Week 2: #

16.3: Homomorphisms, subrings, ideals

Def: Given rings R and S, a **ring homomorphism** is a map

$$\phi: R \to S$$

such that ① $\phi(a+b) = \phi(a) + \phi(b)$

② $\phi(ab) = \phi(a)\phi(b)$

$\forall\, a, b \in R$

remarks:

1) First condition implies (for free) $\phi(0_R) = 0_S$

2) But if R and S both have unity, then are not enough to guarantee $\phi(1_R) = 1_S$

if $\phi(1_R) \neq 1$ then $\phi(r)$ is a zero-divisor for all $r \in R$

Examples:

① $\pi: \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$

$a \longmapsto [a]$

this is a homomorphism: $[a+b] = [a] + [b]$

$[ab] = [a] \cdot [b]$

and have $1 \mapsto [1]$

② $ev_i: \mathbb{R}[x] \to \mathbb{C}$ "evaluate at i"

$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \longmapsto p(i) = a_0 + a_1 i + \dots + a_n i^n$

this is a ring homomorphism $(p+q)(i) = p(i) + q(i)$

$(p \cdot q)(i) = p(i) \cdot q(i)$

$p(x) = 1 \longmapsto 1$

(unity is sent to unity)

③ (non-examples) $\det: M_2(\mathbb{R}) \to \mathbb{R}$

$A \longmapsto \det(A)$

$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longmapsto 1$ (unity set to unity)

we see $\det(AB) = \det(A)\det(B)$

BUT $\det(A+B) \neq \det(A) + \det(B)$

Recall: 1st isomorphism theorem for groups

If $\varphi: G \to H$ is a group homomorphism

1) $\operatorname{im}(\varphi)$ is a subgroup of H 2) $\ker(\varphi)$ is a normal subgroup of G

3) map $G/\ker(\varphi) \to \operatorname{im}(\varphi)$ given by $g\ker(\varphi) \mapsto \varphi(g)$ is an isomorphism

1st isomorphism theorem for Rings

If $\phi: R \to S$ is a ring homomorphism, then

1) $\text{im}(\phi)$ is a subring of S
2) $\text{Ker}(\phi)$ is an ideal of R
3) the map $R/\text{Ker}(\phi) \to \text{im}(\phi)$ given by $r + \text{Ker}(\phi) \mapsto \phi(r)$ is an isomorphism

A subring of a ring R is a subset $T \subseteq R$ that is itself a ring under the same operation (we assume $1 \in T$)

equivalently: 1) T is nonempty ($\iff 0 \in T$)
2) T closed under difference (+ and add. inverse)
3) closed under product: if $t_1, t_2 \in T$ then $t_1 t_2 \in T$

Claim: If $\phi: R \to S$ is a ring homomorphism
$\text{Ker}(\phi) = \{r \in R : \phi(r) = 0\}$ is an additive (normal) subgroup
that is "closed under scaling"
if $k \in \text{Ker}(\phi)$ and $r \in R$, then $rk, kr \in \text{Ker}(\phi)$
(proof, use homomorphism prop.) $\phi(rk) = \phi(r)\phi(k) = \phi(r) \cdot 0 = 0$
(similar for kr)

An ideal of a ring R is a subset $I \subseteq R$ with

1) I is nonempty
2) I closed under difference
3) I closed under scaling, if $i \in I$ and $\boxed{r \in R}$ then $ir \in I$

As with groups
if $I \subseteq R$ is an ideal of R, we can form a quotient ring

set R/I = additive cosets of I $= \{r + I : r \in R\}$
(where $r + I = \{r + i : i \in I\}$
and $r + I = r' + I \iff r - r' \in I$)

operations $(r_1 + I) + (r_2 + I) = r_1 r_2 + I$ (already know this is well-defined)
$(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I$ ← well defined?

Suppose $r_1 + I = r_1' + I$ ($\iff r_1 - r_1' \in I$, $r_1 - r_1' = i_1 \in I$)
$r_2 + I = r_2' + I$ ($\iff r_2 - r_2' \in I$, $r_2 - r_2' = i_2 \in I$)

then $r_1 r_2 - r_1' r_2' = r_1 r_2 - (r_1 - i_1)(r_2 - i_2) = r_1 r_2 - r_1 r_2 + r_1 i_2 + i_1 r_2 - i_1 i_2$
$= r_1 i_2 + i_1 r_2 - i_1 i_2 \in I$ (closed under scaling)

then $R \to R/I$, $r \mapsto r+I$ is a ring homomorphism

Ex: $\pi: \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, $4\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal

Ex 1: Suppose $\phi: R \to S$ is a ring homo. between rings with unity

notice: If $r \in R$ is any element, then $\phi(r) = \phi(1_R \cdot r) = \phi(1_R) \cdot \phi(r)$

so $\phi(r) - \phi(1_R)\phi(r) = 0 \Rightarrow 1_S \phi(r) - \phi(1_R)\phi(r) = 0$

