lecture 5 Feb 2, 2022 -1-

$\alpha : R \to S$ homomorphism

$\alpha(a+b) = \alpha(a) + \alpha(b)$ respects addition

$\alpha(ab) = \alpha(a)\alpha(b)$ respects multiplication

$\alpha(1) = 1$ identity to identity

(as for sets)

$\mathrm{Im}(\alpha) = \{ s \in S \mid s = \alpha(a) \text{ for some } a \in R \} = \{ \alpha(a) \mid a \in R \}$

image of α, image of R under α

Prop $\mathrm{Im}(\alpha)$ is a subring of S Exercise.

$\ker(\alpha) = \{ a \in R \mid \alpha(a) = 0 \}$ kernel of α, a subset of R.

α is a homomorphism of abelian groups $\Rightarrow \ker(\alpha) \subset R$ is an abelian group under addition.

$\ker(\alpha) = \{a \in R \mid \alpha(a) = 0\}$.

1). If $a \in \ker(\alpha)$, $b \in R \Rightarrow ab \in \ker(\alpha)$.

Need to check $\alpha(ab) = \alpha(a)\alpha(b) = 0 \cdot \alpha(b) = 0$. True

$\Rightarrow \ker(\alpha)$ is closed under multiplication by elements of R.

$\ker(\alpha) \subset R$ is an abelian subgroup of R under the addition operation, and closed under multiplication by elements of R — ideal in R

Example 1) $\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/n$ $\alpha(a) = a \pmod n$ $\alpha(a) = a + n\mathbb{Z}$

$\ker(\alpha) = n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$. $n\mathbb{Z}$ - abelian subgroup, closed under mult.

2) Lemma: any homomorphism $\alpha : R \to S$ is injective iff $\ker(\alpha) = \{0\}$

$\{0\}$ is the smallest possible kernel for a homomorphism.

$\ker(\alpha)$ always contains 0, for any homomorphism α

$$\begin{array}{ccc} \alpha: R & \longrightarrow & S \\ \cup & & \cup \\ \ker(\alpha) & & \operatorname{im}(\alpha) \\ \text{ideal of } R & & \text{subring} \end{array}$$

To prove lemma:

If α is injective, $\ker(\alpha)$ contains unique element $0 \in R$.

If $\ker(\alpha) = \{0\}$ and α not injective $\Rightarrow$

$\exists\, a, b \in R$, $a \neq b$ such that $\alpha(a) = \alpha(b) \Rightarrow$

$\alpha(a) - \alpha(b) = 0$, $\alpha(a-b) = 0 \Rightarrow a - b \in \ker\alpha$, $a - b \neq 0$ Contradiction.

Similar to homomorphisms of groups $\alpha : G \to H$ group

α injective $\Leftrightarrow \ker(\alpha) = \{1\}$ trivial subgroup.

<u>Def</u> An ideal I in a ring R is an abelian subgroup (under $+$) closed under multiplications by elements of R

(a) $(I, +)$ an abelian group ($\Rightarrow I \neq \emptyset$ not empty)

(b) $a \in I, r \in R \Rightarrow ra \in I$

work with ~~order~~ commutative rings only $\Rightarrow ra = ar$

Reminder

define $rI =: \{ra \mid a \in I\}$ $rI \subset I$.

$I \subset R$ is called a <u>proper</u> ideal if $I \neq R$

Ring R always contains ideals $\{0\}, R$

<u>Prop</u> Ideal $I = R$ iff $1 \in I$ iff I contains an invertible element.

Hint: $1 \in I \Rightarrow r \cdot 1 = r \in I$ $\forall r \in R$. complete the proof

Pick $a \in R$. Ideal $Ra = \{ra \mid r \in R\}$ is called <u>principal</u> ideal generated by a. $Ra = (a)$.

notation

<u>Exercise</u> $Ra = (a)$ is an ideal.

Take $a_1, \dots, a_n \in R$. Consider sums of products $r_1 \dots r_n \in R$

$r_1 a_1 + r_2 a_2 + \dots + r_n a_n$.

