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* $\oplus$,

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

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

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

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 $\oplus: S \times S \to S$ 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 $\oplus: S \times S \to S$ with left* ***zero*** *0_R 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****(or* ***zero****) for a binary operation is* ***unique****.*

Def *6 Let* $\oplus: S \times S \to S$ *and* $\boldsymbol{e} \in S$ *is an* ***identity*** *for the operation* $\oplus$*,*
if $x \oplus y = \boldsymbol{e}$*, then* x *is the* ***left inverse*** *of* y *and*
y *is the* ***right inverse*** *of* y *w.r.t. the operation* $\oplus$*.*
If both $x \oplus y = y \oplus x = \boldsymbol{e}$*,*
x *is the* ***inverse*** *(or* ***two-sided inverse****) of* y *w.r.t.* $\oplus$*, wrtitten* y^{-1}*,* $\oplus$*.*

Thm*. 3 If an element has both a left inverse and right inverse w.r.t. an* ***associative*** *operation* $\oplus: S \times S \to S$*. Then*
the left and right (or two-sided) ***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 an right* ***inverse*** *of* x*.*
$\therefore\ y = y \oplus e = y \oplus (x \oplus z) = (y \oplus x) \oplus z = e \oplus z = z$*.*
$y = z$ *is a two-sided* ***inverse*** *of* x*.*

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 a **binary** operation on $\oplus$: $S \times S \to S$.

Ex. 0. $(\aleph_1, +)$ is an algrbra. $\forall i, j \in \aleph_1,\ i+j \in \aleph_1$.

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

1. S is an **algebraic system** and $\oplus: S \times S \to S$, $\forall x,y \in S,\ x \oplus y \in S$
2. $\oplus$ is **associative** operation $(x \oplus y) \oplus z = x \oplus (y \oplus z) = x \oplus y \oplus z$.

$(\ldots((a_1 \oplus a_2) \oplus a_3) \oplus \ldots \oplus a_{n-1}) \oplus a_n$ left **associative**

$= a_1 \oplus (a_2 \oplus (\ldots (a_{n-1} \oplus a_n)\ldots))$ right **associative**

infix	**prefix**	**postfix**
$= a_1 \oplus a_2 \oplus \ldots a_{n-1} \oplus a_n$	$= \oplus a_1\ a_2 \ldots a_n$	$= a_1\ a_2 \ldots a_n \oplus$.
$a \oplus a \oplus \ldots \oplus a$	$= \oplus a\ a \ldots a$	$= a\ a \ldots a \oplus = a^n$.

$\oplus: S^n \to S$ $\oplus$ is an n-ary operator($n \geq 0$)(**associative**)

$\oplus\ a_1\ a_2 \ldots a_n = \oplus_{i \in \mathrm{N}_{1,n}} a_i$. (**prefix**) **indexed**(i) **set**($\mathrm{N}_{1,n}$) notation

*Ex. 1.1 $(\aleph_1, +)$ is a **semigroup** **generated**$(++)$ by $\{1\}$*

$2 = 1 + 1, 3 = 1 + 1 + 1, \quad \dots, n = 1 + 1 + \dots + 1, \dots$

$2 = ++(1), 3 = ++(++(1)), \quad \dots, n = ++^n(1), \quad \dots$

*Ex. 1.2 $(\Sigma^+, \cdot)$ is a **semigroup** **generated**$(\cdot)$ by a set of **symbols** in Σ(**vocabulary**, **alphabet**; a set of **symbols**).*

*We define a set of **strings** over V of **length** $n(\geq 1)$ as*

$\Sigma^n =_R \Sigma^{n-1}.\Sigma.$ $^\forall x = (a_1\cdot(a_2\cdot \dots \cdot(a_{n-1}\cdot a_n)\dots)) \in V^n, 1 \leq {}^\forall i \leq n, a_i \in V.$

or $\Sigma^n =_R \Sigma\cdot\Sigma^{n-1}.$ $^\forall x = ((\dots(a_1\cdot a_2)\cdot \dots \cdot a_{n-1})\cdot a_n) \in V^n, 1 \leq {}^\forall i \leq n, a_i \in V.$

*The length of a string x is n, written $|x| = n$. We write $x = a_1a_2\dots a_n$ (**just-taxaposed**) instead of $(a_1\cdot(a_2\cdot\dots\cdot(a_{n-1}\cdot a_n)\dots)) = ((\dots(a_1\cdot a_2)\cdot\dots\cdot a_{n-1})\cdot a_n)$*

$= (a_1 \cdot a_2 \cdot \dots \cdot a_n) = (a_1, a_2, \dots, a_n) = a_1\cdot a_2\cdot\dots\cdot a_n.$.

$\Sigma^+ = \cup_{n\in\aleph_1} \Sigma^n = \Sigma \cup \Sigma^2 \cup \dots \cup \Sigma^n \cup \dots$ ***all strings** of pos. length.*

$|\Sigma^n| = |\Sigma|^n$ *and* $|\Sigma^+| = |\Sigma| + |\Sigma|^2 + \dots + |\Sigma|^n + \dots = \aleph.$

Ex. 1.2.1 Let $\Sigma = \{a, b, \dots, z\}$. Then school$\in\Sigma^6$, boy$\in\Sigma^3$, schoolboy$\in \Sigma^9$.

