

12 Algebraic Structure and Coding Theory

12.1 The Structure of Algebra

Def 1 Let S be a set and \oplus be a **binary operation** on S ($\oplus: S \times S \rightarrow S$).

2. The operation \oplus is **associative** over S , if $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.
1. The operation \oplus is **commutative** over S , if $a \oplus b = b \oplus a$.

Def 2 Let S be a set and $S' \subseteq S$. Let \oplus be a **binary operation** on S and \otimes be an **unary operation** of S . Then

1. S' is **closed** w.r.t. \oplus , if $\forall a, b \in S', a \oplus b \in S'$.
- 1'. S' is **closed** w.r.t. \otimes , if $\forall a \in S', \otimes a \in S'$.

Let us denote an **algebra(algebraic system)** (S, O, C) where

- (i) S is an **underlying set**,
- (ii) O is the set of **operations**, and
- (iii) C is the set of **constants**.

Def 3 Let $A = (S, O, C)$ be an algebra. Then

$A' = (S', O', C)$ is a **subalgebra** of A , if

i) $S' \subseteq S$ and

ii) $O' \subseteq O$, $\forall o \in O'$: o is same as **restricted** to S' .

$$(\oplus \in O' \wedge s, t \in S' \Rightarrow s \oplus t \in S')$$

Ex. 7 $(E, +, 0)$ is a **subalgebra** of $(I, +, 0)$ but $(O, +, 0)$ is not.

Def 4 Let $\oplus: S \times S \rightarrow S$.

An element $e \in S$ is an **identity(unit)** element for the operation \oplus ,

$$\text{if } e \oplus s = s \oplus e = \mathbf{s}, \forall s \in S.$$

An element $\mathbf{0} \in S$ is an **zero** element for the operation \oplus ,

$$\text{if } \mathbf{0} \oplus s = s \oplus \mathbf{0} = \mathbf{0}, \forall s \in S.$$

Exam. 9 $0 \in \mathbf{Z}$ is a **identity** element for the algebra $(\mathbf{Z}, +)$.

$0 \in \mathbf{Z}$ is a **zero** element and for the algebra (\mathbf{Z}, \times) .

$1 \in \mathbf{Z}$ is a **identity** element for the algebra (\mathbf{Z}, \times) .

Def 5 Let (S, \oplus) be an algebra,

$e_L \in S$ is a left identity element for the operation \oplus , if $e_L \oplus s = s, \forall s \in S$.

$0_L \in S$ is a left zero element for the operation \oplus , if $0_L \oplus s = 0_L, \forall s \in S$.

$e_R \in S$ is a right identity element for the operation \oplus , if $s \oplus e_R = s, \forall s \in S$.

$0_R \in S$ is a right zero element for the operation \oplus , if $s \oplus 0_R = s, \forall s \in S$.

Thm 1 Let $\oplus: S \times S \rightarrow S$ with left identity e_L and right identity e_R . Then

$e_L = e_R$ and $e = e_L = e_R$ is called as two-sided identity.

proof $e_R =_L e_L \oplus e_R =_R e_L$.

Thm 2 Let $\oplus: S \times S \rightarrow S$ with left zero 0_L and right zero 0_R . Then

$0_L = 0_R$ and $0 = 0_L = 0_R$ is called as two-sided zero.

proof $0_L =_L 0_L \oplus 0_R =_R 0_R$.

Cor 1 A two-sided identity(zero) for a binary operation is **unique**.

Def 6 Let $\oplus: S \times S \rightarrow S$ and $e \in S$ is an **identity** for the operation \oplus , if $x \oplus y = e$, then x is the left inverse of y and y is the right inverse of x w.r.t. the operation \oplus .

If both $x \oplus y = y \oplus x = e$,

x is the **inverse** of y (or two-sided inverse of y , y^{-1}) w.r.t. \oplus .