$\Rightarrow (1_S - \phi(1_R))\phi(r) = 0_S$

case 1: $1_S - \phi(1_R) = 0$ i.e. $\phi(1_R) = 1_S$

case 2: $1_S - \phi(1_R) \neq 0$ i.e. $\phi(1_R) \neq 1_S$ then $\phi(r)$ is a zero divisor in S

$\Rightarrow im(\phi)$ is all zero-divisors

Assumptions from now on:

1) All rings have unity (no rngs)

2) Ring hom.s preserve unity

Ex 2: Suppose R is a ring (with unity)

Claim: there is a unique ring hom. $\phi: \mathbb{Z} \to R$

Proof: (uniqueness) Suppose $\phi: \mathbb{Z} \to R$ is a ring hom.

then $\phi(1) = 1_R$ (also $\phi(0) = 0_R$)

Take any $n > 0$ in $\mathbb{Z}$, then $\phi(n) = \phi(\underbrace{1+1+\dots+1}_{n \text{ times}}) = \underbrace{\phi(1)+\phi(1)+\dots+\phi(1)}_{n \text{ times}}$

$= 1_R + 1_R + \dots + 1_R$

$= n \cdot 1_R$ (n times 1_R)

If $n < 0$, $\phi(n) = \phi(-(-n)) = -\phi(-n) = -(1_R + 1_R + \dots + 1_R) = n \cdot 1_R$

($-n$: positive integer)

Can check: $\phi(n) = n \cdot 1_R$ defines a homomorphism

Ex 3: Let R be any ring and $\phi: \mathbb{Z} \to R$ be the unique hom.

consider $Ker(\phi) = \{n \in \mathbb{Z} : n \cdot 1_R = 0\} \subseteq \mathbb{Z}$

$Ker(\phi)$ is an ideal in the integers

$\Rightarrow$ its an additive subgroup - also closed under scaling

$\Rightarrow Ker(\phi) = \langle d \rangle = d\mathbb{Z} = \{\dots, -2d, -d, 0, d, 2d, \dots\}$ for some $d \geq 0$

Case 1: $d = 0$, i.e. $Ker(\phi) = \{0\}$ i.e. ϕ is injective

$\Rightarrow \mathbb{Z} \cong im(\mathbb{Z}) \Rightarrow$ R contains a copy of the integers

E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}(\sqrt{2}), \mathbb{R}[x], M_n(\mathbb{R})$

so in this case where $\ker(\phi) = \{0\}$ we say R has <u>characteristic zero</u>

$\text{char}(R) = 0$

<u>Case 2</u>: $I \neq 0$, i.e. $\ker(\phi) = d\mathbb{Z} = \{\dots -d, 0, d, \dots\}$

i.e. $\underbrace{1_R + 1_R + \dots + 1_R}_{d \text{ times}} = 0_R$ $\quad$ d is the smallest pos. int. s.t. this work

we say that R has <u>characteristic d</u>

example: $\text{char}(\mathbb{Z}/n\mathbb{Z}) = n$

$\text{char}(M_2(\mathbb{Z}/2\mathbb{Z})) = 2$

<u>Ex 4</u>: Later $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ will be defined as the smallest subfield of $\mathbb{Q}$ containing $\sqrt{2}, \sqrt{3}$

but for for now: $R(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\}$

Hard question: why is this a field? inverses

strategy #1: use definition of the inverse

given a fixed nonzero element $\theta = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

Try to solve $(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(w + x\sqrt{2} + y\sqrt{3} + z\sqrt{6}) = 1$

$$(aw + 2bx + 3cy + 6dz)1 + (ax + bw + 3cz + 3dy)\sqrt{2} + (ay + 2bz + cw + dx)\sqrt{3} + (az + by + cx + dw)\sqrt{6} = 1 + 0\sqrt{2} + 0\sqrt{3} + 0\sqrt{6}$$

fact: $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ are linearly independent

$\Rightarrow$ solve: $aw + 2bx + 3cy + 6dz = 1$

$\vdots$

$az + by + cx + dw = 0$

strategy #2: $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ is linearly dependent

so there is some $c_0 1 + c_1\theta + c_2\theta^2 + c_3\theta^3 + c_4\theta^4 = 0$ for some $c_i \in \mathbb{Q}$ not all 0

Use this equation to find a formula for θ^{-1}

strategy #3: Use "conjugate strategy"

$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \underbrace{(a + b\sqrt{2})}_{\alpha} + \underbrace{(c + d\sqrt{2})}_{\beta}\sqrt{3} = \alpha + \beta\sqrt{3}$ $\quad$ where $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$ (a field)

Idea: $(\alpha + \beta\sqrt{3})(\alpha - \beta\sqrt{3}) = \alpha - 3\beta^2 \in \mathbb{Q}(\sqrt{2})$

if $\alpha^2 - 3\beta^2 \neq 0$, then it has an inverse in $\mathbb{Q}(\sqrt{2})$, say $\gamma \in \mathbb{Q}(\sqrt{2})$

so $\underbrace{(\alpha + \beta\sqrt{3})}_{\theta}\underbrace{[(\alpha - \beta\sqrt{3})\gamma]}_{\in \mathbb{Q}(\sqrt{2}, \sqrt{3})} = 1$