Abstract Algebraic Structures

Rings, Fields, and Groups

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

November 6, 2022

Rings

Definitions and Basic Properties

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

November 6, 2022

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

$$a \oplus b = a + b - 1$$
$$a \odot b = a + b - ab$$

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 $M_2(\mathbb{Z})$.
- $\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} - \begin{pmatrix} u & u+v \\ u+v & u \end{pmatrix} = \begin{pmatrix} x-u & (x-u)+(y-v) \\ (x-u)+(y-v) & x-u \end{pmatrix}$.
- $\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} \begin{pmatrix} u & u+v \\ u+v & u \end{pmatrix} = \begin{pmatrix} (2u+v)x+(u+v)y & (2u+v)x+(u+v)y+(-vy) \\ (2u+v)x+(u+v)+(-vy) & (2u+v)x+(u+v) \end{pmatrix}$.

Modular Arithmetic

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

November 6, 2022

Congruence Modulo n

- Take $n \in \mathbb{N}$ (preferable to have $n \geqslant 2$).
- Two integers $a, b \in \mathbb{Z}$ are said to be **congruent** modulo n if $n | (a - b)$.
- We denote this as $a \equiv b \pmod{n}$.
- Congruence modulo n is an equivalence relation on $\mathbb{Z}$.
- There are n equivalence classes: $[0], [1], [2], \ldots, [n-1]$.

Integers Modulo n

- Define $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$.
- You may view $\mathbb{Z}_n$ as the set of remainders of Euclidean division by n.
- You can also view the elements of $\mathbb{Z}_n$ as representatives of the equivalence classes under congruence modulo n.
- There is also an algebraic description (not covered). $\mathbb{Z}_n$ is quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ with respect to the ideal $n\mathbb{Z}$ of $\mathbb{Z}$.
- For $a, b \in \mathbb{Z}_n$, define the following operations.
  - $a +_n b = \begin{cases} a+b & \text{if } a+b < n, \\ a+b-n & \text{if } a+b \geqslant n. \end{cases}$
  - $a \cdot_n b = (ab) \operatorname{rem} n$.
- $\mathbb{Z}_n$ is a *commutative ring with identity* under these two operations.

Units of $\mathbb{Z}_n$

Theorem: $a \in \mathbb{Z}_n$ is a unit if and only if $\gcd(a,n) = 1$.

Proof [If] There exist integers u, v such that $ua + vn = 1$. We can choose u such that $0 \leqslant u < n$. But then $ua \equiv 1 \pmod{n}$.
[Only if] If a is a unit of $\mathbb{Z}_n$, then $ua \equiv 1 \pmod{n}$ for some $u \in \mathbb{Z}_n$, that is, $ua = 1 + vn$ for some v. Since $\gcd(a,n)$ divides a (and so ua) and n (and so vn), it divides 1, that is, $\gcd(a,n) = 1$.

- $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$.
- $|\mathbb{Z}_n^*| = \phi(n)$ (Euler totient function).
- Since $\mathbb{Z}_n^*$ is a group, we have $a^{\phi(n)} \equiv 1 \pmod{n}$ for any $a \in \mathbb{Z}_n^*$ (**Euler's theorem**).
- For a prime p, we have $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$, and $\phi(p) = p - 1$.
- For $a \in \mathbb{Z}_p^*$, we have $a^{p-1} \equiv 1 \pmod{p}$ (**Fermat's little theorem**).

Modular Exponentiation

Given $a \in \mathbb{Z}_n$ and $e \in \mathbb{N}_0$, to compute $a^e \pmod{n}$.

The square-and-multiply algorithm

modexp (a, e, n)
{
    If $(e = 0)$, return 1.
    Write $e = 2f + r$ with $f = \lfloor e/2 \rfloor$ and $r \in \{0, 1\}$.
    Set $t = \text{modexp}(a, f, n)$.
    Set $t = t^2 \pmod{n}$.
    If $(r = 1)$, set $t = ta \pmod{n}$.
    Return t.
}

Modular Exponentiation: Iterative Version

Let $e = (e_{l-1}e_{l-2}\ldots e_2e_1e_0)_2$ be the binary expansion of e.

```
modexp (a, e, n)
{
    Initialize t = 1.
    For i = l-1, l-2, ..., 2, 1, 0, repeat:
        Set t = t^2 (mod n).
        If (e_i = 1), set t = ta (mod n).
    Return t.
}
```

For $e < n$, the running time is $O(\log^3 n)$.

Groups

Definitions and Basic Properties

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

November 6, 2022

Definitions

- A set G with a binary operation $\circ : R \times R \to R$ is called a **group** if for all $a, b, c \in G$, the following conditions are satisfied.
  (1) $(a \circ b) \circ c = a \circ (b \circ c)$ [$\circ$ is associative]
  (2) There exists $e \in R$ such that $e \circ a = a \circ e = a$ [Identity]
  (3) For all $a \in G$, there exists $b \in G$ such that $a \circ b = b \circ a = e$ [Inverse]
- If $\circ$ is addition, the inverse of a is denoted by $-a$.
- If $\circ$ is multiplication, the inverse of a is denoted by a^{-1}.
- If $\circ$ is commutative, that is, $a \circ b = b \circ a$ for all $a, b \in G$, we call G a **commutative** or an **Abelian** group.

