April13

Monday, April 12, 2021 8:57 PM

Announcements

1) TH2 Graded

Regrade Requests by Friday.

Median: 93.5/120

2) Grades So far posted on bCourses

A	Range	85+
B	Range	75-85
C	Range	65-75
D	Range	55-65

Correction/Clarifications

1) A division ring should have $1 \neq 0$ & all $a \neq 0$ have b s.t. $ab = ba = 1$

$\rightsquigarrow \{0\}$ not a division ring or a field.

2) $1 \in R$ then $a \in R^{\times}$ if $\exists\ b$ w/ $ab = ba = 1$

(I wrote $ab = 1$)

Example In (2) need both directions.

Let $V = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \cdots$

∞-dimensional real vector space.

$$A = \{\phi : V \longrightarrow V : \phi \text{ is linear}\}.$$

Ring

$$\left.\begin{aligned} (\phi+\psi)(v) &= \phi(v)+\psi(v) \\ (\phi\times\psi)(v) &= \phi(\psi(v)) \end{aligned}\right\} \text{Check } A \text{ is a ring.}$$

$$\mathcal{L} : V \longrightarrow V$$

$$\rotatebox{90}{$\in$}$$

$$(x_1, x_2, x_3, \dots) \longmapsto (x_2, x_3, x_4, \dots)$$

$$\mathcal{R} : V \longrightarrow V$$

$$(x_1, x_2, x_3, \dots) \longmapsto (0, x_1, x_2, \dots)$$

$$\mathcal{L}\circ\mathcal{R}(x_1, x_2, x_3, \dots)$$

$$\mathcal{L}(0, x_1, x_2, \dots) = (x_1, x_2, x_3, \dots)$$

So $\mathcal{L}\circ\mathcal{R} = \mathrm{id}_V$.

$$\mathcal{R}\circ\mathcal{L}(x_1, x_2, \dots) = \mathcal{R}(x_2, x_3, x_4, \dots)$$

$$= (0, x_2, x_3, x_4, \dots)$$

So $\mathcal{R}\circ\mathcal{L} \neq \mathrm{id}_V$

In fact $\boxed{\mathcal{L} \notin A^\times}$

$$\left.\begin{aligned} &\mathcal{L}(1, x_2, x_3, \dots) = \mathcal{L}(2, x_2, x_3, \dots) \\ &\text{so } \mathcal{L} \text{ not injective} \\ &\Longrightarrow \mathcal{L} \text{ has } \underline{\text{NO}} \text{ left inverse.} \end{aligned}\right\} \text{HW1 \#4}$$

Question:

* What is the right type of function between rings?

* Can we define quotients?

↳ Expectation should be yes.

$\mathbb{Z}/n\mathbb{Z}$ know is a quotient group.
Inherits multiplication from $\mathbb{Z}$.
Should be a quotient ring.

Def^n

Let R, S be rings

① A ring homomorphism $\phi: R \longrightarrow S$ is a function satisfying.

i) $\phi(a+b) = \phi(a) + \phi(b)$

(ϕ is a group homomorphism on underlying abelian groups).

ii) $\phi(ab) = \phi(a)\phi(b)$

② The kernel of ϕ is

$$\ker\phi = \{r \in R : \phi(r) = 0\}$$

(kernel is the same kernel as the underlying homorphism of abelian groups).

③ If ϕ is a bijective ring homomorphism it is called a ring isomorphism.

Examples & nonexamples

i) $\pi: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$$

$$\pi(ab) = \overline{ab} = \bar{a}\,\bar{b} = \pi(a)\pi(b)$$

✓

$\ker \pi = n\mathbb{Z}$. = multiples of n.

↑ (nonunital) subring of $\mathbb{Z}$.

2) Nonexample

$n \in \mathbb{Z}$.

$$\begin{array}{rccc} M_n : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & nx \end{array} \qquad \left(\begin{array}{l} n(x+y) \\ = nx+ny \end{array} \right)$$

This is a group homomorphism.

