Chap 17: Rings

Def: A ring is a set A with operations called addition and multiplication which satisfy the following axioms:

(i) A with addition alone is an abelian group

(ii) Multiplication is associative

(iii) Multiplication is distributive over addition: $\forall a,b,c \in A$:

$$a(b+c) = ab+ac \text{ and } (b+c)a = ba+ca.$$

- $a+0=0+a=a$. $a+(-a)=(-a)+a=0$.
- $a-b = a+(-b)$.

Ex: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathcal{F}(\mathbb{R})$; $\mathbb{Z}_n$

Thm (i) $a \cdot 0 = 0$, $0a = 0$ $\forall a \in \mathbb{R}$ (ii) $a(-b) = -(ab)$, $(-a)\cdot b = -ab$.

(iii) $(-a)(-b) = ab$.

Pf: (i) $a0 + a\cdot 0 \overset{\text{distributive}}{=} a\cdot(0+0) = a\cdot 0 \Rightarrow a \cdot 0 = 0$. similarly: $0 \cdot a = 0$.

(ii) $a\cdot(-b) + a\cdot b = a(-b+b) = a0 = 0 \Rightarrow a\cdot(-b) = -ab$

(iii) $(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(ab)) = ab$

Optional features for rings:

- commutative ring: $a\cdot b = ba$ $\forall a,b \in A$ (not automatic)
- ring with unity: $\exists 1 \in A$, s.t. $\forall a \in A$, $a \cdot 1 = 1 \cdot a = a$
- nontrivial ring: $A \neq \{0\}$.

If A is nontrivial with the unity 1 then $1 \neq 0$.

- If A is a ring with unity, elements which have a multiplicative are called invertible.

an element a is invertible if there is some $x \in A$ s.t. $ax = xa = 1$.

For example, in $\mathbb{R}$ every nonzero element is invertible: $x^{-1} = \frac{1}{x}$ $\forall x \in \mathbb{R}^*$

in $\mathbb{Z}$, the only invertible elements are 1 and -1.

- zero is never an invertible element of a ring except if the ring is trivial:

$0 = 0 \cdot x = 1 \Rightarrow$ ring is trivial.

Def: If A is a commutative ring with unity in which every nonzero element is invertible, A is called a field.

Examples of fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

finite fields: $\mathbb{Z}_p$, p is a prime number.

Def: In any ring, a nonzero element a is called a divisor of zero if there is a nonzero element b in the ring s.t. the product ab or ba is equal to zero.

Ex: · In $\mathbb{Z}_6$, $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0} = 0 \Rightarrow \bar{2}$ and $\bar{3}$ are both divisors of zero

$\bar{4} \cdot \bar{3} = \bar{12} = \bar{0} = 0 \Rightarrow \bar{4}$ (and $\bar{3}$) are divisors of zero.

· In $M_2(\mathbb{R})$, many divisors of zeros.

ring of nxn matrices.

$\det(A) \neq 0 \Rightarrow \ker(A) \neq \{0\} \Rightarrow \exists v \in \mathbb{R}^n$ s.t. $Av = 0$

$\Rightarrow A(v \cdots v) = 0$ $\quad A \neq 0$, $(v \cdots v) \neq 0$ $\Rightarrow A$ is a divisor of zero

- In a ring, the cancellation property is not necessarily true:

In $\mathbb{Z}_6$, $\underbrace{\bar{2} \cdot \bar{3} = \bar{4} \cdot \bar{3}}_{\bar{0}}$ but $\bar{2} \neq \bar{4}$.

Def: A ring is said to have the cancellation property if

$ab = ac$ or $ba = ca$ implies $b = c$.

for any elements $a, b,$ and c in the ring if $a \neq 0$.

Thm 2: A ring has the cancellation property iff it has no divisors of zero

Pf: If A has the cancellation property, then $a \neq 0$. $ab = 0 = a \cdot 0$ $\Rightarrow b = 0$ so a is not a divisor of zero

$ba = 0 = 0 \cdot a$

Conversely, if A has no divisors of zero, then

$$\underset{a \neq 0}{ab = ac} \Rightarrow \underset{a \neq 0}{a(b-c) = 0} \Rightarrow b = c$$

OR $ba = ca \Rightarrow (b-c)a = 0 \Rightarrow b = c$

so A has the cancellation property.

Def: An integral domain is a commutative ring with unity having the cancellation property.

equivalently, an integral domain is a commutative ring with unity having no divisors of zero.

Ex:
- every field is an integral domain.
- $\mathbb{Z}$ is an integral domain but not a field.

Exer: D. Ring of Subsets of a Set.

Let D be a set, P_D: the power set of D = all the subsets of D.

$\forall A, B \in P_D$. $A + B = (A - B) \cup (B - A)$, and $AB = A \cap B$.

$\begin{pmatrix} A \subseteq D \\ B \subseteq D \end{pmatrix}$ Chap 3. Exer C shows that $(P_D, +)$ is an abelian group with $0 = \phi$

D.1: P_D is a commutative ring with unity.

- multiplication is associative: $(AB)C = (A\cap B)\cap C = A\cap(B\cap C) = A(BC)$
- distributive: $A(B+C) = A\cap((B-C)\cup(C-B)) = (A\cap B - A\cap C)\cup(A\cap C - A\cap B)$
$$= (A\cap B) + (A\cap C) = AB + AC$$
Similarly. $(B+C)A = BA + CA$.
- Commutative ring: $AB = A\cap B = B\cap A = BA$
- multiplicative unity: $\left.\begin{array}{l} A\cdot D = A\cap D = A \\ D\cdot A = D\cap A = A \end{array}\right\} \Rightarrow D = 1$ in $(P_D, +, \cdot)$ the ring.