Thm. 3 If an element has both a left inverse and right inverse w.r.t. an **associative** operation $\oplus: S \times S \rightarrow S$. Then

the left and right inverse elements are **equal**.

proof Let e be an **identity** element for the op. \oplus .

Assume $x \in S$, $y \oplus x = x \oplus z = e$.

y is a left inverse of x and z is a right inverse of x .

$$\therefore y = y \oplus e = y \oplus (x \oplus z) = (y \oplus x) \oplus z = e \oplus z = z.$$

12.2 Semigroups, Monoids, and Groups

Def. 0 Algebraic System: (S, \oplus) is an algebra (or algebraic system), if

1. S is an closed w.r.t \oplus and $(\mathbb{N}_1, +)$ is an algebra

Def 1 Semigroup: (S, \oplus) is a semigroup, if

1. S is an algebraic system and $\forall x, y \in S, x \oplus y \in S.$
2. \oplus is associative operation $(\mathbb{N}_1, +)$ is a semigroup

$$(x \oplus y) \oplus z = x \oplus (y \oplus z) = x \oplus y \oplus z.$$

$$(\dots((a_1 \oplus a_2) \oplus a_3) \oplus \dots \oplus a_{n-1}) \oplus a_n \quad \text{left associative}$$

$$= a_1 \oplus (a_2 \oplus (\dots (a_{n-1} \oplus a_n) \dots)) \quad \text{right associative}$$

$$= a_1 \oplus a_2 \oplus \dots a_{n-1} \oplus a_n = \oplus a_1 a_2 \dots a_n = a_1 a_2 \dots a_n \oplus.$$

infix

prefix

postfix

$$a \oplus a \oplus \dots \oplus a = \oplus a a \dots a = a a \dots a \oplus = a^n.$$

$\oplus: S^n \rightarrow S$ \oplus is a n -ary operator ($n \geq 0$)

$$\oplus a_1 a_2 \dots a_n = \oplus_{i \in \mathbb{N}_{1,n}} a_i. \quad \text{(prefix) indexed(i) set}(\mathbb{N}_{1,n}) \text{ notation}$$

Def 2 Monoid: (S, \oplus, e) is a **monoid**, if

2. (S, \oplus) is a **semigroup** and
3. $e \in S$ is an **identity element**.

$(\mathbb{N}_1, +, ?)$ is **not a monoid!** But $(\mathbb{N}_0, +, 0)$ is a monoid.

Let V be a set of symbols called as **vocabulary**(or **alphabet**).

We define **strings** over V of length n as

$$V^0 =_B \{\lambda\}. \quad \lambda(\text{or } \varepsilon; \text{empty string}, |\lambda|=0): \forall x \in V^*: x\lambda = \lambda x = x.$$

$$V^n =_R V^{n-1}V. \quad \text{where } AB = \{ab \mid a \in A, b \in B\}$$

We define the **universe of strings** over V : V^* (all strings of length 0, 1, ...)

$$V^* = \cup_{n \in \mathbb{N}_0} V^n. \quad V^+ = \cup_{n \in \mathbb{N}_1} V^n \quad \text{strings of **positive** length}$$

We define **concatenation**(\cdot) of two strings over V .

$$\therefore V^* \times V^* \rightarrow V^* .\exists. \forall x, y \in V^*: x \cdot y = xy.$$

(V^*, \cdot, λ) is a (**free**) **monoid** generated by the **vocabulary** V .

Def 3 Group: (S, \oplus, e) is a group, if $(\mathbb{N}_0, +, 0)$ is **not** a group
 3. (S, \oplus, e) is a monoid and $(\mathbb{Z}, +, 0)$ is a group
 4. $\forall x \in S, \exists! x^{-1} \in S$ (**unique inverse**) w.r.t \oplus . \exists . $x \oplus x^{-1} = x^{-1} \oplus x = e$.