But $M_n(x) \cdot M_n(y) = nx\,ny = n^2xy$

$$M_n(xy) = nxy.$$

In particular
$$\left.\begin{array}{l} M_n(1)\cdot M_n(1) = n^2 \\ M_n(1.1) = n \end{array}\right\}$$

M_n is a ring homomorphism $\iff n = 0, 1$

3) Nonexamples

$$\begin{array}{rccc} \text{Norm} : & \mathbb{Q}(\sqrt{D}) & \longrightarrow & \mathbb{Q} \\ & a+b\sqrt{D} & \longmapsto & a^2 - b^2D \end{array}$$

Is multiplicative

Not additive

$$N(a+b) = a^2 + 2ab + b^2$$

$$N(a) + N(b) = a^2 + b^2$$

4) $\varepsilon_0 : \mathbb{Q}[x] \longrightarrow \mathbb{Q}$ evaluation @ 0

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

$$\varepsilon_0(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) = a_0$$

$$\begin{tikzcd}
(a_0+a_1x+\dots) \arrow[d, mapsto, "\varepsilon_0"'] & + & (b_0+b_1x+\dots) \arrow[d, mapsto] & = & a_0+b_0+(a_1+b_1)x+\dots \arrow[d, mapsto] \\
a_0 & + & b_0 & = & a_0+b_0
\end{tikzcd}$$

$$\begin{tikzcd}
(a_0+a_1x+\dots) \arrow[d, mapsto] & (b_0+b_1x+\dots) \arrow[d, mapsto] & = & a_0b_0+(a_1b_0+a_0b_1)x+\dots \arrow[d, mapsto] \\
a_0 \cdot & b_0 & = & a_0b_0
\end{tikzcd}$$

$\ker \varepsilon_0 = \{a_1x + a_2x^2 + \dots + a_nx^n\}$

$=$ "multiples of x" $\Big\}$ (nonunital!) subring of $\mathbb{Q}[x]$.

Observations about kernels

1) $a \in n\mathbb{Z} = \ker \pi$

$b \in \mathbb{Z}$ $\Longrightarrow$ $ab \in n\mathbb{Z}$

Pf $a = n \cdot a'$

$\Longrightarrow ab = na'b$

2) $f \in \ker \mathcal{E}_0$, $g \in \mathbb{Q}[x]$. $\Longrightarrow$ $fg \in \ker \mathcal{E}_0$

Pf/ i) $f = xf'$

so $fg = x(f'g)$

$\uparrow$ constant term 0.

2) $(fg)(0)$

$= f(0) \cdot g(0)$

$= 0 \cdot g(0)$

$= 0$

so $fg \in \ker \mathcal{E}_0$.

Rmk In both cases, these kernels are subrings in a strong way.

Prop (✱) Let R, S be rings. $\phi : R \to S$ a ring homomorphism.

① $\operatorname{im}\phi$ is a subring of S.

② $\ker\phi$ is a subring of R.

③ If $a \in \ker\phi$ and $b \in R$, then

$ab \in \ker\phi$

$ba \in \ker\phi$

Pf/ Exercise.

Rmk $\ker\phi$ & $\operatorname{im}\phi$ are additive subgroups of R & S respectively.

(by HW3 #2).

Quotient Rings

Recall

Quotient Groups $\longleftrightarrow$ Images of homomorphism.

Let $\phi: R \longrightarrow S$ be a surjective ring homomorphism. $\ker\phi = I$

As groups (have F.I.T.)

as groups w/ +

$$\begin{array}{ccc} R/I & \xrightarrow{\sim} & S \\ r+I & \longmapsto & \phi(r). \end{array}$$

Bijective group homomorphism.

Can we make R/I into a ring?

$$\begin{array}{lcl} (r_1+I)+(r_2+I) & \longleftrightarrow & \phi(r_1)+\phi(r_2) \\ & & \quad \| \\ + \quad (r_1+r_2)+I & \longleftrightarrow & \phi(r_1+r_2) \end{array}$$

$$\begin{array}{lcl} (r_1+I)(r_2+I) & \overset{\longrightarrow}{\longleftrightarrow} & \phi(r_1)\phi(r_2) \\ & & \quad \| \\ \times \quad r_1r_2+I & \overset{\longrightarrow}{\longleftrightarrow} & \phi(r_1r_2) \end{array}$$

So we define + & × in R/I

$$\boxed{\begin{aligned} (\dagger)\quad (r_1+I)+(r_2+I) &= (r_1+r_2)+I \\ (r_1+I)(r_2+I) &= \underline{r_1r_2}+I \end{aligned}}$$

This makes R/I into a ring.

