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 _ideal_ of R.

Rmk An ideal $I \subseteq R$ is in particular a subring of R.

Examples
- For any ring R, $\{0\} \subset R$ and $R \subset R$ are ideals. An ideal $I \subsetneq R$ is called _proper_ and an ideal $\{0\} \subsetneq I \subset R$ is called _nontrivial_.

- $n\mathbb{Z} \subseteq \mathbb{Z}$ 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

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

  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 $\pi : R \longrightarrow R/I$ defined by

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

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

Thm (1st Isom Thm) Let $\varphi : R \longrightarrow R'$ be a homomorphism with kernel I.
Then
$$\overline{\varphi} : R/I \longrightarrow \varphi(R)$$
$$a + I \longmapsto \varphi(a)$$

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

(ii) If $\text{char}(F) = p$, 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

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

(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 with unity. 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. $u^{-1} \cdot u = 1 = u \cdot u^{-1}$. 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 commutative ring with unity is a field iff it has no proper nontrivial ideals.

From now on, we restrict our attention to commutative rings with $1 \neq 0$. Let R be such a ring.

Def A <u>maximal ideal</u> 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) I' is an ideal of $R' \Rightarrow \phi^{-1}(I')$ is an ideal of R.

Pf: Q.22(a),(c) of §26. #

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

Pf: ($\Rightarrow$): Suppose that $M \leq R$ is a maximal ideal.
Then R/M is a nontrivial commutative ring with unity.

Let $\bar{a} = a + M \in R/M$ s.t. $a \notin M$.

Consider the principal ideal
$$\langle \bar{a} \rangle = \{(r+M)(a+M) \mid r \in R\} \subseteq R/M.$$

By the Lemma (ii) above, $\pi^{-1}\langle\bar{a}\rangle$ is an ideal in R where $\pi: R \longrightarrow R/M$ is the canonical map.

Note that $\pi^{-1}(\langle\bar{a}\rangle) \supsetneqq M$. Hence $\pi^{-1}(\langle\bar{a}\rangle) = R$.

In particular, $\pi(1) = 1 + M \in \langle\bar{a}\rangle$. So $\bar{a}$ is a unit in R/M.

($\Longleftarrow$): Suppose that R/M is a field. If $\exists$ a proper ideal

$$M \subsetneqq N \subsetneqq R$$

then $\pi(N)$ is an ideal of R/M by Lemma (i) above.

It is nontrivial since $M \neq N$ and

proper since $\pi(N) = R/M \Rightarrow 1 \in N \Rightarrow N = R$.

This contradicts the fact that a field doesn't contain any nontrivial proper ideals. #

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 $F[x] \to F$ induces an isomorphism $F[x]/\langle x \rangle \cong F$
$$f(x) \mapsto f(0)$$

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

  More generally, given $a_1, a_2, \ldots, a_n \in F$,
$$\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$$
  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 $\mathbb{R}[x]$.

$\|$ <u>Def</u> 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

$\|$ <u>Prop</u> 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
$$\iff \langle n \rangle \subseteq \mathbb{Z} \text{ is maximal}$$
$$\iff n \text{ is a prime number}$$

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.

|| <u>Prop</u> F[x] is a PID.

<u>Pf</u> : 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 division 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 ⟹ 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 $\mathbb{Q}$

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

   is a field.

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

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