Rings

Definitions and Basic Properties

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

October 5, 2020

Definitions

- A set R with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ is called a **ring** if for all $a, b, c \in R$, the following conditions are satisfied.
  (1) $a + b = b + a$ [+ is commutative]
  (2) $(a+b)+c = a+(b+c)$ [+ is associative]
  (3) There exists $0 \in R$ such that $0 + a = a + 0 = a$ [additive identity]
  (4) There exists $-a \in R$ such that $a + (-a) = (-a) + a = 0$ [additive inverse]
  (5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ [$\cdot$ is associative]
  (6) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ [$\cdot$ is distributive over +]
- A ring $(R, +, \cdot)$ is called **commutative** if for all $a, b \in R$, we have:
  (7) $a \cdot b = b \cdot a$ [$\cdot$ is commutative]
- A ring $(R, +, \cdot)$ is called a **ring with identity** (or a **ring with unity**) if
  (8) there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. [multiplicative identity]

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under standard addition and multiplication are commutative rings with identity.
- Let $n \in \mathbb{N}$, $n \geqslant 2$. Denote by $M_n(\mathbb{Z})$ (resp. $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, $M_n(\mathbb{C})$) the set of all $n \times n$ matrices with integer (resp. rational, real, complex) entries. These sets are rings under matrix addition and multiplication. These rings are not commutative, but contains the identity element (the $n \times n$ identity matrix).
- Let S be a set with at least two elements (S may be infinite). $\mathscr{P}(S)$ is a commutative ring with identity under the operations Δ (symmetric difference) and $\cap$ (intersection). The additive identity is $\emptyset$, and the multiplicative identity is S. The additive inverse of $A \subseteq S$ is A itself.
- Let $n \in \mathbb{N}$, $n \geqslant 2$. The set $\{0,1\}^n$ of n-bit vectors is a commutative ring with identity under bit-wise XOR and AND operations. The zero vector is the additive identity, and the all-1 vector is the multiplicative identity. The additive inverse of a bit vector v is v.

Examples

$\mathbb{Z}$ under the two operations

$$\begin{aligned} a \oplus b &= a + b - 1 \\ a \odot b &= a + b - ab \end{aligned}$$

is a commutative ring with identity.

- Check associativity of $\oplus$ and $\odot$:
  $(a \oplus b) \oplus c = a \oplus (b \oplus c) = a + b + c - 2,$
  $(a \odot b) \odot c = a \odot (b \odot c) = a + b + c - ab - bc - ca + abc.$
- Check distributivity of $\odot$ over $\oplus$:
  $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c) = a + b + 2c - ac - bc - 1.$
- 1 is the additive identity because $a \oplus 1 = 1 \oplus a = a + 1 - 1 = a$ for all $a \in \mathbb{Z}$.
- The additive inverse of a is $2 - a$ because $a \oplus (2 - a) = a + (2 - a) - 1 = 1$.
- 0 is the multiplicative identity because $a \odot 0 = 0 \odot a = a + 0 - a \times 0 = a$ for all $a \in \mathbb{Z}$.

Zero Divisors

An element $a \in R$ is called a **zero divisor** if $a \cdot b = 0$ for some $b \neq 0$.
0 is always a zero divisor.
We are interested in non-zero (or proper) zero divisors.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under standard operations do not contain non-zero zero divisors.
- The matrix rings contain non-zero zero divisors. For example, $\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\mathscr{P}(S)$ contains non-zero zero divisors. Take any non-empty proper subset A of S. Then $A \cap (S \setminus A) = \emptyset$.
- The ring $(\mathbb{Z}, \oplus, \odot)$ does not contain non-zero zero divisors, because $a \odot b = a + b - ab = 1$ implies $(a-1)(b-1) = 0$, that is, either $a = 1$ or $b = 1$.

Units

Let R be a ring with identity.

An element $a \in R$ is called a **unit** if there exists $b \in R$ such that $ab = ba = 1$ (so b is also a unit). We say a and b are **multiplicative inverses** of one another.

We write $b = a^{-1}$ and $a = b^{-1}$.

- The only units of $(\mathbb{Z}, +, \cdot)$ are ± 1.
- All non-zero elements of $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are units.
- The units of $M_n(\mathbb{Z})$ are precisely those matrices with determinant ± 1.
- The units of $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are the invertible matrices.
- The only unit in $\mathscr{P}(S)$ is S.
- Consider $(\mathbb{Z}, \oplus, \odot)$. $a \odot b = 0$ implies $a + b - ab = 0$, that is, $b = \frac{a}{a-1}$. Since b is an integer, the only possibilities for a are 0 and 2. These are the only units, and are equal to their respective inverses.

