Def 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) $a \in I, r \in R \Rightarrow ra \in I$

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

lecture 4, Sept. 21

work with commutative rings only

$\Rightarrow ra = ar$

↑ Reminder

$I \subset R$ is called a proper ideal if $I \neq R$

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

Prop 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 principal ideal generated by a. $Ra = (a)$.

↑ notation

Exercise $Ra = (a)$ is an ideal.

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

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

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

Thm $(a_1, \dots, a_n)$ is an ideal of R

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

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

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

Complete the proof

$\alpha: R \longrightarrow S$ homomorphism of rngs

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

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

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

$\alpha(1) = 1$ identity.

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

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

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

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

$= 0 \in S$

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, $r \in I$. $\Rightarrow r^{-1} \cdot r \in I \Rightarrow 1 \in I$

$\Rightarrow a \in I \ \forall a \in F$ a·1 ∎.

Corollary Any homomorphism $F \xrightarrow{\alpha} R$ of a field F into a rng R is injective

$\alpha(1) = 1 \in R \Rightarrow \ker(\alpha) \neq F \Rightarrow \ker(\alpha) = 0 \Rightarrow \alpha$ injective (except on $R = \{0\}$)

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 rng, $(2) = 2\mathbb{Z}$, $(3) = 3\mathbb{Z}$, ...

(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.

$\alpha: R \longrightarrow S$

$\cup$ $\quad$ $\cup$

$\ker(\alpha)$ $\quad$ $\mathrm{im}(\alpha)$

ideal $\quad$ subring.

want to say that subring $\mathrm{Im}(\alpha)$ is the quotient of R by ideal $\ker(\alpha)$, since elements of $\mathrm{Im}(\alpha)$ are sets $r + \ker(\alpha)$

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 sets 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? check $0 + I = I$

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

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

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

$\pi(r) = r + I$. 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 $ss' + I = rr' + I$ $\quad$ $(s+I)(s'+I) = ss' + I$

$$rr' - ss' = (rr' - rs') + (rs' - ss') = r(r' - s') + (r - s)s'$$

($r - s \in I$, $r' - s' \in I$)

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

Indeed, multiplication is well-defined.

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

Proof: (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 $\big((a+I)(b+I)\big)(c+I) = (ab+I)(c+I) = (ab)c + I$

$$(ab)c + I = abc + I = a(bc) + I$$

$$(a+I)\big((b+I)(c+I)\big) = (a+I)(bc+I) = a(bc)+I$$

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

Thm 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.

Example $I = (n) \subset \mathbb{Z}$.

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

$(r) = Rr$.

Theorem (First isomorphism theorem for rings)

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

Proof View R, S as abelian groups only $(R,+)$, $(S,+)$.

1st Isom Theorem for groups says that

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

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

Also, Φ respects identities

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

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

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

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

(mult. in R/I on the left; mult. in $\operatorname{im}(\varphi) \subset S$ on the right)

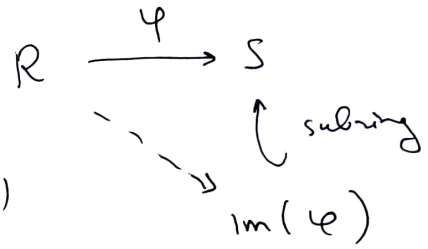
$r+I$, $r'+I$ cosets

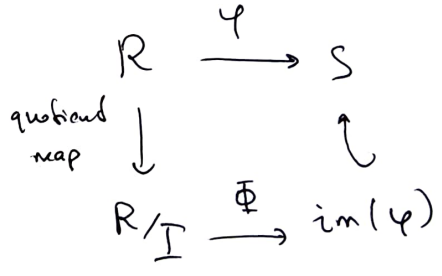
r, r' in R

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

or

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





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

Φ bijective, respects $+$, $\cdot$, takes 1 to 1 $\Rightarrow$ Φ is an isomorphism $R/I \cong \operatorname{im}(\varphi)$

$R \to R[x]$ 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

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

Example $R = \mathbb{Z}$, $\mathbb{Z}[x_1, x_2] = \mathbb{Z}[x_1][x_2] \simeq \mathbb{Z}[x_2][x_1]$

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

$$= \underset{\uparrow}{(2 - 7x_1 + x_1^2 - x_1^3)} + \underset{\uparrow}{(4 + 3x_1) x_2} + \underset{\uparrow}{(x_1^2) x_2^2} \underbrace{- 2x_1 x_2^3}_{\uparrow} =$$

$\mathbb{Z}[x_1]$ $\quad$ $\mathbb{Z}[x_1]$ $\quad$ $\mathbb{Z}[x_1]$ $\quad$ $\mathbb{Z}[x_1]$

$$= \underset{\uparrow}{(2 + 4x_2)} + \underset{\uparrow}{(-7 + 3x_2 - 2x_2^3) x_1} + \underset{\uparrow}{(1 + x_2^2) x_1^2} + \underset{\uparrow}{(-1) x_1^3}$$

$\mathbb{Z}[x_2]$ $\quad$ $\mathbb{Z}[x_2]$ $\quad$ $\mathbb{Z}[x_2]$ $\quad$ $\mathbb{Z}[x_2]$

Evaluation homomorphism pick R and $r \in R$

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

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

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

$R \to R[x]$ inclusion homomorphism $a \mapsto a$ (R → constant polynomial)

Before

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

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

After

Prop ev_r is a homomorphism.

Proof 1) ev_r is a homomorphism of abelian groups

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

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

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

3) $ev_r(1)=1$ □

Example $R=\mathbb{Z}$ $f(x) = 2-4x+x^3$, $r=5$

$\mathbb{Z}[x]$ $\qquad f(5) = 2-4\cdot 5+5^3 = 107 \in \mathbb{Z}$

Question: Is ev_r surjective? Yes!

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

$R \to R$ $\qquad$ what is $\ker(ev_r)$? polynomials $f(x)$

$a \mapsto a$ $\qquad$ such that $ev_r(f(x)) = 0$

constant polynomials $\qquad f(r)=0$. 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) $r=0$ $\quad R[x] \xrightarrow{ev_0} R$

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

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

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) $r=-1$ $\quad f(x) \longmapsto a_0-a_1+a_2+\dots \pm a_n$ alternating sum of coefficients

$\pm a_n$

$\uparrow$

$+(-1)^n a_n$

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

Thm $\quad ev_r : R[x] \longrightarrow R \qquad f(x) \longmapsto f(r) \qquad r \in R$

is a homomorphism.

$\ker(ev_r) = (x-r)$

principal ideal generated by polynomial $x-r$,

consists of polynomials

$(x-r)f(x)$, $f(x) \in R(x)$