$(a_1, \dots, a_n) \overset{def}{=} \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_1, \dots r_n \in R\}$

<u>Thm</u> $(a_1, \dots, a_n)$ is an ideal of R.

closed under subtraction $\Leftarrow$ (our hack to show subset is an abelian subgroup)

$r_1 a_1 + \dots + r_n a_n - (r_1' a_1 + \dots + r_n' a_n) = (r_1 a_1 - r_1' a_1) + (r_2 a_2 - r_2' a_2) + \dots + (r_n a_n - r_n' a_n) =$

$= (r_1 - r_1') a_1 + (r_2 - r_2') a_2 + \dots + (r_n - r_n') a_n$

<u>Complete the proof</u>

$$\begin{array}{ccc} \alpha : R & \longrightarrow & S \\ \cup & & \cup \\ \ker(\alpha) & & \operatorname{Im}(\alpha) \\ \text{ideal} & & \text{subring} \end{array}$$

homomorphism of rings

$\alpha(a+b) = \alpha(a) + \alpha(b)$ addition

$\alpha(ab) = \alpha(a)\alpha(b)$ mult.

$\alpha(1) = 1$ identity.

$\ker(\alpha) \subset R$

Prop $\ker(\alpha)$ is an ideal of R

Proof: nonempty, $0 \in \ker(\alpha)$

$\alpha(a)=0, \alpha(b)=0 \Rightarrow \alpha(a-b) = \alpha(a) - \alpha(b) = 0$

$\alpha(a)=0 \Rightarrow \alpha(ra) = \alpha(r)\alpha(a) = \alpha(r)\cdot 0$
$= 0 \in S$

closed under mult. by elements of R

Prop $\{0\}$ and F are the only ideals of a field F.

Proof Any nonzero element of F is invertible. If $I \subset F$ ideal, either $I = \{0\}$ or contains a nonzero element r, $r \in I$. $\Rightarrow r^{-1} r \in I \Rightarrow 1 \in I$
$\Rightarrow a \in I \ \forall a \in F$ $a \cdot 1$ D.

Corollary Any homomorphism $F \xrightarrow{\alpha} R$ of a field F into a ring R is injective
$\alpha(1) = 1 \in R \Rightarrow \ker(\alpha) \neq F \Rightarrow \ker(\alpha) = 0 \Rightarrow \alpha$ injective (exception $R = \{0\}$)

Ideal $(a) = R$ iff a is invertible, $ab = 1$ some b. $(b = a^{-1})$

Ideals in $\mathbb{Z}$ $I \subset \mathbb{Z}$ either $I = \{0\}$ or $\exists n \in I, n > 0$ $(I = -I)$

Choose smallest $n > 0, n \in I$. Then $n\mathbb{Z} \subset I$. if $n\mathbb{Z} \neq I$, choose $a \in I \setminus n\mathbb{Z}$

$a = nk + r$ $0 < r < n$ $r = a - nk$; $a \in I, nk \in I \Rightarrow r \in I$, contradiction

Prop Any ideal of $\mathbb{Z}$ has the form (0) or $(n) = n\mathbb{Z}, n > 0$.

Case $n=1$ $(1) = \mathbb{Z}$ entire ring, $(2) = 2\mathbb{Z}$, $(3) = 3\mathbb{Z}$, ..

(n) principal ideal generated by n, $(-n) = (n)$ $(ra) = (a)$ if r is invertible

Def Ring R is called a PID (principal ideal domain)

if every ideal of R is principal & R is an integral domain (no zero divisors)

Corollary $\mathbb{Z}$ is a PID.

$\alpha: R \to S$ want to say that subring $\mathrm{Im}(\alpha)$ is the quotient of R by ideal $\ker(\alpha)$,

$\ker(\alpha) \subset R$ ideal, $\mathrm{im}(\alpha) \subset S$ subring.

since elements of $\mathrm{Im}(\alpha)$ are cosets $r + \ker(\alpha)$.

α-surjective $\Rightarrow$ $S = \mathrm{Im}(\alpha)$

Let $I \subset R$ be an ideal. $(I, +) \subset (R, +)$ abelian subgroup. $\Rightarrow$

Can form the abelian group of cosets R/I (I is normal in R, since R is abelian)

elements of R/I have the form $r+I$, $r \in R$ $\quad$ $r+I = r'+I$ iff $r-r' \in I$

R/I abelian group under addition

$(r+I) + (r'+I) = (r+r') + I$

Identity element of R/I under addition? coset $0+I = I$

The inverse of $r+I$ under $+$? $(-r)+I$

$(r+I) + (-r+I) = (r-r) + I = 0 + I = I.$

Have the natural surjective map $\pi: R \to R/I$

$\pi(r) = r+I$. π is a homomorphism of abelian groups.

