

(§ 16.3) Ring Homomorphisms & Ideals.

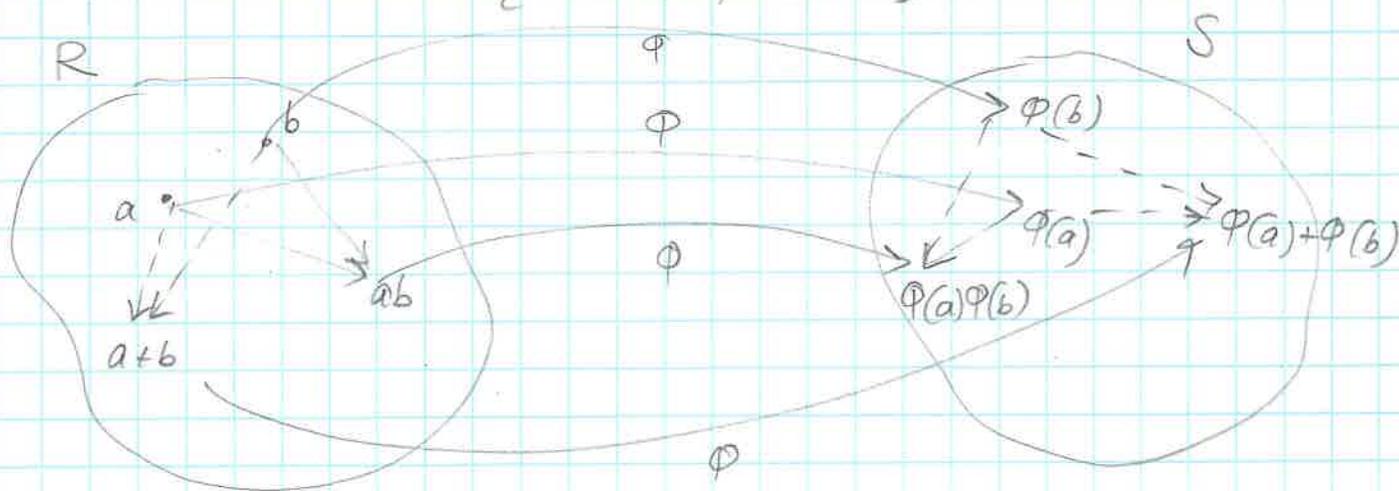
(1)

- Group homomorphism $G \rightarrow H$ preserves the operation of G .
- Rings: a homomorphism preserves two operations.

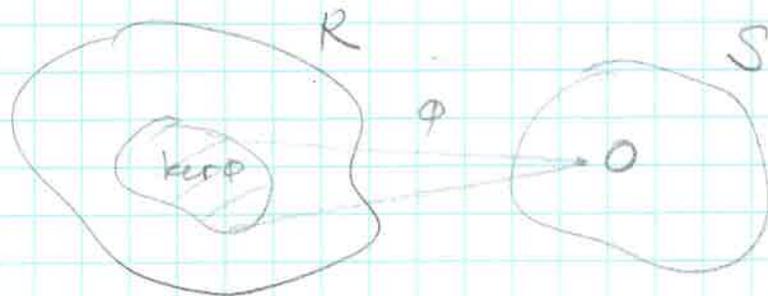
Def: • If R & S are rings, then a ring homomorphism is a map $\phi: R \rightarrow S$ satisfying $\forall a, b \in R$

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

- If ϕ is a bijection $\Rightarrow \phi$ is called a ring isomorphism.
- The kernel of a ring homomorphism is the set $\ker \phi = \{r \in R, \phi(r) = 0\}$



$\ker \phi$:



Examples:

- ① \forall positive $n \in \mathbb{Z}$, $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ defined by $\phi(a) = a \pmod{n}$ is a ring homomorphism:

$$\varphi(a+b) = (a+b) \pmod{n} = a \pmod{n} + b \pmod{n} = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = (ab) \pmod{n} = a \pmod{n} \cdot b \pmod{n} = \varphi(a)\varphi(b)$$

$$\ker \varphi = \{a \in \mathbb{Z}, \varphi(a) = 0 \pmod{n}\} = n\mathbb{Z}$$

② $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ by $\varphi(a+bi) = a-bi$ is a ring isomorphism. $\ker \varphi = \{0\}$ (automorphism)

It is a bijection & addition/multiplication preserving. (similar to group isomorphism, see Ex. 34, HW 8)

③ $\mathbb{R}[x]$ is a ring of polynomials w/ real coeff's.

