Groups & Rings: Lecture #16

Homomorphisms & ideals

- Homomorphisms
- Kernel & image
- Ideals
- Ideals of $\mathbb{Z}$ ($\mathbb{Z}$ is a PID)
- Quotient rings
- Isomorphism theorems.

Ring homomorphisms

Def: Let R, S be rings. A ring homomorphism is a map $\phi: R \to S$ s.th.

(i) $\phi(r+s) = \phi(r) + \phi(s)$ $\Rightarrow \phi(0) = 0$

(ii) $\phi(rs) = \phi(r)\phi(s)$ $(\Rightarrow \phi(1) = \phi(1)\phi(1) \not\Rightarrow \phi(1)=1)$

$\boxed{\text{(iii)} \quad \phi(1_R) = 1_S}$ Book does not require this. (only makes sense if R, S have unities)

Def: A ring isomorphism is a bijective ring homo.

Rmk: If $\phi: R \to S$ is a ring iso $\Rightarrow$ $\phi^{-1}: S \to R$ is a ring iso

(pf: $\phi^{-1}(xy) = \phi^{-1}(\phi(r)\phi(s)) = \phi^{-1}(\phi(rs)) = rs = \phi^{-1}(x)\phi^{-1}(y)$)

Def: R, S are rings. The cartesian product is the ring

$R \times S = \{(r,s) : r \in R, s \in S\}$ $\quad (r,s) + (r',s') = (r+r', s+s')$

$(r,s)(r',s') = (rr', ss')$

Ex: (Gaussian integers)

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \cong \mathbb{Z} \times \mathbb{Z}$

$= \{(a,b) : a, b \in \mathbb{Z}\}$ as a group, not as rings

Mult. is not componentwise: $i^2 = -1$

$(a+bi)(c+di) = (ac - bd) + (ad + bc)i$

$(a,b)(c,d) = (ac-bd, \ ad+bc)$

Add is componentwise though:

$(a,b) + (c,d) = (a+c, b+d)$

Ex: Ring homo $\mathbb{Z}[i] \longrightarrow \mathbb{C}$. ker $= 0$

$$a+bi \longmapsto a+bi$$

Ex: Ring homo $\mathbb{C} \xrightarrow{\phi} M_2(\mathbb{R})$ ker $= 0$

$$a+bi \longmapsto \begin{pmatrix} \boxed{\begin{matrix} a \\ b \end{matrix}} & \boxed{\begin{matrix} -b \\ a \end{matrix}} \end{pmatrix} = \text{matrix of mult by } a+bi = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$$

$$(a+bi)\cdot 1 = (a+bi)$$

$$(a+bi)\cdot i = (-b+ai)$$

Exc: ϕ is a homo because of how it is defined (ass. of mult of cplx numbers)

Verify this explicitly

$$\phi((a+bi)+(c+di)) = \phi(a+bi) + \phi(c+di)$$

matrix add.

and sim for $\cdot$.

$$\phi(1) = I$$

Ex: $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/n\mathbb{Z}$ $\ker(\phi) = n\mathbb{Z}$

$a \longmapsto a + n\mathbb{Z}$ $\mathrm{im}(\phi) = \mathbb{Z}/n\mathbb{Z}$ (surj)

Ex: $C([0,1], \mathbb{R}) \xrightarrow{ev_a} \mathbb{R}$ evaluation at point $x=a$.

$$f \longmapsto f(a)$$

This is a ring homo since add + mult in $C(\cdots)$ is pointwise.

$$(f+g)(a) = f(a)+g(a) \quad \ldots$$

$$\ker(ev_a) = \{f : f(a) = 0\}$$

$$\mathrm{im}(ev_a) = \mathbb{R} \quad \text{(surj)}$$

Kernels and images

Let $\phi: R \to S$ homo of rings.

Def: The kernel of ϕ is $\phi^{-1}(0)$. (an ideal)
The image of ϕ is $\phi(R)$ (a subring of S)

$\phi(r_1)+\phi(r_2)=\phi(r_1+r_2)$
$\phi(r_1)\phi(r_2)=\phi(r_1r_2)$
so $\phi(R)$ closed under $+$ and $\cdot$

Properties: (i) If R is commutative
$\Rightarrow \phi(R)$ is commutative
(ii) If R is a field and $S \neq 0$
$\Rightarrow \phi(S)$ is a field

if $\phi(1_R)=1_S$

pf (ii): $\phi(r)\neq 0 \Rightarrow r\neq 0 \Rightarrow \exists r^{-1}\in R$
$\phi(r)\phi(r^{-1})=\phi(rr^{-1})=\phi(1_R)=1_S \Rightarrow \phi(r)^{-1}=\phi(r^{-1})$

Rmk: From $\uparrow$ we see that (ass. $\phi(1_R)=1_S$):
if $r\in R$ invertible $\Rightarrow \phi(r)$ is invertible.