Pf/ well defined b/c well defined is S.

Ring b/c S is a ring.

First Isomorphism Theorem For Rings

If $\phi : R \longrightarrow S$ is a ring homomorphism with kernel I, then the rules defined in $(+)$ make R/I into a ring isomorphic to $\operatorname{im}\phi$

Recall

w/ Groups, given $H \leq G$, look at set of cosets G/H. To be a group, needed H to be normal.

Analogously

Let $K \leq R$ be an additive subgroup. Then R/K is a group!

Pf/ $(R,+)$ is abelian so $K \trianglelefteq R$)

When is R/K a ring? (under $(+)$)

Is it always a ring? NO

Pf/ If R/K a ring, then

$\pi : R \longrightarrow R/K$ is a ring homomorphism w/ kernel $= K$.

Know gp hom, kernel $= K$ by HW4

& $\pi(r_1 r_2) = r_1 r_2 + K = (r_1 + K)(r_2 + K)$

$= \pi(r_1)\pi(r_2)$.

So K is a subring in the strong way of prop $(*)$

2) See this directly.

Consider $r+K,\ s+K \in R/K$

Studying whether

$(*)$ $(r+K)(s+K) = rs+K$ is well defined.

Fix $\alpha, \beta \in K$.

$$r+K = r+\alpha+K$$
$$s+K = s+\beta+K$$

$(r+\alpha+K)(s+\beta+K) = rs + \alpha s + r\beta + \alpha\beta + K$ $(**)$

Suppose $(*)$ is well defined.

Letting $r=s=0$

Says $\alpha\beta + K = K \implies \alpha\beta \in K$

$\implies K$ subring.

Let $s=\alpha=0$

$r\beta + K = K$ so $r\beta \in K$

Similarly, $r=\beta=0$

$\implies \alpha s \in K$.

So K is strong subring in sense of $(*)$.

This motivates the following definition

Defn

R a ring. $I \leq R$ a subring.

1) I is a left ideal if $\forall\ i \in I$ and $r \in R$, $ri \in I$

2) I is a right ideal if $\forall\ i \in I$ & $r \in R$ $ir \in I$

3) I is an ideal (two sided ideal) iff it is both a left & right ideal.

Exercise

Suppose R commutative & $I \leq R$. TFAE

i) I left ideal
ii) I right ideal
iii) I ideal.

Prop

Suppose $I \leq R$. Then $(\dagger)$ gives well defined multiplication in $R/I \iff I$ is a two sided ideal.

Pf $\implies$ Already saw.

$\Longleftarrow$ To show well defined

$$rs + \underbrace{r\alpha}_{\in I} + \underbrace{\beta s}_{\in I} + \underbrace{\alpha\beta}_{\in I} + I = rs + I \quad \checkmark$$

Theorem w/ operations defined in (†)

R/I a ring $\Longleftrightarrow$ I an ideal.

Pf/ $\Longrightarrow$ Already saw

$\Longleftarrow$ Mostly done. (†) is well defined.

Check ring axioms.

$(R/I, +)$ abelian group (✓)

Remains $\times$ is associative

distributive law holds.

e.g./ $(a+I)((b+I)+(c+I)) = (a+I)(b+c+I)$

$= a(b+c) + I$

R has distributive law

$= ab+ac + I$

$= (ab+I)+(ac+I)$

$= (a+I)(b+I) + (a+I)(c+I)$ ✓

Rest Exercise.

Defn $I \subseteq R$ be an ideal.

The quotient ring R/I is the set of cosets $\{r+I : r\in R\}$ w/

$$(+)\quad \begin{aligned}(a+I)+(b+I) &= a+b+I\\ (a+I)(b+I) &= ab+I\end{aligned}$$

Theorem (First isomorphism theorem for rings)

① Let $\phi : R \longrightarrow S$ be a ring homomorphism.

Then 1) $\ker\phi \subseteq R$ an ideal $\quad\Big\}$ $(*)$

2) $\operatorname{im}\phi \subseteq S$ is a subring

$$\begin{tikzcd} R/\ker\phi \arrow[r, "\overline{\phi}"] & \operatorname{im}\phi \\ r+\ker\phi \arrow[r, mapsto] & \phi(r) \end{tikzcd}$$

is an isomorphism of rings.