Definitions

Let R be a commutative ring with identity.

R is called an **integral domain** if R contains no non-zero zero divisors.

R is called a **field** if every non-zero element of R is a unit.

- $(\mathbb{Z}, +, \cdot)$ is an integral domain but not a field.
- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.
- The matrix rings are neither integral domains nor fields.
- $\mathscr{P}(S)$ is neither an integral domain nor a field.
- $(\mathbb{Z}, \oplus, \odot)$ is an integral domain but not a field.

Elementary Properties of Rings

Theorem: In a ring R, the additive identity is unique. Moreover, for every $a \in R$, the additive inverse $-a$ is unique.

Proof Let 0 and $0'$ be additive indentities. Then $0 = 0 + 0' = 0'$.
If b and c are additive inverses of a, we have
$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$. ◀

Theorem: In a ring R with identity, the multiplicative identity is unique. Moreover, for every unit a in R, the multiplicative inverse a^{-1} is unique. ◀

Elementary Properties of Rings

Theorem: (*Cancellation laws of addition*) Let a, b, c be elements in a ring R.

(i) If $a+b = a+c$, then $b = c$.

(ii) If $a+c = b+c$, then $a = b$.

Proof $a+b = a+c \Rightarrow -a+(a+b) = -a+(a+c) \Rightarrow (-a+a)+b = (-a+a)+c \Rightarrow 0+b = 0+c \Rightarrow b = c$. ◀

Theorem: (*Cancellation laws of multiplication*) Let R be a ring with identity. Let a be a unit in R, and b, c any elements in R.

(i) If $ab = ac$, then $b = c$.

(ii) If $ba = ca$, then $b = c$. ◀

Elementary Properties of Rings

Theorem: Let R be a ring, and $a, b, c \in R$.

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

(ii) $-(-a) = a$.

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

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

Proof (i) $0+0=0 \Rightarrow a\cdot(0+0) = a\cdot 0 \Rightarrow a\cdot 0 + a\cdot 0 = a\cdot 0 = a\cdot 0 + 0$. Now use cancellation.

(ii) $(-a)+a = a+(-a) = 0 \Rightarrow -(-a) = a$.

(iii) $(-a)b+ab = (-a+a)b = 0b = 0$, so $-(ab) = (-a)b$. Likewise, $-(ab) = a(-b)$.

(iv) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. ◀

Elementary Properties of Rings

Theorem: Let R be an integral domain. Let a, b, c be elements of R with $a \neq 0$. Then $ab = ac$ implies $b = c$.

Proof $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0$ (since R does not contain non-zero zero divisors) $\Rightarrow b = c$. ◀

Theorem: Every field is an integral domain.

Proof Let F be a field. Take $a, b \in F$ such that $ab = 0$. We have to show that either $a = 0$ or $b = 0$. Suppose that $a \neq 0$. Then a is a unit. We can use cancellation from $ab = 0 = a \cdot 0$ to get $b = 0$. ◀

Theorem: Every *finite* integral domain is a field.

Proof Let R be an integral domain consisting of only finitely many elements. Take any non-zero $a \in R$. The map $R \to R$ taking $x \mapsto ax$ is injective and so bijective. In particular, there exists x such that $ax = 1$. Thus a is a unit. ◀

Subrings

Definition: Let $(R,+,\cdot)$ be a ring. A non-empty subset S of R is called a **subring** of R if S is a ring under the operations $+$ and $\cdot$ inherited from R.

Theorem: S is a subring of R if for all $a,b \in S$, we have $a-b, ab \in S$.

Proof Commutativity of addition, associativity of addition and multiplication, and distributivity of multiplication over addition are inherited from R.
Since S is non-empty, there exists $a \in S$, so $a-a=0 \in S$. Therefore $0-a=-a \in S$.
Finally, for $a,b \in S$, we have $a+b=a-(-b) \in S$. So S is closed under addition and multiplication. ◀

Subrings: Examples

- $\mathbb{Z}$ is a subring of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
  $\mathbb{Q}$ is a subring of $\mathbb{R}, \mathbb{C}$.
  $\mathbb{R}$ is a subring of $\mathbb{C}$.
- Let $n \in \mathbb{N}$. $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$.
- Let $S = \left\{ \begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} \mid x, y \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$.
- $\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} - \begin{pmatrix} u & u+v \\ u+v & u \end{pmatrix} = \begin{pmatrix} x-u & (x-u)+(y-v) \\ (x-u)+(y-v) & x-u \end{pmatrix}$.
- $\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} \begin{pmatrix} u & u+v \\ u+v & u \end{pmatrix} = \begin{pmatrix} (2u+v)x+(u+v)y & (2u+v)x+(u+v)y+(-vy) \\ (2u+v)x+(u+v)+(-vy) & (2u+v)x+(u+v) \end{pmatrix}$.

