# 14th abstract algebra

2022年2月26日 星期六 上午10:08

**Definition:** Let $R$ be a ring. We say that $R$ is commutative if multiplication is commutative. $a \cdot b = b \cdot a$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \neq \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

**Definition:** Let $R$ be a ring. We say that $R$ is boolean if for every $a \in R$. $a^2 = a$.

lemma

Every boolean ring is commutative.

**Proof:**

$$\begin{aligned} a+b &= (a+b)^2 \\ &= a^2 + ab + ba + b^2 \\ a+b &= a + ab + ba + b \\ b &= ab + ba + b \\ 0 &= ab + ba \\ ab &= -ba. \end{aligned}$$

$a \in R$, $b \in R$

let $b = 1$ $a = a \cdot 1 = -\cdot 1 \cdot a = -a$

similarly: $-b = b$.

$-(ba) = (-b) \cdot a = ba.$

$ab = ba$ $\square$

**Definition:** Let $R$ be a ring. We say that $R$ is a division ring if $R - \{0\}$ is a group under multiplication.

If the division ring is commutative, we say that $R$ is a field.

a ring is a division ring iff every non-zero element has a multiplicative inverse.

example: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. subfields.

$\mathbb{Z}$ is not a field. $2 \cdot _$

subring of a division ring is a domain.

lemma. The quaternions are a division ring.

proof: we only prove that every non-zero number has a multiplicative inverse.

let $q = a + bi + cj + dk$ $\qquad q\bar{q} = a^2+b^2+c^2+d^2 \neq 0$ iff $q \neq 0$

$\bar{q} = a - bi - cj - dk$.

conjugate.

$$\frac{q \cdot \bar{q}}{a^2+b^2+c^2+d^2} = 1 \Rightarrow q \cdot \frac{\bar{q}}{a^2+b^2+c^2+d^2} = 1$$

$p = \dfrac{\bar{q}}{a^2+b^2+c^2+d^2}$ is the multiplicative inverse of $q$. $\square$

**Definition lemma.** Let $R$ be a ring. We say that $a \in R$ $a \neq 0$ is a zero divisor if there is an element $b \in R$ $\underline{b \neq 0}$, such that either

$$ab = 0 \quad \text{or} \quad ba = 0$$

If $a$ has a multiplicative inverse in $R$ then $a$ is not a zero divisor.

**Proof.** suppose $ba = 0$ $\qquad c$ is a multiplicative inverse of $a$

$\underline{bac}$ $\qquad b \cdot (ac) = b \cdot 1 = b$

$(b \cdot a) \cdot c = 0 \cdot c = 0$ $\Big\}$ $b = 0$

Thus $a$ is not a zero divisor. $\square$.

ring $\to$ division ring $\to$ field.

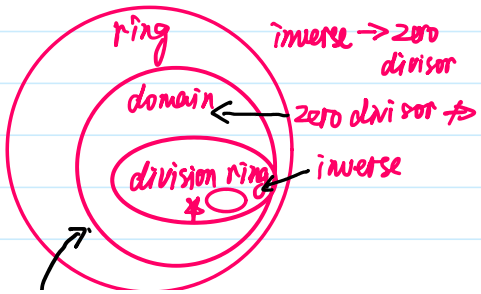
ring $\to$ commutative $\to$ field.

ring $\to$ field: ×××××× domain.

integral domain.

**Definition lemma.** Let $R$ be a ring. We say that $R$ is a domain if $R$ has no zero divisors. If a domain $R$ is commutative. then we say that $R$ is an integral domain.

Every division ring is a domain.




**Example.** $\mathbb{Z}$ is an integral domain.

Example. $\mathbb{Z}$ is an integral domain.

Let $R$ be any ring. suppose that $n>1$ $M_n(R)$ is not a domain.

$n=2$: $A=B=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ $AB=\begin{pmatrix}0&0\\0&0\end{pmatrix}$

$R$ is an integral domain iff $ab=0$ either $a=0$ or $b=0$.

## Ring homomorphisms and ideals

Definition: Let $\phi: R\to S$ be a function between two rings. We say that $\phi$ is a ring homomorphism if for every $a,b\in R$

$$\phi(a+b)=\phi(a)+\phi(b)$$
$$\phi(a\cdot b)=\phi(a)\cdot\phi(b) \qquad \phi(1)=1$$

object: ring

morphism: ring homomorphism.