Then $\varphi: \mathbb{R}[x] \rightarrow \mathbb{R}$ defined by $\varphi(p(x)) = p(0)$ is a ring homomorphism. Note: φ is onto.

$$\text{OP. for } \bullet: \varphi([pq](x)) = [pq](0) = p(0)q(0) = \varphi(p(x))\varphi(q(x)),$$

Onto: $\forall a \in \mathbb{R}, \exists p(x) = x+a \in \mathbb{R}[x]$ s.t.

$$\varphi(\underbrace{x+a}_{p(x)}) = \underbrace{0+a}_{p(0)} = a, \quad \text{Note: } \ker \varphi = \{p(x) \mid \underbrace{p(0)=0}_{\varphi(p(x))}\}$$

④ $C[a,b]$ is a ring of continuous real-valued functions on $[a,b]$. Fix $d \in [a,b]$.

Then $\varphi_d: C[a,b] \rightarrow \mathbb{R}$ defined by $\varphi_d(f(x))$

$= f(d)$ is a ring homomorphism onto \mathbb{R} .

$$\& \ker \varphi_d = \{f(x) \mid f(d) = 0\}$$

Examples ③ & ④

are examples of evaluation homomorphism.

⑤ let R be a commutative ring w/ $\text{char } R = 2$.

Then $\varphi: R \rightarrow R$ defined by $\varphi(r) = r^2$ ($\forall r \in R, 2r=0$) is a ring homomorphism: $\varphi(r+q) = (r+q)^2 = r^2 + 2rq + q^2 = r^2 + q^2 = \varphi(r) + \varphi(q)$ & $\varphi(rq) = (rq)^2 = r^2q^2 = \varphi(r)\varphi(q)$ "0"

Proposition (16.22): Properties of Ring Homomorphisms. (3)

Let $\phi: R \rightarrow S$ be a ring homomorphism.
Then:

easy (1) $\forall r \in R, n > 0, n$ integer, $\phi(nr) = n\phi(r)$
and $\phi(r^n) = [\phi(r)]^n$.

we will prove it (2) If A is a subring of R then $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S .

HWII (3) If R is commutative $\Rightarrow \phi(R)$ is commutative
($ab=ba$) ($\phi(a)\phi(b)=\phi(b)\phi(a)$)

HWII (4) $\phi(0_R) = 0_S$

we'll prove it (5) If ϕ is onto then $\phi(1_R) = 1_S$

DIY (6) If R is a field & $\phi(R) \neq \{0_S\} \Rightarrow \phi(R)$ is a field.

DIY (7) ϕ is an isomorphism $\Leftrightarrow \phi$ is onto & $\ker \phi = \{r \in R, \phi(r) = 0_S\} = \{0_R\}$.

Proof: (1) & (3) are from operation preservation.

Prove (4) (HWII) to use in proof for (2)

Proof of

(5): $\forall r \in R, 1_R \cdot r = r \cdot 1_R = r$.

next page!

Since ϕ is onto, $\forall s \in S, \exists r \in R$ s.t. $\phi(r) = s$.

Then $s = \phi(r) = \phi(r \cdot 1_R) = \phi(r)\phi(1_R)$ & also

$s = \phi(1_R)\phi(r)$. Thus, $\phi(1_R)$ is the identity

of S , 1_S . Note 1_S is unique (if we had 1_S & $1_S'$ then $1_S = 1_S \cdot 1_S' = 1_S'$) \square 2 identities

(2): $\Phi(A) = \{ \phi(a) \mid a \in A \}$ where A is a subring of S , let us use the subring test to prove $\Phi(A)$ is a subring of S . (4)

$\Phi(A) \neq \emptyset$ since $\phi(0_R) = 0_S \in \Phi(A)$ (see (4))