D.2 divisors of zeros: $\forall A\in P_D,\ A\neq\phi,\ A\neq D \Rightarrow \underset{A\cdot A^c}{A\cap A^c} = \phi = 0$
$\Downarrow$ $A^c\neq\phi, A^c\neq D$.

$\Rightarrow A$ is a divisor of zero.

$A = D = 1$ is not a divisor of zero.

So any proper nonempty subset is a divisor of zero.

Ex: $A = \mathbb{Z} + \mathbb{Z}\cdot\sqrt{n} = \{x + y\sqrt{n};\ x, y\in\mathbb{Z}\}$.

- $(A,+)$ is an abelian group with $0 = 0 + 0\cdot\sqrt{n}$. $-(x+y\sqrt{n}) = -x - y\sqrt{n}$
- multiplication is associative
- multiplication is distributive over addition
- multiplication is commutative
- $1 = 1 + 0\cdot\sqrt{n}$ is the multiplicative unity.

Ex: A.1 $A = \mathbb{Z}$ with addition: $a \oplus b = a+b-1$

$$a \odot b = ab-(a+b)+2$$

$(A, \oplus)$ is an abelian group with identity 1 and $\ominus a = 2-a \ \forall a \in A$.

$(A, \odot)$ is associative: $(a\odot b)\odot c = (ab-(a+b)+2)\odot c$

$$= (ab-(a+b)+2)c-(ab-(a+b)+2+c)+2$$

$$= abc-ac-bc-ab+a+b+c$$

$a\odot(b\odot c) = a\odot(bc-(b+c)+2)$

$$= a(bc-(b+c)+2)-(a+bc-(b+c)+2)+2 = abc-ab-ac-bc+a+b+c$$

$(\mathbb{Z}, \oplus, \odot)$ is isomorphic to $(\mathbb{Z}, +, \times)$:

$$f: \mathbb{Z} \longrightarrow \mathbb{Z} \qquad x \longmapsto x-1$$

f is bijective: $f^{-1}(y) = y+1$.

$$f(x\oplus y) = x\oplus y-1 = (x+y-1)-1 = x-1+y-1 = f(x)+f(y)$$

$$f(x\odot y) = x\odot y-1 = xy-(x+y)+2-1 = (x-1)\cdot(y-1) = f(x)\cdot f(y).$$

Exer: A is integral domain

H.4: $x = x^{-1} \Leftrightarrow x^2 = 1 \Rightarrow 0 = x^2 - 1 = (x+1)(x-1) \Rightarrow x+1=0$ or $x-1=0$

So $x=-1$ or $x=1$

H.5. $(a+b)(1+1) = (a+b)1 + (a+b)1 = a+b+a+b$
$\;\;\;\; \| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Big\} \Rightarrow a+b=b+a$
$a(1+1)+b(1+1) = a+a+b+b$

H.6. If the additive group of a ring A is cyclic, then A is a commutative ring.

$(A,+) = \langle a \rangle = \{ m \cdot a \,;\, m \in \mathbb{Z} \}$

$$ma = \begin{cases} \underbrace{a + \cdots + a}_{m} & m>0 \\ -[\underbrace{(+a) + \cdots + (+a)}_{-m}] & m<0 \\ 0 & m=0 \end{cases}$$

$m_1 a \cdot m_2 a = (m_1 m_2) \cdot a^2 = (m_2 m_1) a^2 = m_2 a \cdot m_1 a$

J.2. If ab is a divisor of zero, then a or b is a divisor of zero.

If: $ab \cdot c = 0$, $c \neq 0$
- if $bc \neq 0$, then a is a divisor of zero
- if $bc = 0$, then b is a divisor of zero

If: $c \cdot ab = 0$, $c \neq 0$
- if $ca \neq 0$, then b is a divisor of zero
- if $ca = 0$, then a is a divisor of zero

K. Boolean ring: $a^2 = a$. $\forall a \in A$

1. For every $a \in A$, $a = -a$: $(a+a)^2 = (2a)^2 \overset{\text{Boolean ring}}{=} 2a \Rightarrow 2a = a+a = 0$
$\qquad \| \qquad\qquad \|$
$\qquad 4a^2 = 4a$

2. A is commutative: $(a+b)\cdot(a+b) = a^2 + ab + ba + b^2$
$\qquad \| \qquad\qquad\qquad \| \qquad\qquad \Rightarrow ab+ba=0$
$\qquad a+b = a+ab+ba+b \qquad \Downarrow$ part 1
$\qquad ba = -ab \overset{}{=} ab$

If A is unity:

3. $a^2 - a = a(a-1) = 0 \Rightarrow$ if $a \neq 0$ and $a \neq 1$, then a is a divisor of zero.

4. $1 = ab (\underset{\text{A is commutative}}{=} ba) \Rightarrow$ a is not a divisor of zero $\Rightarrow a = 1$ ($a=0$ is not invertible)

5. $a \vee b = a+b+ab$. $a \vee bc = a + bc + abc \;=\; a^2 + bc + abc$

$(a \vee b)(a \vee c) = (a+b+ab)(a+c+ac) = a^2 + \cancel{ac} + \cancel{a^2c} + \cancel{ba} + bc + bac$
$\qquad + \cancel{aba} + \cancel{abc} + \cancel{abac}$

$a \vee (1+a) = a + 1 + a + a(1+a) = 1 + a + a^2 = 1 + a + a = 1$

$a \vee a = a + a + a^2 = a + a + a = a \qquad (a+a=0)$

$a(a \vee b) = a(a+b+ab) = a^2 + ab + a^2 b = a + ab + ab = a$