Ring Homomorphisms and Isomorphisms

Definition: Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings. A function $f : R \to S$ is called a **homomorphism** if for all $a, b \in R$, we have:

(1) $f(a+b) = f(a) \oplus f(b)$, and
(2) $f(a \cdot b) = f(a) \odot f(b)$.

A bijective homomorphism is called an **isomorphism**.

- The map $\mathbb{C} \to \mathbb{C}$ taking $a + \mathrm{i}b$ to $a - \mathrm{i}b$ is an isomorphism of fields.
- The map $\mathbb{R} \to M_2(\mathbb{R})$ taking a to $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ is a homomorphism of rings.
- The map $\mathbb{C} \to M_2(\mathbb{R})$ taking $a + \mathrm{i}b$ to $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is a homomorphism of rings.

Ring Homomorphisms and Isomorphisms

- $(\mathbb{Z}, +, \cdot)$ is a ring.
- $(\mathbb{Z}, \oplus, \odot)$ is a ring, where $a \oplus b = a + b - 1$, and $a \odot b = a + b - ab$.
- Define a map $f : \mathbb{Z} \to \mathbb{Z}$ taking a to $1 - a$.
- $f(a+b) = 1 - a - b$, whereas
  $f(a) \oplus f(b) = (1-a) \oplus (1-b) = 1 - a + 1 - b - 1 = 1 - a - b$.
- $f(ab) = 1 - ab$, whereas $f(a) \odot f(b) = (1-a) \odot (1-b) =$
  $(1-a) + (1-b) - (1-a)(1-b) = 2 - a - b - 1 + a + b - ab = 1 - ab$.
- f is clearly bijective.
- f is therefore an isomorphism from $(\mathbb{Z}, +, \cdot)$ to $(\mathbb{Z}, \oplus, \odot)$.

Properties of Homomorphisms

Theorem: Let $f : (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring homomorphism.

(i) $f(0_R) = 0_S$.

(ii) $f(-a) = -f(a)$ for all $a \in R$.

(iii) $f(na) = nf(a)$ for all $a \in R$ and $n \in \mathbb{Z}$.

(iv) $f(a^n) = f(a)^n$ for all $a \in R$ and $n \in \mathbb{N}$.

(v) If A is a subring of R, then $f(A)$ is a subring of S.

Proof (i) $0_R + 0_R = 0_R \Rightarrow 0_S \oplus f(0_R) = f(0_R) = f(0_R + 0_R) = f(0_R) \oplus f(0_R)$.

(ii) $f(a + (-a)) = f(0_R) = 0_S$, that is, $f(a) \oplus f(-a) = 0_S$.

(iii) and (iv) Use induction on n and (ii).

(v) Since A is non-empty, $f(A)$ is non-empty too. Let $u, v \in f(A)$. Then $u = f(a)$ and $v = f(b)$ for some $a, b \in A$. $a - b \in A$ (since A is a subring of R). So $f(a - b) = f(a) \ominus f(b) = u \ominus v \in f(A)$. Likewise, show that $u \odot v \in f(A)$.

Properties of Homomorphisms

Theorem: Let $f : (R, +, \cdot) \to (S, \oplus, \odot)$ be a *surjective* ring homomorphism, where $|S| > 1$.

(i) If R has the identity 1_R, then $f(1_R)$ is the identity of S.

(ii) If a is a unit in R, then $f(a)$ is a unit in S, and $f(a^{-1}) = f(a)^{-1}$.

(iii) If R is commutative, then S is commutative.

Proof (i) Take any $u \in S$. Since f is surjective, $u = f(a)$ for some $a \in R$. But then $u = f(a) = f(a \cdot 1_R) = f(a) \odot f(1_R) = u \odot f(1_R)$. Likewise, $u = f(1_R) \odot u$. ◀