$\forall x, y \in \Phi(A)$, $x = \phi(a)$ & $y = \phi(b)$ for $a, b \in R$

$\Rightarrow xy = \phi(a)\phi(b) \stackrel{op}{=} \phi(\underbrace{ab}_{\in A}) \in \Phi(A)$ (closure \checkmark)

Now consider

$x - y = \phi(a) - \phi(b) \stackrel{*}{=} \phi(a) + \phi(-b) = \phi(\underbrace{a-b}_{\in A}) \in \Phi(A) \checkmark$

$\left[\begin{array}{l} (*) \phi(0_R) = \phi(b-b) = \phi(b) + \phi(-b) = 0_S \\ \Rightarrow -\phi(b) = \phi(-b) \end{array} \right]$

So, $\Phi(A)$ is a subring of S . □

Ideals

Def. An ideal of a ring R is a subring I of R s.t. if $a \in I$ and $r \in R$, then ar and $ra \in I$, i.e. $rI \subset I$ & $Ir \subset I \forall r \in R$.

- Often referred to as two-sided ideal

- Ideals "absorb" elements of a ring:

$$rI = \{ ra \mid a \in I \} \subset I \text{ and } Ir = \{ ar \mid a \in I \} \subset I$$

- Ideals "play role" of normal subgroups and are used to construct factor rings.

- Ideal I is proper if I is a proper set of R .

- For any ring R , there are two trivial ideals:

$\{0\}$ and R itself.

Note: If R is a ring w/ identity 1 & $\textcircled{5}$
 I is an ideal of R s.t. $1 \in I$, then
 $\forall r \in R, \left. \begin{array}{l} r \cdot 1 = r \in I \\ 1 \cdot r = r \in I \end{array} \right\} \text{(by def. of } I) \Rightarrow \underline{I = R}$.

Examples of ideals: $\textcircled{1}$ $\forall n > 0$, integer, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is an ideal of \mathbb{Z} .

(Recall $n\mathbb{Z}$ is a subring of \mathbb{Z} . Then consider $a \in n\mathbb{Z} \Rightarrow a = nb, b \in \mathbb{Z} \Rightarrow \forall r \in \mathbb{Z}, ar = (nb)r = n(br) \in n\mathbb{Z}$ and $ra = r(nb) = n(rb) \in n\mathbb{Z}$.)

(\mathbb{Z} is a comm. ring w/ unity)

$\textcircled{2}$ If R is a commutative ring w/ unity and $a \in R$, then the set $\langle a \rangle = \{ar \mid r \in R\}$ ($= \{ra \mid r \in R\}$) is an ideal of R called the principal ideal generated by a .

(Recall: $\langle a \rangle$ also denotes a cyclic group generated by a)

Why is $\langle a \rangle$ an ideal of R ? First, $\langle a \rangle \neq \emptyset$ since $0 = a0$ and $a = a1$ are in $\langle a \rangle$. Also, $\forall x, y \in \langle a \rangle, xy = (ar_1)(ar_2) = a(r_1 r_2) \in \langle a \rangle$ for some $r_1, r_2 \in R$.
 $(\Rightarrow$ closure)

and $x - y = ar_1 - ar_2 = a(r_1 - r_2) \in \langle a \rangle \Rightarrow \langle a \rangle$ is a subring of R .

For any $x \in \langle a \rangle, x = ar$ for some $r \in R$. Let $s \in R$

$\Rightarrow s(ar) = a(sr) \in \langle a \rangle \Rightarrow \langle a \rangle$ is an ideal (called principal ideal)
 (R is commutative)

Theorem (16.25) Every ideal in the ring \mathbb{Z} is a principal ideal.

(Read proof! \leftarrow see text)

\Rightarrow Note: the sets $n\mathbb{Z}$ are the only ^{nontrivial} principal ideals for \mathbb{Z} .

③ Let A be the set of polynomials w/ real coefficients and constant term 0. Then A is an ideal of $\mathbb{R}[x]$. ⑥

First of all, A is a subring of $\mathbb{R}[x]$ (show!).
use subring test

Then $\forall p \in A$, $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x = q(x) \cdot x = x q(x)$
 w/ $q(x) \in \mathbb{R}[x]$

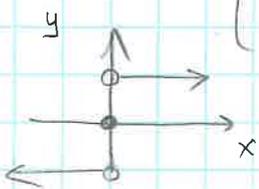
Therefore, $A = \langle x \rangle = \{ q(x)x \mid q(x) \in \mathbb{R}[x] \}$
 i.e., A is a principal ideal of $\mathbb{R}[x]$.