Let's define inverse of \oplus : $\oplus^{-1}: S \times S \rightarrow S$ as $\forall x, y \in S, x \oplus^{-1} y = x \oplus y^{-1}$.
 We use to denote a **group** $(S, \oplus, e, \oplus^{-1})$ instead of (S, \oplus, e)
 to specify the unique inverse x^{-1} and binary inverse operation \oplus^{-1} .

$(\mathbb{N}, +, 0, -)$ is **not** a group but $(\mathbb{Z}, +, 0, -)$ is a **group**.
 $\exists x, y \in \mathbb{N} .\exists. x - y \notin \mathbb{N}$ but $\forall x, y \in \mathbb{Z}, x - y \in \mathbb{Z}$.

Ex. 3 $R = \{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ and $\oplus: R \times R \rightarrow R$. \exists .
 $r_{\theta_1} \oplus r_{\theta_2} = r_{\theta}$ where $\theta = [\theta_1 + \theta_2]_{360}$.

$(R, \oplus, r_0, \oplus^{-1})$ is a **group**. $\oplus \leftrightarrow \oplus_6$.

\oplus : Rotate clackwise \oplus^{-1} : Rotate **count**er clockwise.

$G = (S, \oplus, e, \oplus^{-1})$ is a group, if

1. S is an **closed** w.r.t \oplus ,
 2. \oplus is **associative** operation,
 3. $e \in S$ is an **identity** element for the operation \oplus , and
 4. $\forall x \in S, \exists!$ **unique inverse** element $x^{-1} \in S$ w.r.t \oplus .
- 4.5 $\forall x, y \in S, x \oplus^{-1} y = x \oplus y^{-1}$.

Def. 3.5 Commutative (or Abelian) group

1. $(S, \oplus, e, \oplus^{-1})$ is a **group**, and
2. \oplus is **commutative**.

Ex. 4 $(\mathbf{Z}, +, 0, -)$ is a **group**. and $(\mathbf{Z}, \times, 1)$ is a **monoid**.

Consider three operations on \mathbf{Z} , \oplus_n, \oplus_n^{-1} , and \otimes_n .

$\oplus_n, \oplus_n^{-1}, \otimes_n: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}_n$ where $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$,

$a \oplus_n b = [a+b]_n$, $a \oplus_n^{-1} b = [a-b]_n$, $a \otimes_n b = [a \times b]_n$.

addi. mod. of n , **inverse of addi.,** **multi. mod. of n**

Consider a subalgebra $(\mathbf{Z}_n, \{\oplus_n, \oplus_n^{-1}, \otimes_n\}, \{0, 1\})$.

1. \mathbf{Z}_n is **closed** under \oplus_n and \otimes_n ; i.e. $\forall a, b \in \mathbf{Z}: a \oplus_n b, a \otimes_n b \in \mathbf{Z}_n$.
2. \oplus_n is **commutative** and **associative**. 0 is an **identity** of \oplus .
6. If $a \in \mathbf{Z}_n$, inverse of a w.r.t \oplus_n , $a^{-1} = n \oplus_n^{-1} a \in \mathbf{Z}_n$.
3. $(\mathbf{Z}_n, \oplus_n, 0, \oplus_n^{-1})$ is a **group**.
4. \otimes_n is **closed**, **commutative** and **associative**. 1 is an **identity** of \otimes_n .
- 4'. $a \in \mathbf{Z}_n$, $\exists a^{-1} \in \mathbf{Z}$ inverse of a w.r.t \otimes_n . $\exists. a \otimes_n a^{-1} = 1$.
- 4''. $(\mathbf{Z}_n, \otimes_n, 1)$ is a **monoid** but **not a group**.
5. \otimes_n **distributes** over \oplus_n . $a \otimes_n (b \oplus_n c) = (a \otimes_n b) \oplus_n (a \otimes_n c)$.

