MATH 3030 ALGEBRA I

Lecture 6

Ideals

Def An additive subgroup I of a ring R satisfying
$$aI \subseteq I \quad \text{and} \quad Ib \subseteq I \quad \forall a,b \in R$$
is called an <u>ideal</u> of R.

<u>Examples</u>

- For any ring R, $\{0\} \subset R$ and $R \subset R$ are ideals.
  An ideal $I \subsetneq R$ is called <u>proper</u> and
  an ideal $\{0\} \subsetneq I \subset R$ is called <u>nontrivial</u>.
- $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal for any $n \in \mathbb{Z}$ (and any ideal of $\mathbb{Z}$ is of this form).

- For $R = \{\text{functions } f : \mathbb{R} \to \mathbb{R}\}$,

  $I_a := \{f \in R \mid f(a) = 0\} \subset R$ is an ideal;

  $S := \{\text{const. fcns } f : \mathbb{R} \to \mathbb{R}\} \subset R$ is a subring but NOT an ideal.

- Let R be a commutative ring, and $a \in R$. Then

$$\langle a \rangle := \{ra \mid r \in R\}$$

is an ideal, called the <u>principal ideal</u> <u>generated by a</u>.

More generally, let $A \subset R$ be a nonempty subset. Then

$$\langle A \rangle := \{r_1 a_1 + \dots + r_n a_n \mid n \in \mathbb{Z}_{>0},\ r_i \in R,\ a_i \in A\}$$

is <u>the ideal generated by A</u>.

Ideals are important because of the following:

Thm Let $I \subseteq R$ be a subring. Then the multiplication on cosets

$$(a+I)(b+I) = ab + I \qquad (*)$$

is well-defined iff I is an ideal.

Cor Let $I \subseteq R$ be an ideal. Then the additive cosets of I form a ring R/I, called the quotient ring (or factor ring) of R by I, with the operations

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I) \cdot (b+I) = ab + I$$

Prop Let $I \subseteq R$ be an ideal. Then $\pi : R \to R/I$ defined by

$$\pi(a) = a + I$$

is a homomorphism with $\mathrm{Ker}(\pi) = I$.

Thm (1st Isom Thm) Let $\varphi : R \to R'$ be a homomorphism with kernel I.

Then

$$\begin{aligned} \overline{\varphi} : R/I &\longrightarrow \varphi(R) \\ a + I &\longmapsto \varphi(a) \end{aligned}$$

is an isomorphism s.t. $\varphi = \overline{\varphi} \circ \pi$.

Examples

- $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ as rings
- $R = \{\text{functions } f : \mathbb{R} \to \mathbb{R}\}$, $I_a = \{f \in R \mid f(a) = 0\}$ where $a \in \mathbb{R}$.

  Then $R/I_a \cong \mathbb{R}$

Cor Let F be a field.

(i) If $\mathrm{char}(F) = 0$, then $\exists\, \iota : \mathbb{Q} \hookrightarrow F$.

(ii) If $\mathrm{char}(F) = p$, then $\exists\, \iota : \mathbb{Z}_p \hookrightarrow F$

Pf: Consider the map

$$\iota : \mathbb{Z} \longrightarrow F$$
$$n \longmapsto n \cdot 1$$

This is a homomorphism, and

$$\mathrm{Ker}(\iota) = \begin{cases} 0 & \text{if } \mathrm{char}(F) = 0 \\ p\mathbb{Z} & \text{if } \mathrm{char}(F) = p \end{cases}$$

(Rmk: For any ring R w/ 1, we can define the homo.

$$\iota : \mathbb{Z} \longrightarrow R$$
$$n \longmapsto n \cdot 1$$

and $\ker \iota = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. When $R = D$ is an integral domain, either $m = 0$ or $m = p$ prime)

(i) In this case, ι induces $\iota : \mathbb{Q} \hookrightarrow F$ since $\mathbb{Q}$ is field of quotients of $\mathbb{Z}$.

(ii) In this case, ι induces $\iota : \mathbb{Z}_p \hookrightarrow F$. #

Rmk $\mathbb{Q}, \mathbb{Z}_p$ are called prime fields.

Prime and Maximal ideals

Prop Let R be a ring. If $I \subseteq R$ is an ideal containing a unit, then $I = R$.

Pf: Suppose that $u \in I$ is a unit. So $\exists\, u^{-1} \in R$ s.t. $u^{-1} u = 1 = u \cdot u^{-1}$. Since I is an ideal, $1 = u^{-1} u \in I$. But then $r = r \cdot 1 \in I$ $\forall r \in R$. #

Cor A nonzero commutative ring is a field iff it has no proper nontrivial ideals.

From now on, we restrict our attention to nonzero commutative rings. Let R be such a ring.

Def A *maximal ideal* of R is a proper ideal $M \subseteq R$ s.t. $\nexists$ a proper ideal $N \subseteq R$ s.t. $M \subsetneq N \subsetneq R$.

Lemma Let $\phi : R \longrightarrow R'$ be a homomorphism. Then

(i) I is an ideal of $R \Rightarrow \phi(I)$ is an ideal of $\phi(R)$.

(ii) J is an ideal of $R' \Rightarrow \phi^{-1}(J)$ is an ideal of R.

Thm Let R be a commutative ring.
Then $M \subseteq R$ is a maximal ideal iff R/M is a field.

