15th abstract algebra

2022年3月5日 星期六　　上午10:06

Isomorphism theorem. Let $\phi: R \to S$ be a homomorphism of rings. Suppose that ϕ is onto and let I be the kernel of ϕ. Then

$$S \text{ is isomorphic to } R/I.$$

Definition: Let R be a ring, we say that $u \in R$ is a unit, if u has a multiplicative inverse.

lemma Let I be the ideal of a ring R. If I contains a unit, then $I = R$.

Proof: Suppose $u \in I$ is a unit of R

ideal

$\underset{R}{\underline{v}} \cdot \underset{I}{\underline{u}} = \underset{\in I}{1}$ for some $v \in R$

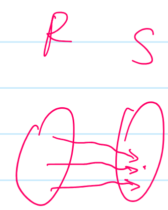
$1 = vu \in I$

Pick $a \in R$ $\qquad \underset{R}{\underline{a}} \cdot \underset{I}{\underline{1}} = \underset{\in I}{a} \in I \Rightarrow I = R$ $\qquad \square$.

Proposition: Let R be a division ring. ⊇ field
Then the only ideals of R are the zero ideal and the whole of R.
In particular if $\phi: R \to S$ is any ring homomorphism, then ϕ is injective.

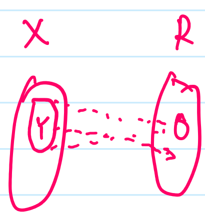
proof: Let I be an ideal not equal to $\{0\}$
pick $u \in I$ $u \neq 0$. As R is a division ring, u is a unit.

$$I = R.$$



$\phi: R \to S$ be a ring. homomorphism. let I be the kernel.
I cannot be the whole of R $\qquad I = \{0\}$. ϕ is injective. $\square$.

Example: X: set $\qquad X \xrightarrow{F} R \qquad F$: ring
R. ring



$Y \subseteq X$

I: functions from X to R whose restriction to Y is zero ✓.
I is the ideal of R.

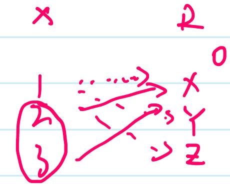
I is the ideal of R.

non-empty: zero function

$f, g \in I$. $\quad f+g \in I$. $\quad f \in I \quad g \in F$.

$f(Y) = g(Y) = 0 \quad f(Y)+g(Y)=0 \quad \underbrace{g(Y)}\cdot \underbrace{f(Y)}_{0} = 0 \quad gf \in I$

consider F/I

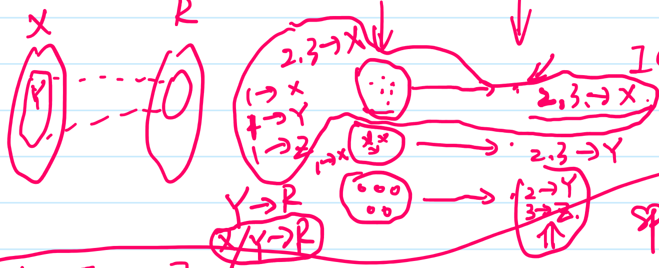


ϕ: $f \to f|_Y$ - kernel is I

$G: Y \to R \leftarrow$

$F: X \to R$

function $f \in F$ $\quad f|_Y \in G$ $\cong$ surjective ? ✓



Isomorphism theorem: G is isomophic to F/I.

space of maps is a copy of $\mathbb{R}$.

$X: [0,1]$

$R: \mathbb{R}$

$Y = \{\frac{1}{2}\}$

$G: \{\frac{1}{2}\} \to \mathbb{R}$

$F: [0,1] \to \mathbb{R}$. $\quad G$ is isomphic to F/I

$I: \{\frac{1}{2}\} \to 0 \quad I = F$.

$[0,1] \to \mathbb{R}$.

Example: Gaussian integers. R: $a+bi$.