If $n \geq 2$, then

$(\mathbf{Z}_n, \oplus_n, 0, \oplus_n^{-1})$ is a **finite** ($n \geq 2$) **homomorphic** image of
(**Aberian**) **group** $(\mathbf{Z}, +, 0, -)$.

$(\mathbf{Z}_n, \otimes_n, 1)$ a **finite** **homomorphic** image of a **monoid** $(\mathbf{Z}, \times, 1)$.

Finite Groups

$(\{a\}, \{(a \oplus a = a)\}, a)$	a group of order 1
$(\{a, b\}, \oplus, a)$	a group of order 2
$(\{a, b, c\}, \oplus, a)$	a group of order 3
$(\{a, b, c, d\}, \oplus, a)$	two groups of order 4
$(\{a, b, c, d, e\}, \oplus, a)$??? groups of order 5

Finite Subgroup

Thm. 1 Let (T, \oplus, e) be a group and $T' \subseteq T$. If T' is **finite**, then (T', \oplus, e) is a **subgroup** of (T, \oplus, e) , if T' is **closed** under \oplus .

proof Let $a \in T'$. Then $(\oplus$ is associative and **closed**)

$$a^2, a^3, a^4, \dots, a^n, \dots \in T'.$$

Since T' is **finite**, $a^n = a^m$ for some $n, m > 0, n < m$.

$$\therefore a^n = a^n \oplus a^{m-n}, m - n > 0.$$

$e = a^{m-n}$ is an **identity** and in T' .

Two cases for **identity**, $e = a^{m-n}$, since T' is **finite**.

(2) If $m - n = 1$, $a^1 = e$,

$$\therefore a^{n+1} = a^n \oplus a^1 = a^n \oplus e = a^n = a \quad \therefore a = a \oplus a = a^2.$$

a is identity and **inverse** of a and in T' . $\therefore T' = \{a\}$.

T' is a **singleton set**.

(1) If $m - n > 1$, $a^{m-n} = a \oplus a^{m-n-1} = e$.

$\therefore a^{m-n-1}$ ($m - n - 1 > 0$) is the **inverse** of a and in T' .

$$\therefore T' = \{a^1, a^2, \dots, a^{m-n-1}, a^{m-n}, \dots, a^{m-1}\}.$$

$$|T'| \geq 2.$$

Generators for a group

Let (T, \oplus) be an algebraic system, and $S \subseteq T$.

Let $S_1 = S \cup \{a \oplus b \in A \mid a, b \in S\}$.

S_1 is called the set **generated directly** by S .

$$S_2 = S_1 \cup \{a \oplus b \in A \mid a, b \in S_1\}$$

...

$$S_{i+1} = S_i \cup \{a \oplus b \in A \mid a, b \in S_i\}$$

$$S^* = S \cup S_1 \cup S_2 \cup \dots$$

$$\therefore \forall c \in S^*, \exists a, b \in S^* . \exists. a \oplus b = c.$$

$\forall x \in S^*$, x is said to be **generated** by S .

$S^* \subseteq T$ is the **subsystem generated** by S .

(S^*, \oplus) is called the **subsystem generated** by S .

If S^* is **finite**, (S^*, \oplus) is the **subgroup**. (Theorem 12.2.1)

If $B^* = A$, B is called a **generating set** or a **set of generators** of the algebraic system (A, \oplus) .

A group that has generating consisting of a **single element** is called as a **cyclic group**.

Let (A, \oplus) be a cyclic group with generating set $\{a\}$.

$$A = \{a, a^2, a^3, \dots\}$$

$$a^i \oplus a^j = a^j \oplus a^i = a^{i+j}. \quad \text{associative}$$

\therefore Any **cyclic** group is **commutative** group

Let B be a generating set of an algebraic system (A, \oplus) .

For $a \in A$, $\exists r \geq 1$, and $a_r = a$.

$$a_1 \ a_2 \ \dots \ a_r \quad \text{generating sequence for } a \in A$$

$$1 \leq \forall i \leq r, \exists j, k < i \ .\exists. a_i = a_j \oplus a_k.$$

Example)

$(\mathbb{N}, +, 0)$ is an commutative **cyclic** group generated by $\{1\}$ with the identity 0 .