② If $I \subseteq R$ is an ideal, then

$$\begin{tikzcd} \pi : R \arrow[r] & R/I \\ r \arrow[r, mapsto] & r+I \end{tikzcd}$$

is a surjective ring homomorphism w/ $\ker\pi = I$.

Pf/ $(*)$ Exercise.

$\overline{\phi}$ is a group isomorphism by the first iso thm for groups.

Only remains to check

$$\begin{array}{c}
\overline{\phi}((r_1+\ker\phi)(r_2+\ker\phi)) = \overline{\phi}(r_1 r_2 + \ker\phi) \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \\
\overline{\phi}(r_1+\ker\phi)\,\overline{\phi}(r_2+\ker\phi) = \phi(r_1)\phi(r_2) = \phi(r_1 r_2)
\end{array}$$

2) $\pi : R \longrightarrow R/I$ is a surjective group homomorphism w/ kernel I.

Check

$$\begin{array}{rcl}
\pi(r_1)\pi(r_2) & = & (r_1+I)(r_2+I) \\
 & & \quad \| \quad (\dagger) \\
\pi(r_1 r_2) & = & r_1 r_2 + I
\end{array}$$

Rmks

① Write $\bar{r}$ instead of $r+I$.

② Second, Third, & Fourth isomorphism theorems will be just as easy.

Idea: Know the theorem for groups.

Check respects ring enhancements.

Examples

1) $R, \{0\} \subseteq R$ are ideals.

$R/R \simeq \{0\}$ $\qquad$ $R/\{0\} \simeq R.$ ← First iso thm

2) $n\mathbb{Z}$ an ideal

$$r(ns) = n(rs) \in n\mathbb{Z}.$$

& $\mathbb{Z}/n\mathbb{Z}$ = ring of ints mod n.

3) $\mathbb{Z}[x]$

$$(x) = \left\{\begin{array}{l}\text{ideal of polynomials whose}\\ \text{constant term is } 0\end{array}\right\}$$

$$= \{xa_1 + x^2a_2 + \cdots\} \quad \text{in } \mathbb{Z}[x]/(x)$$

$$\overline{(a_0 + a_1x + a_2x^2 + \cdots)} = \overline{(b_0 + b_1x + b_2x^2 + \cdots)}$$

$$\iff a_0 - b_0 + (a_1 - b_1)x + \cdots \in (x)$$

$$\iff a_0 - b_0 = 0$$

$$\iff a_0 = b_0.$$

$$\frac{\mathbb{Z}[x]}{(x)} \longleftrightarrow \mathbb{Z}$$

Each coset has a unique representative that is a constant polynomial.

$$\overline{a_0 + a_1x + \cdots} = \overline{a_0}$$

$$\begin{array}{ccc}\overline{(a_0 + a_1x + \cdots)} + \overline{(b_0 + b_1x + \cdots)} & = & \overline{a_0 + b_0 + (a_1 + b_1)x + \cdots}\\ \| & & \\ \overline{a_0} + \overline{b_0} & = & \overline{a_0 + b_0}\end{array}$$

$$\begin{array}{ccccc}
\overline{(a_0+a_1x+\cdots)} & \overline{(b_0+b_1x+\cdots)} & = & \overline{a_0b_0+(a_1b_0+a_0b_1)x+\cdots} \\
\shortparallel & \shortparallel & & \shortparallel \\
\overline{a_0} \quad \cdot & \overline{b_0} & = & \overline{a_0b_0}
\end{array}$$

Looks like we just proved

$$\frac{\mathbb{Z}[x]}{(x)} \simeq \mathbb{Z}.$$

We can give a slicker proof

Pf/

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "\varepsilon_0"] & \mathbb{Z} \\
f(x) \arrow[r, mapsto] & f(0)
\end{tikzcd}$$

Saw $\ker(\varepsilon_0) = (x)$

F.I.T. $\Longrightarrow \dfrac{\mathbb{Z}[x]}{(x)} \simeq \mathbb{Z}.$

Rmk Similar proof

$$\frac{R[x]}{(x)} \simeq R.$$

R is a subring & a quotient of $R[x]$