Pf : The above Lemma gives a bijection

$$\left\{ \begin{matrix} N \text{ is an} \\ \text{ideal in } R \end{matrix} : M \subseteq N \subseteq R \right\} \longleftrightarrow \left\{ \begin{matrix} J \text{ is an} \\ \text{ideal in } R/M \end{matrix} \right\}$$

$$N \longmapsto \pi_M(N)$$

$$\pi_M^{-1}(J) \longleftarrow J$$

where $\pi_M : R \longrightarrow R/M$ is the projection map.

Now the Thm follows from the previous Cor. #

Examples • $n\mathbb{Z} \subseteq \mathbb{Z}$ is a maximal ideal iff $n=p$ is a prime.

• $I_a = \{f \in R \mid f(a)=0\} \subseteq R = \{\text{functions } f: \mathbb{R} \to \mathbb{R}\}$ is a maximal ideal.

• For any field F, $\langle x \rangle \subseteq F[x]$ is a maximal ideal since the evaluation map
$$\begin{aligned} F[x] &\longrightarrow F \\ f(x) &\longmapsto f(0) \end{aligned}$$
induces an isomorphism $F[x]/\langle x \rangle \cong F$

Similarly, $\langle x-a \rangle \subseteq F[x]$ is a maximal ideal for any $a \in F$.

More generally, given $a_1, a_2, \dots, a_n \in F$,
$$\langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle \subseteq F[x_1, \dots, x_n]$$
is a maximal ideal.

- Consider $\langle x^2+1\rangle \subseteq \mathbb{R}[x]$, and the map $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{C}$, $f(x) \mapsto f(i)$.
  φ is a ring homomorphism with $\ker\varphi = \{f \in \mathbb{R}[x] \mid f(i) = f(-i) = 0\}$
  $= \langle x^2+1\rangle$

  So φ induces an isom $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. Hence $\langle x^2+1\rangle$ is a maximal ideal in $\mathbb{R}[x]$.

Def A proper ideal $I \subsetneq R$ of a commutative ring R is called a <u>prime ideal</u> if $ab \in I \Rightarrow a \in I$ or $b \in I$.

It follows from this definition that

Prop Let R be a commutative ring with unity. Then a proper ideal $I \subsetneq R$ is prime iff R/I is an integral domain.

Cor Every maximal ideal in a commutative ring with unity is a prime ideal.

Examples

- In an integral domain D, $\{0\} \subseteq D$ is a prime ideal
- In $\mathbb{Z}[x]$, $\langle x \rangle \subseteq \mathbb{Z}[x]$ is prime but not maximal.
- In $\mathbb{Z}$, we have $\langle n \rangle \subseteq \mathbb{Z}$ is prime

$\iff$ $\langle n \rangle \subseteq \mathbb{Z}$ is maximal

$\iff$ n is a prime number

Ideals in $F[x]$

Def An integral domain D is called a principal ideal domain (PID) if every ideal in D is principal.

Example
- $\mathbb{Z}$ is a PID since any ideal in $\mathbb{Z}$ is of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$
- Any field F is a PID since it has no proper nontrivial ideals.

Prop $F[x]$ is a PID.

Pf: Let $I \subset F[x]$ be a nontrivial ideal.

Let $g(x) \in I \setminus \{0\}$ be an elt with minimum +ve degree.

We claim that $I = \langle g(x) \rangle$.

To see this, let $f(x) \in I \setminus \{0\}$. By the divison algorithm,

$\exists\, q(x), r(x) \in F[x]$ s.t. $f(x) = q(x) \cdot g(x) + r(x)$

where either $r(x) = 0 \in F[x]$ or $\deg r(x) < \deg g(x)$.

But $r(x) = f(x) - q(x) \cdot g(x) \in I$ as I is an ideal.

So we must have $r(x) = 0$, meaning that $f(x) \in \langle g(x) \rangle$.

This shows that $I \subseteq \langle g(x) \rangle$ and hence $I = \langle g(x) \rangle$. #

Prop Let $f(x) \in F[x]$ be a nonconstant polynomial. Then TFAE:

1. $f(x)$ is irreducible over F. (Recall that this means $f(x)$ cannot be written as the product of two lower degree polynomials.)
2. $\langle f(x) \rangle$ is maximal.
3. $\langle f(x) \rangle$ is prime

Pf: 1 $\Rightarrow$ 2: Suppose that $f(x)$ is irreducible over F.

Let I be an ideal of $F[x]$

s.t. $\langle f(x) \rangle \subsetneq I \subset F[x]$

By the above proposition, $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$.

This implies that $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$.

But $f(x)$ is irreducible over F and $\langle f(x)\rangle \neq I$.
So $g(x)$ must be a nonzero constant and thus $I = F[x]$.
Hence $\langle f(x)\rangle$ is maximal.

② $\Rightarrow$ ③ : By previous results.

③ $\Rightarrow$ ① : Suppose that $\langle f(x)\rangle$ is prime.
Let $f(x) = g(x)\,h(x)$ with $\deg g, \deg h < \deg f$.
Now $g \cdot h \in \langle f\rangle \Rightarrow$ either $g \in \langle f\rangle$ or $h \in \langle f\rangle$.
WLOG, assume $g \in \langle f\rangle$.
This implies that $g = f \cdot u$ for some $u \in F[x]$.
But then we have $\deg g \geq \deg f$, which is a contradiction. #

e.g. • x^2-2 is irreducible over $\mathbb{Q}$

$\Longrightarrow \mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

is a field.

• x^2+x+1 is irreducible over $\mathbb{Z}_2$

$\Longrightarrow \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field (of order $2^2=4$).