$(V^*, \cdot, \varepsilon)$ is a (**free**) **monoid** generated by V with identity ε .

Example) Consider $(I, +)$, $B = \{1\}$, and consider 9 **addition chain**

- 1 2 3 4 5 6 7 8 9 original addition chain for 9(++)
- 1 2 3 4 5 9 shorter addition chain for 9 (4+5)
- 1 2 3 5 8 9 shorter addition chain for 9(3+2, 5+3)
- 1 2 3 6 9 the shortest addition chain for 9(3+3, 3+6)

The shortest addition chain

Method 1. If $n = p \times q$.

If $p_1 p_2 \dots p_{i-1} p$ is the **shortest** addition chain(i) for p and

$q_1 q_2 \dots q_{j-1} q$ is the **shortest** addition chain(j) for q . Then

$q_1 q_2 \dots q_{j-1} q$ $q \cdot p_2 q \cdot p_3 \dots q \cdot p_{i-1} q \cdot p$ or $p_1 p_2 \dots p_{i-1} p$ $p \cdot q_2 p \cdot q_3 \dots p \cdot q_{j-1} p \cdot q$.
 the **shortest** addition chain($j+i-1 = i+j-1$) for $n=p \cdot q$

$$45 = 5 \times 9$$

$$5: \quad 1, 2, 3, 5$$

$$9: \quad 1, 2, 4, 8, 9$$

$$45: \quad 1, 2, 4, 8, 9, 18, 27, 45 \quad \text{or}$$

$$1, 2, 3, 5, 10, 20, 40, 45$$

Method 2

If n is even, determine addition chain for $n/2, n$.

If n is odd, determine addition chain for $(n-1)/2, (n-1), n$.

$$45, 44, 22, 11, 10, 5, 4, 2, 1$$

$$1, 2, 4, 5, 10, 11, 22, 44, 45$$

$$|\text{Method 2}| \leq |\text{Method 1}| + 1.$$

Method 2 is **semi optimal!**

Cosets and Lagrange's Theorem

Let (T, \oplus) be an **algebraic system**. and $H \subseteq T$. Then

Left coset of H w.r.t. $a \in T$, denoted as, $a \oplus H = \{a \oplus x \mid x \in H\}$.

Right coset of H w.r.t. $a \in T$, denoted as, $H \oplus a = \{x \oplus a \mid x \in H\}$.

Thm. 4 Let $a \oplus H$ and $H \oplus a$ be two cosets of H . Then

$$a \oplus H = H \oplus a \text{ or } a \oplus H \cap H \oplus a = \emptyset.$$

Thm. 5 (Lagrange's Theorem) The order of any **subgroup** of a **finite group** divides the order of the sybgroup.

Thm. 6 Any group of **prime order** is **cyclic** and any element other than the **identity** is a **generator**. It also follows that it is **abelian**.

Isomorphism and Automorphism

Two systems(algebra) (T, \oplus) and (S, \otimes) are **isomorphic**, if

\exists a **bijective** function $f: T \leftrightarrow S$, such that

$$\forall a, b \in T: f(a \oplus b) = f(a) \otimes f(b).$$

An **isomorphism** from (T, \oplus) to (T, \oplus) is called **automorphism**.

Permutation Group

Consider $S_3 = \{1, 2, 3\}$ be a set and a set of **bijective** mappings on S_3 .