Q: What about zerodivisors? If $xy=0$ in R
$\Rightarrow \phi(x)\phi(y)=0$ in S

Even if $x\neq 0$, $y\neq 0$, then perhaps $\phi(x)$ or $\phi(y)$ is zero?

4 zerodiv $\longmapsto$ 4 invertible $\Rightarrow$ not zerodiv.

Ex: $\mathbb{Z}/10\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/5\mathbb{Z}$ (well-defined b/c $5|10$)
$x+10\mathbb{Z} \longmapsto x+5\mathbb{Z}$
$4\cdot 5=0 \longmapsto 4\cdot 0=0$

Exc: Are the following rings isomorphic? (subrings of $\mathbb{C}$)

(a) $\mathbb{R}$ vs $\mathbb{C}$ (no!)

(b) $\mathbb{Z}[\sqrt{2}]$ vs $\mathbb{Z}[\sqrt{3}]$ (no!)

(c) $\mathbb{Z}[\pi]$ vs $\mathbb{Z}[e]$ (yes!)

Either find an iso or show that $\nexists$ iso.

(a) What distinguishes $\mathbb{R}$ and $\mathbb{C}$? (isomorphic as sets and also as grps)

$\exists i \in \mathbb{C} : i^2 = -1$ $\qquad \nexists x \in \mathbb{R} : x^2 = -1$ b/c $x^2 \geq 0$

If $\exists \phi : \mathbb{R} \xrightarrow[\text{homo}]{\text{bij}} \mathbb{C}$ $\Rightarrow \phi(x^2) \Rightarrow \phi(x)\phi(x) = i \cdot i = -1 = \phi(-1)$

$x \longmapsto i$ $\qquad \Rightarrow x^2 = -1$

(or argue w/ $\phi : \mathbb{C} \xrightarrow{\cong} \mathbb{R}$)

(b) $\mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}[\sqrt{3}] \cong \mathbb{Z} \times \mathbb{Z}$ as abelian groups

$x : x^2 = 2 \qquad y : y^2 = 3$

$\phi(1+1) = \phi(1) + \phi(1)$

$\phi : \mathbb{Z}[\sqrt{2}] \xrightarrow{\text{homo}} \mathbb{Z}[\sqrt{3}]$ $\qquad \alpha \cdot \alpha = \phi(x)\phi(x) = \phi(x^2) = \phi(2) = 2$

$x \longmapsto \alpha$ $\qquad \alpha = \phi(x)$ has square 2

$x = 0 + 1\sqrt{2}$ $\qquad$ i.e. α square root of 2.

$\alpha = a + b\sqrt{3} \qquad \alpha^2 = \underbrace{a^2}_{\in \mathbb{Z}} + \underbrace{2ab}_{\in \mathbb{Z}}\sqrt{3} + \underbrace{3b^2}_{\in \mathbb{Z}} \neq 2$

(c) $\mathbb{Z}[\pi]$ vs $\mathbb{Z}[e]$ (π and e are transcendental numbers: no alg rel.)

$\mathbb{Z}[\pi]$ = smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and π : $\quad 1, \pi, \pi^2, \pi^3, \ldots$ "lin indep"

$= \left\{ \sum_{i=0}^{n} a_i \pi^i : \text{ some } n \in \mathbb{N},\ a_i \in \mathbb{Z} \right\} \cong \mathbb{Z}[x] \cong \mathbb{Z}[e]$. So $\mathbb{Z}[\pi] \cong \mathbb{Z}[e]$

pol. ring $\qquad \sum a_i \pi^i \mapsto \sum a_i e^i$

Ideals

Def: An ideal I of a ring R is a subset $I \subseteq R$ s.th.

(i) $I \subset R$ subgroup ($i+j \in I$ $\forall i,j \in I$)

(ii) $ri \in I$, $ir \in I$ $\forall r \in R$, $i \in I$. (more than $ij \in I$ $\forall i,j \in I$)

(equiv if R is comm)

Prop (16.27): $\phi : R \to S$ ring hom $\Rightarrow$ $\ker\phi$ is an ideal

pf: $\ker\phi$ is a (normal) subgroup (group theory)

$i \in \ker\phi$, $r \in R$, $\phi(ri) = \phi(r)\phi(i) = \phi(r)\cdot 0 = 0$

$\phi(ir) = \phi(i)\phi(r) = 0 \cdot \phi(r) = 0$ $\square$

(The book mentions that ideals are subrings but usually $1_R \notin I$ so I not subring w/ identity and of very different flavor.)

Ex: $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/10\mathbb{Z}$, $\ker\phi = 10\mathbb{Z} = \{\ldots, -10, 0, 10, \ldots\}$

$= (10) =$ all mult. of 10.