Example: automorphism: ① $\phi: \mathbb{C}\to\mathbb{C}$. $\phi^2=I$.

$a+bi \quad a-bi$.

$\phi: \mathbb{C}\to\mathbb{C}$

$a-bi \quad a+bi$.

② $\phi: R[x]\to R[x]$.

$f(x)\to f(x+1)$ $\phi\phi'=I$

$\phi': R[x]\to R[x]$

$f(x)\to f(x-1)$

Definition: Let $\phi: R\to S$ be a ring homomorphism.
The kernel of $\phi$, denoted $\ker\phi$, is the inverse image of zero.

kernel is a normal subgroup $\phi(I)=0$ $\phi(\ker\phi)=0$

kernel is a normal subgroup $\phi(I) = 0$ $\phi(\ker\phi) = 0$

Abelian group : all subgroups are normal. $\trianglelefteq$

Definition : Let $R$ be a ring. Let $I$ be a subset of $R$.

lemma. we say that $I$ is an ideal of $R$ and write $I \triangleleft R$ if $I$ is an additive subgroup of $R$ and for every $a \in I$. $r \in R$ we have.

$$ra \in I, \quad \text{and} \quad ar \in I.$$

let $\phi: R \to S$ be a ring homomorphism. and let $I$ be the $\ker\phi$. then $I$ is an ideal of $R$.

Proof: $I$ is an additive subgroup. suppose. $a \in I$. $r \in R$.

$$\phi(ra) = \phi(r)\cdot\underbrace{\phi(a)}_{=0} = \phi(r)\cdot 0 = 0$$

$ra \in \ker\phi$. $\ker\phi$ is an ideal of $R$. $\square$.

$ar \in \ker\phi$.

Given an additive subgroup $H$ of $R$: $R/H$ : the group of left cosets of $H$ in $R$.

$[aH], [bH], [cH], \cdots$

Proposition: let $R$ be a ring. and let $I$ be an ideal of $R$. $I \neq R$.

$R/I$ is a ring.

There is a natural ring homomorphism: $u: R \to R/I$

$u(r) = r + I$.

Proof: $R/I$ is a group. under addition.

multiplicative: $r+I$, $s+I \in R/I$

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

well defined. $r+I = r'+I$ $r' = r+i$ $r's' = (r+i)(s+j) = rs + is + rj + ij$.

$s+I = s'+I$. $s' = s+j$ $i, j \in I$.

$I$ is an ideal. $is + rj + ij \in I$. $\Rightarrow$ $r's' + I = rs + I$.

multiplicative is well-defined.

$I$ is an ideal. $is + rj + ij \in I$. $\Rightarrow$ $r's' + I = rs + I$.

multiplicative is well-defined.

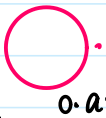
Associativity: $[(r+I)\cdot(s+I)](t+I) = (rs+I)\cdot(t+I) = rst + I$
$(r+I)\cdot[(s+I)(t+I)] = (r+I)\cdot(st+I) = rst + I$ $\Big\}$ ✓ $\square$

ring homomorphism: $\phi(r+s) = r+s+I$.

$\phi(r)+\phi(s) = r+\underline{I}+s+\underline{I} = r+s+I$.

**Definition.** Let $R$ be a commutative ring and let $a \in R$ be an element of $R$.

**Lemma.** the set $I = \langle a \rangle = \{ra \mid r \in R\}$ is an ideal and any ideal of this form is called principal.



$\cdot a = I$. (principal)

$0 \cdot a = 0$

Proof: $I$ is an additive subgroup. let $x, y \in I$. $x = ra$, $y = sa$. $r, s \in R$.

$x + y = ra + sa = (r+s)a$ $r+s \in R$. $(r+s)\cdot a \in I$.

$I$ is closed under addition.

$-x = -ra = (-r)\cdot a$ $-r \in R$. $(-r)\cdot a \in I$. $-x \in I$.

the inverse of $x \in I$.

$x + (-x) = 0$
inverse.

$I$ is closed under inverse.

$I$ is an additive subgroup.

$x \in I$. $s \cdot x = s \cdot ra = (sr)\cdot a \in I$.

$s \in R$.

$I$ is an ideal. $\square$.

5. Mar. 2022
4pm.