$

Note: $\phi(0) = 0_R = \underbrace{1_R + \cdots + 1_R}_{0 \text{ times}}$

Let $I = \text{Ker}(\phi) \subseteq \mathbb{Z}$. Since $\mathbb{Z}$ is a PID, then $I = (p)$ for some $p \in \mathbb{Z}_{\geq 0}$.

Furthermore, $I \neq \mathbb{Z}$ since $\phi(1_{\mathbb{R}}) = 1_R$ & $1_R \neq 0_R$. Thus: $p = 0$ or $p \geq 2$.

Definition: We call p the characteristic of R.

⚠ We are not assuming p is prime if $p \neq 0$.

By First Isomorphism Theorem $\mathbb{Z}/p\mathbb{Z} \xhookrightarrow{\overline{\Phi}} R$ is an injective ring homomorphism

Lemma: If R is an integral domain, then $p = 0$ or p is a prime number.

Proof: We argue by contradiction, and assume $p \neq 0$ is composite. Pick, $a \neq 1$, $b \neq 1$ with $p = ab$

$\Rightarrow$ $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ with $\bar{a} \cdot \bar{b} = 0$. In particular, since $\overline{\Phi}$ is injective, we

$\overline{\Phi}(\bar{a}) \neq 0_R$ and $\overline{\Phi}(\bar{b}) \neq 0_R$.

Since $\overline{\Phi}(\bar{a})\,\overline{\Phi}(\bar{b}) = 0_R$, we conclude that R is not an integral domain. Contradiction!

Remark: $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$ if p is prime ($\mathbb{Z}/p\mathbb{Z}$ is a field, hence an integral domain)

§40.3 Prime ideals and Maximal ideals:

Let R be a commutative ring. Let $I \subsetneq R$ be a proper ideal and consider the quotient ring $\overline{R} = \frac{R}{I}$.

Definition: We say that I is a prime (respectively, maximal) ideal if $\overline{R} = R/I$ is an integral domain (respectively, a field).

Proposition: Let $I \subsetneq R$ be a proper ideal of R (commutative)

(1) I is prime if, and only if, I is a (proper) ideal and ($ab \in I \Rightarrow a \in I$ or $b \in I$)

(2) I is a maximal ideal if, and only if, I is a (proper) ideal and I is maximal with respect to inclusion among proper ideals, i.e.

$$J \subset R \text{ (an ideal) } \quad I \subseteq J \quad \Rightarrow J = I \text{ or } J = R$$

(3) Any maximal ideal is prime.

Proof: (3) is clear: if $\overline{R}$ is a field, then $\overline{R}$ is an integral domain.

(1) Assume I is proper.

I is prime $\iff$ R/I is an integral domain

$\iff$ ($a \pmod I \cdot b \pmod I = 0 \Rightarrow a = 0 \pmod I$ or $b = 0 \pmod I$)

$\iff$ ($ab \in I \Rightarrow a \in I$ or $b \in I$)

(2) Assume I is proper.

I is maximal $\iff$ R/I is a field

$\iff$ Only ideals of R/I are $\{\{0\}, R/I\}$

Lemma below

Since ideals of R/I correspond to ideals of R containing I (Theorem 2 §38.2)

we conclude I is maximal $\iff$ Set of ideals of R containing I is $\{I, R\}$

Lemma: A commutative ring K is a field, if and only if, Ideals of $K = \{\{0\}, K\}$

Proof: Recall that a commutative ring K is a field $\iff$ $K^{\times} = K \setminus \{0\}$. (ie, every non-zero element is invertible)

($\Rightarrow$) If $I \neq \{0\}$ is an ideal of K, then $\exists\, a \in I \setminus \{0\}$. In this case, we get $I \supset K \cdot a \ni a^{-1} \cdot a = 1$, so $I \supset K \cdot 1 = K$, giving $I = K$.

