13th abstract algebra

2022年2月20日 星期日 上午10:02

Ring

Definition: a ring is a set R. binary operations $\oplus$ $\otimes$.

$\oplus$: R is an abelian group.

1. $(a+b)+c = a+(b+c)$ Associativity. ✓ subset
2. $a+0 = 0+a$ zero ✓
3. $\forall a.\ \exists b$ s.t. $a+b=b+a=0$ Additive inverse ✓ closed
   $b=-a$
4. $\forall a.b.\ \ a+b=b+a$ commutativity $\Leftarrow$ ✓ subset

$\cdot$: associative, multiplicative identity.

5. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ Associativity. } monoid. ✓ subset
6. $\exists 1\neq 0$ (②), $\forall a$, $a\cdot 1 = 1\cdot a$ Unit ● ✓ assumption (①)

$+$ · compatible

7. $a\cdot(b+c) = a\cdot b + a\cdot c$ (*)
   $(b+c)\cdot a = b\cdot a + c\cdot a$ Distributivity ✓ subset

Remark. definition of rings is not standard.
① semigroup
② 1 can be 0.

Example: complex number. $+$ · $a+bi$ ring.

$+$. obvious. · $[(a+bi)\cdot(c+di)]\cdot(e+fi) = (a+bi)[(c+di)(e+fi)]$

$a=1, b=0$ $(c+di)\cdot 1 = 1\cdot(c+di)$

distributivity: $(a+bi)(c+di+e+fi)$ $(a+bi)(c+di)+(a+bi)(e+fi)$

$(a+bi)[e+c+(d+f)i) =$ $ac+ae$

$ae+ac$

Definition: Let R be a ring and let S be a subset of R.

We say that S is a subring of R if S becomes a ring with induced $+$ and $\cdot$.

We say that S is a subring of R if S becomes a ring with induced $+$ and $\cdot$.

Lemma: Let R be a ring and let S be a subset that contains 1.

Then S is a subring iff S is closed under addition, additive inverses and multiplication.

Proof: $\Rightarrow$ obvious.
$\Leftarrow$ subset of R $\square$.

Example: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. subrings.

$\frac{a}{b}$ a, b integers. b odd. is a subring of rational numbers.

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $b \cdot d$: odd.

$\mathbb{Z}_n$. left cosets of $n\mathbb{Z}$ inside $\mathbb{Z}$ (integers modulo n)

$[0], [1] \cdots [n-1]$

zero, unit

$n=6$. $0=[0]$ $1=[1]$ $[2][3]=[2\cdot 3]=[6]=[0]$

Definition-Lemma: Let X be any set and R be any ring.
Then the set $\bar{R}$ of functions from X into R becomes a ring.
$+$ $\cdot$ defined as pointwise.
$f, g \in \bar{R}$. $(f+g)(x) = f(x) + g(x) \in R$ $x \in X$.

$(f \cdot g)(x) = f(x) \cdot g(x) \in R$

$f(x) = 0 \in R$ zero.

$g(x) = 1 \in R$ unit.

$X \to R$ functions ring

Proof: associativity: f, g, h $(f+g)+h = f+(g+h)$.

$((f+g)+h)(x) = (f+g)(x) + h(x) = f(x)+g(x)+h(x)$.

$= f(x) + (g(x)+h(x))$

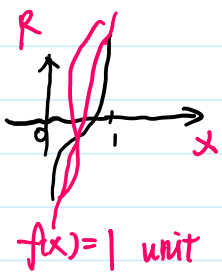
$= [f+(g+h)](x)$

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

$$(f+g)(x) = f(x) + \underbrace{g(x)}_{0} = f(x) = [f+(g+h)](x)$$

□

Example: $X = [0,1]$, $R = \mathbb{R}$ $\quad X \to R$.



continuous function from $[0,1]$ into $\mathbb{R}$

sum and product of continuous functions is continuous.

$f(x) = 1$ unit

$f(x) = \cdots$, $g(x) = -f(x)$ $\quad f(x)+g(x) = 0$. (from definition)

Definition-Lemma. Let R be a ring and let n be a positive integer.

$M_n(R)$ denotes the set of all $n \times n$ matrices with entries in R.

$M_n(R) \ni A = (a_{ij})$, $B = (b_{ij})$ $\quad A+B = (a_{ij}+b_{ij})$ $\quad A \cdot B = \cdots$

ij th entry of $A \cdot B$ is the dot product of the ith row of A and jth column of B.