Def: • Let $a \in R$. Then $(a) := \{ar : r \in R\} \subset R$ is an ideal called a principal ideal (book uses notation $\langle a \rangle$)

• The trivial ideal is the principal ideal $(0) = \{0\} \subset R$.

• The improper ideal is the whole ring R. If $\exists 1_R$, $R = (1)$.

(called trivial by book)

Rmk: (a) is the smallest ideal containing a.

Rmk: Similar notation $(a_1, \ldots, a_n)$ smallest ideal containing $a_1, \ldots, a_n \in R$.

Ideals of $\mathbb{Z}$

Thm (16.25): Every ideal of $\mathbb{Z}$ is principal. ($\mathbb{Z}$ is a principal ideal domain)

pf: Let $I \subseteq \mathbb{Z}$ some ideal. Pick $a \in I$ positive >0 smallest possible. Claim: $I = (a)$.

Pick $b \in I$. (If b not mult of a, then $\gcd(a,b) < a$. The Euclidean algorithm can be used to find gcd. We will argue similarly.)

Division algo:

$$b = q\underbrace{a}_{\in I} + r \quad \text{for unique } q \in \mathbb{Z} \text{ and } 0 \le r \le a-1.$$

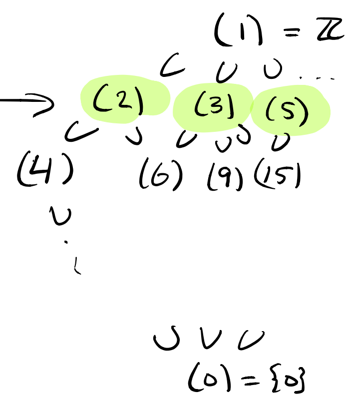
$b \in I$, $qa \in I \Rightarrow qa \in I$

$\Rightarrow r \in I$. But $r < a$ and a is minimal positive $\Rightarrow r = 0$.

$\Rightarrow b = qa \in (a)$ $\square$

Picture of $\mathbb{Z}$:

maximal ideals $\longrightarrow$



$(a) \subseteq (b)$

$\Updownarrow$

$b \mid a$

Def: A maximal ideal is a proper ideal ($I \subsetneq R$) which is maximal among such.

(That is, an ideal $I \subseteq R$ is maximal if $I \neq R$ and $\nexists\, I \subsetneq \underset{\text{ideal}}{J} \subsetneq R$)

Rmk: $(n) \subseteq \mathbb{Z}$ maximal $\Longleftrightarrow$ $n = \pm p$ p prime number.

Quotient rings

Thm (16.29) Let $I \subseteq R$ be an ideal. Then the quotient group R/I is a ring w/ multiplication

$$(r+I)(s+I) = rs + I$$

pf: Mult. is welldefined:

$$r + I = r' + I \iff r' = r + i \qquad i \in I$$
$$s + I = s' + I \iff s' = s + j \qquad j \in I$$

$$r's' + I = (r+i)(s+j) + I = rs + \underbrace{is}_{\in I} + \underbrace{rj}_{\in I} + \underbrace{ij}_{\in I} + I$$
$$= rs + I$$

Exc: Verify that mult is ass & dist. Also if $\exists 1_R$ then $1_{R/I} = 1 + I$. $\square$

Thm (16.30) The canonical homomorphism (or quotient homomorphism)

$$R \longrightarrow R/I \quad \text{is a surjective ring homo, w/ kernel } I.$$
$$r \longmapsto r + I$$

pf: Easy exercise.

Isomorphism theorems

<u>1st isom thm</u> (16.31): Let $\phi: R \to S$ ring homo. Then $\exists$ ring isomorphism $R/\ker\phi \to \operatorname{im}\phi$.

<u>pf</u>: Ok on level grps. Verify that grp isomorp. is ring homo.

<u>2nd isom thm</u> (16.32) $\underset{\text{ideals}}{I, J} \subseteq R \Rightarrow (I+J)/J \cong I/I\cap J$

<u>3rd isom thm</u> (16.33) $\underset{\text{ideals}}{I \subseteq J} \subseteq R \Rightarrow R/J \cong (R/I)/(J/I)$

Here $J/I \subset R/I$ is the ideal $\{j + I : j \in J\} \subset R/I$.
If $q: R \to R/I$ quotient homomorphism, then $q(J) = J/I$.

<u>Correspondence theorem</u> (16.34) Fix an ideal $I \subseteq R$. Then there is a bijection of sets of ideals.

$$\{I \subseteq \underset{\text{ideal}}{J} \subseteq R\} \longleftrightarrow \{\underset{\text{ideal}}{K} \subseteq R/I\}$$
$$J \longmapsto J/I$$