④ Example of "non ideal":

If R is the ring of all real-valued func's of real variable, then the subset S of all differentiable functions is a subring of R (show why), but not an ideal of R .

Why? Consider $S(x) \equiv 1 \in S$. If we take

$r(x) = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$ in R , then $r(x)S(x) = r(x) \notin S$



$r(x) = \text{sgn}(x)$

$\mathbb{Z}_n = \langle 1 \rangle \Rightarrow$
 Its subgroups are $\langle 1^{n/k} \rangle = \langle \frac{n}{k}, 1 \rangle = \langle \frac{n}{k} \rangle$

⑤ Fact: in \mathbb{Z}_n , the ideals are precisely the sets of the form $\langle d \rangle$ where $d \in \mathbb{Z}_n$ and $d \mid n$. Why?

\mathbb{Z}_n is a cyclic additive group w/ subgroups $\langle \frac{n}{k} \rangle$ of order k , where $k \mid n$. So, $d = \frac{n}{k}$ divides n & $\langle d \rangle = \{ md \mid m \in \mathbb{Z} \} \subset \mathbb{Z}_n$
 $\Rightarrow \langle d \rangle = \{ md \mid m \in \mathbb{Z}_n \} \Rightarrow \langle d \rangle$ is the principal ideal generated by d & $d \mid n$.

Proposition (16.27) The kernel of any ring ⑦

homomorphism $\phi: R \rightarrow S$ is an ideal in R .

("kernels are ideals" \leftarrow "kernels are normal subgroups")

(Recall: for groups, $\ker \phi$ is a normal subgroup of G)
($\phi: G \rightarrow H$)

Proof: $\ker \phi = \{r \in R \mid \phi(r) = 0_S\}$ is a subring of R :

$\phi(0_R) = 0_S \Rightarrow \ker \phi \neq \emptyset$. For any $a, b \in \ker \phi$,

$$\phi(a-b) = \phi(a + (-b)) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0 - 0 = 0$$

$$\Rightarrow a-b \in \ker \phi; \quad \phi(ab) = \phi(a)\phi(b) = 0 \Rightarrow ab \in \ker \phi \Rightarrow$$

by the subring test, $\ker \phi$ is a subring of R .

To show it is an ideal, take $a \in \ker \phi$ and $r \in R$.

Then $\phi(ar) = \phi(a)\phi(r) = 0$, similarly, $\phi(ra) = 0$.

Thus, $ar \in \ker \phi$ & $ra \in \ker \phi \Rightarrow \ker \phi$ is an ideal of R .

□

One-sided ideals: let I be a subring of a ring R .

If we require that $rI \subset I \quad \forall r \in R \Rightarrow I$ is called a left ideal, if $Ir \subset I \quad \forall r \in R \Rightarrow I$ is called a right ideal of R .

Note that in a commutative ring, any ideal is two-sided.

Factor rings:

Let R be a ring and I be an ideal of R .

Then $R/I = \{r+I \mid r \in R\}$ is a factor ring of R and I w/ multiplication defined by

$$(r+I)(s+I) = rs + I \quad \left(\text{Addition: } (r+I)+(s+I)=(r+s)+I \right)$$

To confirm that R/I is a ring, read Theorem (16.29) w/ proof: {need to show that $rs+I$ is well-defined + axioms}

Note: the factor ring R/I is also called a quotient ring.