($\Leftarrow$) Let $a \in K \setminus \{0\}$ and set $I = (a)$ ideal generated by a.
Since $a \neq 0$, we have $I \neq 0$, so by assumption, we conclude $I = K$.
In particular, $1 \in I = K(a)$ so $\exists\, b \in K$ with $1 = ba$. Then $a \in K^{\times}$.
Conclude: $K \setminus \{0\} \subseteq K^{\times}$. Since $K^{\times} \subseteq K \setminus \{0\}$ by construction, equality holds □

§40.4 Some examples:

① Proper ideals in $\mathbb{Z}$: $\{0\}$ or $n\mathbb{Z}$ $(n \in \mathbb{Z}_{\geq 2})$

Prime ideals in $\mathbb{Z}$: $\boxed{\{0\}}$ or $\boxed{p\mathbb{Z} \quad (p \in \mathbb{Z}_{\geq 2} \text{ prime})}$

only prime, non-maximal ideal

maximal ideals in $\mathbb{Z}$

② Proper ideals in $\mathbb{C}[x]$: $\{0\}$ or $(g(x))$ $\quad g(x) \in \mathbb{C}[x]$ of degree $(g) = d \geq 1$, g monic. (ie $g = x^d + a_{d-1}x^{d-1} + \cdots + a_0$)

prime ideal

Lemma 1: $(0) \subsetneq R$ is a prime ideal $\iff$ R is an integral domain $(R = R/_{\{0\}})$

Over $\mathbb{C}$, every polynomial factors $g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$
$\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ not necessarily distinct

Lemma 2: Let $g(x) \in \mathbb{C}[x]$ be monic of degree $d \geq 1$

Then $(g(x)) \subsetneq \mathbb{C}[x]$ is prime $\Rightarrow$ degree of $g(x) = 1$ $\Rightarrow (g(x))$ is mxl

Proof: Assume $g(x) = (x - z_1) \cdots (x - z_d)$

$I := (g(x)) \subsetneq \mathbb{C}[x]$ then $d \geq 1$. Recall g is the element of $I \setminus \{0\}$ of smallest degree in I. By Prop §39.3 we have:

If I is prime & $(x-z_1)(x-z_2)\cdots(x-z_d) \in I \Rightarrow x - z_1 \in I$ or $\prod_{j=2}^{d}(x - z_j) \in I$.

Since $\deg(x - z_1) = 1$ & $\deg\left(\prod_{j=2}^{d}(x - z_j)\right) = d-1$, and d is smallest, we conclude $d = 1$. Thus, $g(x) = x - z$ for some $z \in \mathbb{C}$.

We conclude
$$\frac{\mathbb{C}[x]}{I} = \mathbb{C}[x]\big/(x-z) \simeq \mathbb{C} \quad \text{is a ring homomorphism.}$$
$$\overline{f(x)} \longmapsto f(z)$$

This map is induced from the so called evaluation map:

$$ev_\alpha : \mathbb{C}[x] \longrightarrow \mathbb{C} \qquad f(x) \longmapsto f(\alpha)$$

This map is surjective ($\forall a \in \mathbb{C} \subseteq \mathbb{C}[x]$: $ev_\alpha(a) = a$)

Claim: $\mathrm{Ker}(ev_\alpha) = (x - \alpha)$

Pf/ $ev(x-\alpha) = \alpha - \alpha = 0$ so $(x-\alpha) \subseteq \ker(ev_\alpha)$

Pick $f(x) \in \mathrm{Ker}(ev_\alpha)$, then using the Euclidean Algorithm, we have unique $f(x), r(x) \in \mathbb{C}[x]$
$f(x) = f(x)(x-\alpha) + r(x)$ with $r = 0$ or $\deg(r) < \deg(x-\alpha) = 1$.

In both cases, $r(x) \in \mathbb{C}$ ($r = 0$ or $\deg(r) = 0$).

$$\left.\begin{aligned} \text{Then } 0 = ev_\alpha(f(x)) &= ev_\alpha(f(x)(x-\alpha) + r(x)) \\ &= ev_\alpha(f(x))\, ev_\alpha(x-\alpha) + ev_\alpha(\overset{\in \mathbb{C}}{r(x)}) \\ &= ev_\alpha(f(x)) \cdot 0 + r = r \end{aligned}\right\} \Rightarrow r = 0. \text{ so } f(x) \in (x-\alpha)$$

By the 1st Iso Theorem $f = \overline{ev_\alpha}$ is an iso, so $(x-z)$ is maximal by Prop. §39.3. □

Conclusion: Prime ideals of $\mathbb{C}[x] \longleftrightarrow \{\{0\}\} \cup \boxed{\{(x-z) : z \in \mathbb{C}\}}$

↳ maximal ideals of $\mathbb{C}[x]$