Consider a triple (i, j, k) $i, j, k \in S_3$ and $i \neq j, j \neq k, k \neq i$,

$$(i, j, k) \leftrightarrow \{(1, i), (2, j), (3, k)\} = \{f(1) = i, f(2) = j, f(3) = k\}$$

Then there are 6 (=3!) triples,

$$P_3 = \{(1, 2, 3) (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$$

Consider **composition** of permutation $\circ: P_3 \rightarrow P_3$ s.t. $p \circ q(i) = p(q(i))$

$$\text{Ex.) } (2, 3, 1) \circ (3, 1, 2) = (1, 2, 3), (2, 3, 1) \circ (3, 2, 1) = (1, 3, 2)$$

Consider $S_n = \{1, 2, \dots, n\}$ and $P_n = \{p: S_n \leftrightarrow S_n\}$.

Then (S_n, \circ) is called as a **permutation** group of degree n .

$\circ: P_n \times P_n \rightarrow P_n$ where $p \circ q(i) = p(q(i))$;

Note that $|S_n| = n$, $|P_n| = n!$, and $|\circ| = n! \times n! = n!^2$.

Thm. 7 Any **finite** group of order n is **isomorphic** to a **permutation** group of degree n .

12.3 Homomorphisms, Normal Subgroups, and Congruence Relations

Def. 1 Let $A = (S, \oplus, c)$ and $A' = (S', \otimes, c')$ be algebra, and

$h: S \rightarrow S' \ .\exists. h(a) \oplus h(b) = h(a \otimes b), h(c) = c'$. Then

$A' = (S', \otimes, C')$ is called as a **homomorphic image** of $A = (S, \oplus, C)$.

Since we consider h that is onto, $|S'| \leq |S|$.

Def A (equivalent) congruence relation $\sim \subseteq S \times S$ where

$a \sim b$, if $h(a) = h(b) \in S'$.

(Equivalent) Congruence Class $[a]_{\sim} = h(a) \in S'$.

(Equivalent) Congruence Partition $Par_{\sim}(S) \leftrightarrow S'$.

$A' = (S', \otimes, c')$ is called as the **abstract interpretation** of $A = (S, \oplus, c)$

$A = (S, \oplus, c)$ is called as the **refinement** of $A' = (S', \otimes, c')$.

Ex. Group $(N_{n-1}, \oplus_n, 0)$ is an **abstract interpretation** of $(\mathbf{Z}, +, 0)$.

Monoid $(N_{n-1}, \otimes_n, 1)$ is an **abstract interpretations** of $(\mathbf{Z}, \times, 1)$.

Ex. Group $(\{ \text{홀}, \text{짝} \}, \oplus, \text{짝})$ is an **abstract interpretation** of $(\mathbf{Z}, +, 0)$.

Monoid $(\{ \text{홀}, \text{짝} \}, \otimes, \text{홀})$ is an **abstract interpretation** of $(\mathbf{Z}, \times, 1)$.

12.4 Rings, Integral Domain, and Fields

The operation \otimes is **distributes** over \oplus , if

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c).$$

Def. 1 Let (A, \oplus, \otimes) be an algebraic system with two operators \oplus and \otimes . Then (A, \oplus, \otimes) is called as a **ring**, if

1. (A, \oplus) is an **abelian group**,

1.5 $(A, \oplus, e, \oplus^{-1})$ is a **group**,

2. (A, \otimes) is a **semigroup**, and

3. The operation \otimes is **distributive** over \oplus .

We may use $((A, \oplus, \mathbf{0}, \oplus^{-1}, \otimes)$ to denote a **ring** instead of (A, \oplus, \otimes)

Ex. $(\mathbb{N}, +, 0, -, \times)$ is not a ring,

But $(\mathbb{Z}, +, 0, -, \times)$ and $(\mathbb{Z}_n, \oplus_n, 0, \oplus_n^{-1}, \otimes_n)$ are **rings**.

\oplus : **additive** operation of the ring

$a \oplus b$: **sum** of a and b

\otimes : **multiplicative** operation of the ring

$a \otimes b$: **multiplication** of a and b

Let $(A, \oplus, e, \oplus^{-1}, \otimes)$ is a **ring** with **additive identity** 0 .

$$\forall a \in A, 0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a)$$

$$\therefore 0 \otimes a = 0 = a \otimes 0.$$

$\therefore 0$: **multiplicative zero** as well as **additive identity**.