Examples

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are Abelian groups under addition.
- $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ are Abelian groups under multiplication.
- Let $(R, +, \cdot)$ be a ring. Then R is an Abelian group under $+$.
- If R is a ring with identity, then the set of units of R form a multiplicative group.
- In particular, $\mathbb{Z}_n$ is an Abelian group under modulo n addition, and $\mathbb{Z}_n^*$ is an Abelian group under modulo n multiplication.
- The set of all invertible $n \times n$ matrices over a field F is a group under matrix multiplication, called the **general linear group** $\mathrm{GL}_n(F)$.
- The set of all $n \times n$ matrices over a field F and with determinant 1 is a group under matrix multiplication, called the **special linear group** $\mathrm{SL}_n(F)$.
- $\mathrm{GL}_n(F)$ and $\mathrm{SL}_n(F)$ are not commutative in general.

The Symmetry Group

- The set S_n of all bijective functions $f : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$ is a group under function composition. $g \circ f$ is written as gf.
- A permutation f is often written as $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$.
- Every permutation can be written as a product of cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 4 & 1 & 7 & 3 & 2 \end{pmatrix} = (1\ \ 5)(2\ \ 6\ \ 7\ \ 3\ \ 8)(4).$$

- Every cycle can be written as a product of transpositions (swaps).

$$(2\ \ 6\ \ 7\ \ 3\ \ 8) = (2\ \ 6)(6\ \ 7)(7\ \ 3)(3\ \ 8).$$

- For each permutation, the parity of the number of transpositions is invariant.
- The set of all even permutations in S_n form the **alternating group** A_n.

Basic Properties

Theorem: Let $(G, \circ)$ be a group.

(1) The identity e of G is unique.

(2) The inverse of each $a \in G$ is unique.

(3) [*Left cancellation*] If $a \circ b = a \circ c$, then $b = c$.

(4) [*Right cancellation*] If $a \circ c = b \circ c$, then $a = b$.

(5) Let the inverses of a and b be u and v, respectively.
Then, the inverse of $a \circ b$ is $v \circ u$.

Subgroups

- Let $(G, \circ)$ be a group, and H a non-empty subset of G.
- H is called a **subgroup** of G if H is a group under the operation $\circ$ inherited from G.
- G and $\{e\}$ are **trivial** subgroups of G.
- Examples:
  - $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$.
  - $(\mathbb{Q}^*, \cdot)$ is a subgroup of $(\mathbb{R}^*, \cdot)$.
  - $(\mathbb{Z}_n, +)$ is not a subgroup of $(\mathbb{Z}, +)$ (the operations are different).
  - $\{0, 3, 6, 9, 12\}$ and $\{0, 5, 10\}$ are the only non-trivial subgroups of $(\mathbb{Z}_{15}, +)$.
  - $\{1, 4\}$, $\{1, 11\}$, and $\{1, 4, 11, 14\}$ are some non-trivial subgroups of $(\mathbb{Z}_{15}^*, \cdot)$.
  - $\mathrm{SL}_n(F)$ is a subgroup of $\mathrm{GL}_n(F)$.
  - A_n is a subgroup of S_n.

Criterion for Subgroups

Theorem: Let G be a multiplicative group, and H a non-empty subset of H. Then, H is a subgroup of G if and only if

(1) $ab \in H$ for all $a, b \in H$, and

(2) $a^{-1} \in H$ for all $a \in H$.

Proof [$\Rightarrow$] Obvious.

[$\Leftarrow$] Associativity is inherited from G. Pick any $a \in H$. Then $a^{-1} \in H$, and so $aa^{-1} = e \in H$.

Theorem: Let G be a multiplicative group, and H a non-empty finite subset of H. Then, H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof [$\Rightarrow$] Obvious.

[$\Leftarrow$] Let $aH = \{ah \mid h \in H\}$. By cancellation, the map $H \to aH$ taking h to ah is injective, so $|H| \leqslant |aH|$. By closure, $aH \subseteq H$, that is, $|aH| \leqslant |H|$. Therefore $|aH| = |H|$. Since these are finite sets, we have $aH = H$. Take any $a \in H$. Since $e \in H = aH$, we have $ah = e$ for some $h \in H$. Moreover, $(ha)^2 = h(ah)a = hea = ha = (ha)e$. By cancellation, $ha = e$. So $h = a^{-1} \in H$.

Order of a Group

- $|G|$ is the number of elements in G.
- Let G be a (multiplicative) group, and H a subgroup of G. Then, the following conditions are equivalent.
  (1) $aH = bH$.
  (2) $a^{-1}b \in H$.
- These equivalent conditions define an equivalence relation on G.
- The equivalence classes are aH for $a \in G$.
- The equivalence classes are equinumerous.
- **Lagrange's theorem:** Let G be a finite group, and H a subgroup. Then, the order of H divides the order of G.