Examples: ① $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$ (with arrows pointing from \mathbb{Z} to "ring" and from $4\mathbb{Z}$ to "ideal")

How to add & multiply? E.g.,

$$(2+4\mathbb{Z}) + (3+4\mathbb{Z}) = 5+4\mathbb{Z} = 1 + \underbrace{4+4\mathbb{Z}}_{4\mathbb{Z}} = 1+4\mathbb{Z}$$

$$(2+4\mathbb{Z})(3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2 + \underbrace{4+4\mathbb{Z}}_{4\mathbb{Z}} = 2+4\mathbb{Z}$$

② $2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$ (with arrows pointing from $2\mathbb{Z}$ to "ring" and from $6\mathbb{Z}$ to "ideal")

E.g., $(4+6\mathbb{Z}) + (4+6\mathbb{Z}) = 2+6\mathbb{Z}$
 $(4+6\mathbb{Z})(4+6\mathbb{Z}) = 16+6\mathbb{Z} = 4 + \underbrace{12+6\mathbb{Z}}_{\text{multiples of 6}} = 4+6\mathbb{Z}$

Note $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$:

$$\forall r \in 2\mathbb{Z}, q \in 6\mathbb{Z}, rq = (2k)(6l) = 12kl = 6(\underbrace{2kl}_{\in \mathbb{Z}}) \in 6\mathbb{Z}$$

③ $\mathbb{R}[x]$ is the comm. w/unity ring of polynomials w/ real coeff's.

Consider $\langle x^2+1 \rangle = \{ (x^2+1)f(x) \mid f(x) \in \mathbb{R}[x] \}$;

it is the principal ideal generated by $p(x) = x^2+1$.

Then $\mathbb{R}[x] / \langle x^2+1 \rangle = \{ g(x) + \langle x^2+1 \rangle \mid g(x) \in \mathbb{R}[x] \}$

Note: if $g(x) \in \mathbb{R}[x]$ then $g(x) = q(x)(x^2+1) + r(x)$
w/ $r(x) = 0$ or $r(x) \neq 0$ w/ $\text{deg } r < 2 \Rightarrow r(x) = ax+b$,
w/ $a, b \in \mathbb{R}$.

(9)

$$\begin{aligned} \text{So, } g(x) + \langle x^2+1 \rangle &= \underbrace{g(x)(x^2+1)}_{\in \langle x^2+1 \rangle} + \underbrace{r(x)}_{\substack{\text{''} \\ ax+b}} + \langle x^2+1 \rangle \\ &= r(x) + \langle x^2+1 \rangle \end{aligned}$$

$$\text{So, } \mathbb{R}[x]/\langle x^2+1 \rangle = \{ ax+b + \langle x^2+1 \rangle, a, b \in \mathbb{R} \}.$$

Q: How is multiplication done in $\mathbb{R}[x]/\langle x^2+1 \rangle$?

Note: $\text{Ex: } x^2+1 + \langle x^2+1 \rangle = 0 + \langle x^2+1 \rangle \Rightarrow x^2+1=0 \text{ or } x^2=-1.$ Can think ↘

$$\begin{aligned} \text{So, e.g., } (x+3 + \langle x^2+1 \rangle)(2x+5 + \langle x^2+1 \rangle) \\ &= \underbrace{2x^2 + 11x + 15}_{= 2(-1) + 11x + 15} + \langle x^2+1 \rangle = 11x + 13 + \langle x^2+1 \rangle \\ &= 2(-1) = -2 \end{aligned}$$

Interesting fact: $\mathbb{R}[x]/\langle x^2+1 \rangle$ has elements in the form $ax+b + \langle x^2+1 \rangle$ w/ $x^2 + \langle x^2+1 \rangle = -1 + \langle x^2+1 \rangle$ $a, b \in \mathbb{R}$
 $\Rightarrow \mathbb{R}[x]/\langle x^2+1 \rangle$ is algebraically the same as the ring of complex #'s! $\mathbb{C} = \{ a+bi \mid a, b \in \mathbb{R}, i^2 = -1 \}$

Natural (Canonical) Homomorphism:

Let R be a ring, I be an ideal of R .

The map $\phi: R \rightarrow R/I$ defined by $\phi(r) = r+I$ is the canonical ring homomorphism w/ $\ker \phi = I$.

Theorem (6.31) First Isomorphism Theorem (for rings)

Let $\psi: R \rightarrow S$ be a ring homomorphism. Then $\ker \psi$ is an ideal of R . If $\phi: R \rightarrow R/\ker \psi$ is the canonical homomorphism, then

there exists a unique isomorphism η :
 $R/\ker\psi \rightarrow \psi(R)$, s.t. $\psi = \eta\phi$. That is,
 $R/\ker\psi \cong \psi(R)$