Def. 2 $(A, \oplus, 0, \oplus^{-1}, \otimes)$ is called an **integral domain**, if

1. $(A, \oplus, 0, \oplus^{-1}, \otimes)$ is a **ring**, and

2. (A, \otimes) is **commutative semigroup**, and

If $c \neq 0$ and $c \otimes a = c \otimes b$, then $a = b$

where 0 is the **additive identity** and/or **multiplicative zero**.

Ex. 2 Consider is set of integers \mathbf{Z} .

$(\mathbf{Z}, +, 0, -, \times)$ is the **integral domain**

Def. 3 $(A, \oplus, 0, \oplus^{-1}, \otimes, 1, \otimes^{-1})$ is called a **field**, if

1. $(A, \oplus, 0, \oplus^{-1}, \otimes)$ is a **integral domain**.

2. $(A - \{0\}, \otimes, 1, \otimes^{-1})$ is an **abelian group**.

$(A - \{0\}, \otimes, 1, \oplus^{-1})$ is a group

1: multiplicative identity

a^{-1} : multiplicative inverse of $a \in A - \{0\}$. \exists . $a \otimes a^{-1} = 1$.

$\otimes^{-1}: A \times A - \{0\} \rightarrow A$

$\forall a \in A, \forall b \in A - \{0\}: a \otimes^{-1} b = a \otimes (\otimes^{-1} b)$

multiplication of a and multiplicative inverse of b

Example)

Let \mathbf{Q} be the set of **rational** numbers. Then $(\mathbf{Q}, +, 0, -, \times, 1, /)$ is a **field**.

Let \mathbf{R} is the set of **real** numbers. Then $(\mathbf{R}, +, 0, -, \times, 1, /)$ is a **field**.

Let \mathbf{C} is the set of **complex** numbers. Then $(\mathbf{C}, +, 0, -, \times, 1, /)$ is a **field**.

Substruction is not really an **independent** operation

but it is the **addition** of the **additive inverse**.

Division is the **multiplication** of the **multiplcative inverse**.

12.5 Quotient and Product Algebras

Consider $(\mathbb{Z}_n, \oplus, \otimes)$

$a \otimes b =$ the remainder of ab divided by n .

(\mathbb{Z}_n, \oplus) is an abelian group, and \otimes is commutative

$(\mathbb{Z}_n - \{0\}, \otimes)$ is an abelian group iff n is prime.

If n is not prime, $n = ab$ for some $a, b \in \mathbb{Z}_n - \{0\}$,

But $a \otimes b = 0$ **not closed**

If n is prime,

$\forall a, b \in \mathbb{Z}_n - \{0\}, a \otimes b \neq 0 \therefore a \otimes b \in \mathbb{Z}_n - \{0\}$.

\otimes is **associative and commutative**

1 is the **identity** of \otimes .

$\forall a, b \neq c \in \mathbb{Z}_n - \{0\}, a \otimes b \neq a \otimes c$

assume $a \otimes b = a \otimes c$

$ab = kn + r, ac = ln + r$

$a(b-c) = (k-l)n$ (assume $b > c, \therefore k > l$)

Since $a, b-c < n$, and n is **prime**

$$a(b-c) \neq (k-l)n.$$

$$\therefore a \otimes b \neq a \otimes c$$

$$\therefore \forall a \in \mathbb{Z}_n - \{0\}, \exists b \in \mathbb{Z}_n - \{0\} \text{ s.t. } a \otimes b = 1.$$

$$\exists 1/a = b.$$

$\therefore (\mathbb{Z}_n - \{0\}, \oplus, \otimes)$ is a **field**.

field of integers modulus n

12.6 Coding Theory

12.7 Polynomial Rings and Polynomial Codes