$I \subseteq R \quad I$ is an ideal of R ? $\quad a+bi \in I \quad c+di \in I$

$2|a$

$2|b$

$(a+bi)+(c+di) = \underline{a+c} + (\underline{b+d})i \in I$.

closed under addition.

multiplication

a, b: even numbers

$a+bi \in I$

$c+di \in R$

$(c+di)(a+bi) = ac - bd + (ad+bc)i \cdot \in I$

$ac - bd$ even number

$ad + bc$ even number

I is an ideal.

Field of fractions.

$Q \Leftarrow Z$ integral $\quad \dfrac{a \to \text{integers}}{b \to \text{integers.}}$ $\quad \dfrac{a}{b} = \dfrac{ka}{kb} = \dfrac{c}{d} [a, b]$

$\mathbb{Q} \Leftarrow \mathbb{Z}$ integral domain. $\frac{a}{b} \to$ integers

rational numbers, integers.

$\frac{a}{b} = \frac{ka}{kb} = \frac{c}{d}$ $[a, b]$

equivalence classes. $[a, b]$.

$[a,b]$ and $[c,d]$ are equivalent iff $ad = bc$.

Given an arbitrary integral domain R. we have the same operation.

Definition/Lemma: Let R be any integral domain. Let N be the subset of $R \times R$ such that the second coordinate is non-zero.

Define an equivalence relation $\sim$ on N as follows.

$$(a, b) \sim (c, d) \quad \text{iff} \quad ad = bc.$$

Proof. reflexive. symmetry. transitivity

1) $(a, b) \in N$ $\quad (a, b) \sim (a, b) \Leftrightarrow ab = ab$ ✓

2) $(a, b) \sim (c, d)$

$ad = bc$.

$cb = da$. R is commutative. $\Rightarrow (c, d) \sim (a, b)$

$bc = cb$

$ad = da$

3) (a, b). (c, d). $(e, f) \in N$.

$(a, b) \sim (c, d)$ $\quad ad \overset{①}{=} bc$

$(c, d) \sim (e, f)$ $\quad cf \overset{②}{=} de$.

$$(af) \cdot d \overset{com}{=} (ad)f \overset{①}{=} (bc)f \overset{ass}{=} b(cf) \overset{②}{=} b(de) \overset{com}{=} b(ed) \overset{ass}{=} (be)d.$$

$c, d \in N$. $d \neq 0$. $\Rightarrow af = be$.

$(a, b) \sim (e, f)$ $\square$

Definition/Lemma: The field of fractions of R. denoted by F is a set of equivalence classes, under the equivalence relation defined above.

lemma equivalence classes, under the equivalence relation defined above.

Given two elements $[a,b]$ and $[c,d]$ define.

$$\begin{cases} [a,b]+[c,d] = [ad+bc, bd]. & \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}. \\ [a,b]\cdot[c,d] = [ac, bd] & \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd} \end{cases}$$

With these rules of $+$, $\cdot$ F becomes a field.

Moreover, there is a natural injective ring homomorphism.

$$\phi: R \to F.$$

so that we may identity R as a subring of F.

Proof: well-defined. $+$ $\cdot$ $[a,b]=[a',b']$ $ab'=a'b$ $[c,d]=[c',d']$ $cd'=c'd.$ $\Rightarrow \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$ skip.

F is a ring under addition and multiplication

0: $[0,1]$ $\frac{0}{1}=0.$

1: $[1,1]$. $\frac{1}{1}=1$

field: $[a,b]$ $a\neq 0.$ inverse: $[b,a]$

$\frac{a}{b}\cdot ?\frac{b}{a}=\frac{1}{1}$

R is integral domain

$\frac{a}{b}\cdot\frac{c}{d}=\frac{c}{d}\cdot\frac{a}{b}.$ commutative.

$\phi: R\to F.$ injective ring homomorphism.

$\phi(a)=[a,1]$

$a \to \frac{a}{1} \sim \frac{2a}{2}$ $\mathbb{Q}\to\mathbb{Q}$

$a+bi$

Example: $\mathbb{Q} \Rightarrow \mathbb{Z}$ $\mathbb{C}\Rightarrow \mathbb{Q}$

F R F R

$R=K[x]$ K is a field.

field of fractions: $K(x)$. $F. = \frac{f(x)}{g(x)}$ coefficients of $f, g \in K$.

12. Mar. 2022
4 pm.