Define multiplication on R/I:

$$(r+I)(r'+I) = rr' + I$$

Claim: This is well-defined. If $r+I = s+I$ and $r'+I = s'+I$,

need to show $s.s' + I = rr' + I$ $\quad$ $(s+I)(s'+I) = ss'+I$

$$rr' - ss' = (rr' - rs') + (rs' - ss') = r\underbrace{(r'-s')}_{I} + \underbrace{(r-s)}_{I}s'$$

$r(r'-s') \in I$, $(r-s)s' \in I$ $\Rightarrow$ their sum is in I, $rr'-ss' \in I$.

Indeed, multiplication is well-defined.

<u>Theorem</u> For an ideal I in R, the set R/I is a ring with this addition and multiplication.

<u>Proof</u>: (work out details). $(+, \cdot)$ are well-defined operations on R/I

$\underline{0} = 0 + I$ is the zero of R/I

$\underline{1} = 1 + I$ is the identity of R/I.

Ring axioms in R/I follow since R is a ring. To prove a property (associativity, distributivity), lift to R, observe that it holds there, descend to R/I. Or check all properties directly

$(a+I)(b+I)(c+I)$. associativity

$$((a+I)(b+I))(c+I) = (ab+I)(c+I) = (ab)c + I$$
$$\parallel$$
$$abc + I$$
$$\parallel$$
$$(a+I)((b+I)(c+I)) = (a+I)(bc+I) = a(bc)+I$$

Awkward to manipulate cosets, usually want a concrete model (set) for R/I to work with it (basis, or coset representatives, etc.)

<u>Thm</u> the quotient map $\pi: R \to R/I$ is a surjective homomorphism of rings. $I = \ker(\pi)$.

$$R \xrightarrow{\pi} R/I$$
$$1 \mapsto \underline{1} = 1 + I$$

also ok to just write 1 for $1+I$, r for $r+I$ but remember that dealing with cosets.

<u>Example</u> $I = (n) \subset \mathbb{Z}$.

The quotient ring $\mathbb{Z}/(n) \simeq \mathbb{Z}/n$ ring of residues modulo n.

$(n) = n\mathbb{Z}$

ideal (r) can also be written as rR

$(r) = Rr$.

<u>Theorem</u> (First isomorphism theorem for rings)

If $\varphi : R \to S$ is a ring homomorphism with ker $\varphi = I$, then there is an isomorphism $R/I \to \operatorname{im}\varphi$ given by $r+I \longmapsto \varphi(r)$

<u>Proof</u> View R, S as abelian groups only $(R,+)$, $(S,+)$.

1st Isom. Theorem for groups says that

$\Phi : R/I \to \operatorname{im}\varphi$, given by $\Phi : r+I \to \varphi(r)$

is an isomorphism of abelian groups (addition $+$)

Also, Φ respects identities

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, dashed] & S \\ & \operatorname{Im}(\varphi) \arrow[u, hook, "\text{subring}"'] \end{tikzcd}$$

$\Phi(1+I) = \varphi(1) = 1$

$\Phi((r+I)(r'+I)) = \Phi(rr'+I) = \varphi(rr') = \varphi(r)\varphi(r')$

$\varphi(r)\varphi(r') = \Phi(r+I)\Phi(r'+I)$

$\Rightarrow$ mult. in R/I

$\Phi((r+I)(r'+I)) = \Phi(r+I)\Phi(r'+I)$

cosets

mult. in $\operatorname{im}(\varphi) \subset S$

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\text{quotient map}"'] & S \\ R/I \arrow[r, "\Phi"] & \operatorname{im}(\varphi) \arrow[u, hook] \end{tikzcd}$$

isomorphic as abelian groups, Φ an isomorphism, $\Phi(1+I) = 1$

r, r' in R

$r+I$, $r'+I$ cosets multiply, apply Φ $\longrightarrow$ $\Phi((r+I)(r'+I))$

or

apply φ, then multiply. $\Phi(r+I)\Phi(r'+I)$

Φ bijective, respects $+$, $\cdot$, takes 1 to 1 $\Rightarrow$

Φ is an isomorphism $R/I \simeq \operatorname{Im}(\varphi)$

$R \to R[x]$ polynomials in x, coefficients in R

$R[x_1, \dots x_n]$ polynomials in $x_1, \dots, x_n$

$R[x_1, \dots x_n] = R[x_1 \dots x_{n-1}][x_n]$

$R[x_1, x_2]$ elements

$$a_{00} + a_{10} x_1 + a_{01} x_2 + a_{20} x_1^2 + a_{11} x_1 x_2 + a_{02} x_2^2 + \dots$$