0: zero matrix $\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$ $\quad 1$: $\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$ identity matrix.

Ring.

Proof: obvious. □

Example: $M_1(R)$ $\quad [R]$ is a copy of R.

$R = \mathbb{Z}_6$. $\quad n = 2$. $\quad A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}$ $\quad B = \begin{pmatrix} 1 & 5 \\ 1 & 2 \end{pmatrix}$ $\quad AB = \begin{pmatrix} 4 & 5 \\ 0 & 0 \end{pmatrix}$

Definition-Lemma. Let R be a ring and x be an indeterminate.

polynomial ring $R[x]$ is defined to the set of all formal sums.

$$a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 = \sum a_i x^i \quad a_i \in R.$$

f. $\sum_{i=0}^{n} a_i x^i$

g. $\sum_{i=0}^{m} b_i x^i$ $\quad f+g$. $\sum_{i=0}^{n} (a_i+b_i) x^i$ $\quad (m \le n,\ b_i = 0 \text{ for } i > m)$

$f \cdot g$ $\quad \sum_{j} \left[\sum_{i} a_j b_{i-j} \right] x^i$

0. $\leq \deg$ $f \cdot g$ $\sum_i [\sum_j a_j b_{i-j}] x^i$

0: $f = 0$

1. $g = 1$

Proof: from definition. □.

$R = \mathbb{Z}_2$. smallest ring. a ring should contain zero and unit.

$R \to R$ (4) $1 \to 1$, $2 \to 2$; $1 \to 1$, $2 \to 2$; $1 \to 1$, $2 \to 2$; $1 \to 1$, $2 \to 2$

polynomials. infinite many polynomials. $x \to y$

$x \to 2$, $1 \to 1$ x^2 x^5.

Two different polynomials often determine the same function. $x^5 + x \to 2$, $x^6 + 1 \to 1$ $x^4 x \to 2$

complex number $i^2 = -1$ $a + bi$

quaternions. i, j, k $a + bi + cj + dk$. a.b.c.d are real numbers

$a + bi + cj + dk + a' + b'i + c'j + d'k = (a+a') + (b+b')i + (c+c')j + (d+d')k$.

$i^2 = j^2 = k^2 = -1$. $ij = k$ $jk = i$ $ki = j$ $ji = -k$ $kj = -i$ $ik = -j$.

$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') +$
$(ab' + b'a + cd' - dc')i +$
$(ac' + c'a' + db' - bd')j +$
$(ad' + da' + bc' - b'c)k$

This gives us a group. a. $\pm 1 \cong \mathbb{Z}_2$

$a + bi$ $\{\pm 1, \pm i\} \cong \mathbb{Z}_4$.

quaternions $\{\pm 1, \pm i, \pm j, \pm k, \} \cong \mathbb{Z}_8$.

1+0i -1+0i 0+1i 0-1i

$\{1, -1, i, -i\} \cong \mathbb{Z}_4$

Basic properties of Rings

Lemma. Let R be a ring and let a and b be elements of R

(1). $a \cdot 0 = 0 \cdot a = 0$

(2) $a \cdot (-b) = (-a) \cdot b = -(ab)$.

Proof: (1). let $x = a0$

$x = a0$
$= a(0+0)$
$= a0 + a0$
$= x + x$

$x - x = x + x - x$
$0 = x + 0 = x = a0.$

(2) let $y = a(-b)$

want. $y + (ab) = 0$ ✓

$y + ab = a(-b) + ab$
$= a(-b+b)$ distributivity
$= a \cdot 0$
$= 0$

□.

Lemma. Let R be a set that satisfies all the axioms of a ring except $a+b = b+a$.
Then R is a ring.

proof: $(a+b)(1+1) = (a+b)\cdot 1 + (a+b)\cdot 1$
$= a+b+a+b$
$= a+(b+a)+b$

$(a+b)(1+1) = a\cdot(1+1) + b(1+1)$
$= a+a+b+b.$

$a+(b+a)+b = a+a+b+b.$
$b+a+b = a+b+b$
$b+a = a+b.$

□

Lemma. Let R be a ring and let a and b be any two elements of R.
Then
$$(a+b)^2 = a^2+ab+ba+b^2$$

proof: $(a+b)(a+b) = (a+b)\cdot a + (a+b)\cdot b$
$= a^2 + b\cdot a + ab + b^2$
$= a^2 + ab + ba + b^2.$

□

2.26.2022
4pm.