<u>Example</u> $R = \mathbb{Z}$, $\mathbb{Z}[x_1, x_2] = \mathbb{Z}[x_1][x_2] \simeq \mathbb{Z}[x_2][x_1]$

$$f(x_1, x_2) = 2 - 7x_1 + 4x_2 + x_1^2 + 3x_1 x_2 - x_1^3 + x_1^2 x_2^2 - 2x_1 x_2^3 =$$

$$= \underbrace{(2 - 7x_1 + x_1^2 - x_1^3)}_{\in \mathbb{Z}[x_1]} + \underbrace{(4 + 3x_1)}_{\in \mathbb{Z}[x_1]} x_2 + \underbrace{(x_1^2)}_{\in \mathbb{Z}[x_1]} x_2^2 \underbrace{- 2x_1}_{\in \mathbb{Z}[x_1]} x_2^3 =$$

$$= \underbrace{(2 + 4x_2)}_{\in \mathbb{Z}[x_2]} + \underbrace{(-7 + 3x_2 - 2x_2^3)}_{\in \mathbb{Z}[x_2]} x_1 + \underbrace{(1 + x_2^2)}_{\in \mathbb{Z}[x_2]} x_1^2 + \underbrace{(-1)}_{\in \mathbb{Z}[x_2]} x_1^3$$

Evaluation homomorphism   pick R and $r \in R$

$R \longrightarrow R[x]$
inclusion homomorphism
$a \longmapsto a$
$\underset{R}{\uparrow}$ $\uparrow$ constant polynomial

$R[x] \xrightarrow{ev_r} R$

evaluate polynomial $f(x)$ by substituting r in place of x

$f(x) \longmapsto f(r)$

$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ a polynomial (element of $R[x]$) Before

$f(r) = a_0 + a_1 r + a_2 r^2 + \cdots + a_n r^n \in R$ a "number" (element of R) After

Prop ev_r is a homomorphism.

Proof 1) ev_r is a homomorphism of abelian groups

$ev_r(f(x)+g(x)) = f(r)+g(r) = ev_r(f(x)) + ev_r(g(x))$

$ev_r(0)=0$ $ev_r(-f(x)) = -ev_r(f(x))$

2) $ev_r(f(x)g(x)) = f(r)g(r) = ev_r(f(x))\, ev_r(g(x))$

3) $ev_r(1)=1$ $\square$.

Example $R=\mathbb{Z}$ $f(x) = 2-4x+x^3$, $r=5$
$\underset{\mathbb{Z}[x]}{\uparrow}$ $f(5) = 2-4\cdot 5+5^3 = 107 \in \mathbb{Z}$

Question: Is ev_r surjective? Yes!

In fact, ev_r is the identity homomorphism when restricted to R

$R \longrightarrow R$
$a \longmapsto a$
constant polynomials

what is $\ker(ev_r)$? polynomials $f(x)$ such that $ev_r(f(x))=0$
$f(r)=0$. for instance $x-r$
$ev_r(x-r) = r-r = 0$. Also any polynomial $(x-r)g(x)$. Soon will see that $\ker(ev_r) = (x-r)$ ← principal ideal.

Examples a) $r=0$ $\quad R[x] \xrightarrow{ev_0} R$

$f(x) \mapsto f(0)$ constant term

$a_0+a_1x+\dots+a_nx^n \mapsto a_0$ $\quad \ker(ev_0)=(x)$

b) $r=1$ $\quad R[x] \xrightarrow{ev_1} R$

$f(x) \longmapsto f(1)=a_0+a_1+\dots+a_n$ sum of coefficients

$\ker(ev_1)=(x-1)$

c) $r=-1$ $\quad f(x) \mapsto a_0-a_1+a_2+\dots \underset{\substack{\uparrow \\ +(-1)^n a_n}}{\pm a_n}$ alternating sum of coefficients

$\ker(ev_{-1})=(x+1)$

Thm $\quad ev_r : R[x] \to R \quad f(x) \mapsto f(r) \quad r \in R$

is a homomorphism.

$\ker(ev_r)=(x-r)$ principal ideal generated by polynomial $x-r$, consists of polynomials $(x-r)f(x)$, $f(x) \in R(x)$.