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

*2. $(S, \oplus)$ is a **semigroup** and*

*3. $\mathbf{e} \in S$ is an **identity** element.*

*Ex 2.1 $(\aleph_1, +, ?)$ is **not** a monoid! But $(\aleph_0, +, 0)$ is a monoid.*

Ex 2.2 $\Sigma^0 =_B \{\lambda\}$. $\lambda \in \Sigma^0$(or ε; ***empty string***, $|\lambda| = |\varepsilon| = 0$):

$\Sigma^n =_R \Sigma^{n-1}\cdot\Sigma$. $^\forall x = a_1a_2 \dots a_{n-1}a_n \in V^n$, $1 \le {}^\forall i \le n$, $a_i \in V$.

*We define the **universe** of **strings** over Σ.*

$\Sigma^* = \cup_{n\in\aleph_0} \Sigma^n = \{\lambda\} \cup \Sigma^+$. ***universe** of strings*

*We define **concatenation**$(\cdot)$ of strings over Σ^*.*

$\cdot: \Sigma^* \times \Sigma^* \to \Sigma^*$.ə. $^\forall x, y \in \Sigma^*: x \cdot y = xy \wedge (x \cdot y) \cdot z = x \cdot (y \cdot z)$

$^\forall x \in \Sigma^*: x\cdot\lambda = \lambda\cdot x = x$. $\therefore$ λ *is an **identity** w.r.t. $\cdot$(**concatenation**).*

$|\Sigma^*| = 1 + |\Sigma^+| = \aleph$.

*$(\Sigma^*, \cdot, \lambda)$ is a (**free**) **monoid** generated by the **vocabulary** Σ.*

***Def** 3 **Group**: $(S, \oplus, e)$ is a **group**, if*

*3. $(S, \oplus, e)$ is a **monoid** and*

*4. $\forall x \in S, \exists_1 x^{-1} \in S$(**unique inverse**) w.r.t $\oplus$.ə.*

$$x \oplus x^{-1} = x^{-1} \oplus x = e.$$

$(\aleph_0, +, 0)$ is **not** a group

$(\boldsymbol{Z}, +, 0)$ is a group

*We use to denote a **group** $(S, \oplus, e, \oplus^{-1})$ instead of $(S, \oplus, e)$*

*to **specify** the **inverse binary operation** $\oplus^{-1}$ and unique **inverse** x^{-1}.*

***(**$\aleph$, +, 0, –) is **not** a group but $(\boldsymbol{Z}, +, 0, -)$ is a **group**.*

$\exists x, y \in \aleph$.ə. $x - y \notin \aleph$. *But* $\forall x, y \in \boldsymbol{Z}, x - y \in \boldsymbol{Z} \wedge \exists_1 x^{-1} (= -x) \in \boldsymbol{Z}$.

***Ex**. 3 $R = \{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ and $\oplus: R \times R \rightarrow R$.ə.*

$$r_{\theta_1} \oplus r_{\theta_2} = r_\theta \text{ where } \theta = [\theta_1 + \theta_2]_{360}.$$

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

$\oplus$: Rotate clackwise $\oplus^{-1}$*: Rotate **counter** clockwise.*

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

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

   4.5 $^{\forall}x, y \in S, x \oplus^{-1} y = x \oplus y^{-1} = e.$

Def*. 3.5* ***Commutative*** *(or* ***Abelian****)* ***group***

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

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

Consider 3 congruence of modulus n operations $\oplus_n$, $\oplus_n^{-1}$, *and* $\otimes_n$ *on* $\boldsymbol{Z}_n$.

$\oplus_n, \oplus_n^{-1}, \otimes_n : \boldsymbol{Z}_n \times \boldsymbol{Z}_n \rightarrow \boldsymbol{Z}_n$ *where* $\boldsymbol{Z}_n = \{0, 1, \ldots, n\text{-}1\}$,

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

addi*. cong. mod. of n,* ***inverse*** *of addi. of n,* ***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 $\oplus_n$, $\boldsymbol{a^{-1}} = n \oplus_{\boldsymbol{n}}^{-1} a \in \mathbf{Z}_n$.
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 $\otimes_n$.э. $a \otimes_n a^{-1} = 1$.

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**)*

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

*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 $m - n = 1$, $a^1 = e$,

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

*a is idendty 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'.*

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

$|T'| \geq 2$.

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.*

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

…

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

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

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

$\forall x \in S^*$, *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 $\{a\}$.

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

$a^i \oplus a^j = a^j \oplus a^j = a^{i+j}$. ***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 $a_r = a$.

$a_1\ a_2\ \ldots\ a_r$ ***generating sequence*** *for $a \in A$*

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

Example)
*$(\aleph, +, 0)$ 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 $p_1\ p_2 \ldots p_{i-1}\ p$ is the **shortest** addition chain(i) for p and*
*$q_1\ q_2 \ldots q_{j-1}\ q$ is the **shortest** addition chain(j) for q. Then*
$q_1\ q_2 \ldots q_{j-1}\ q\ q{\cdot}p_2\ q{\cdot}p_3 \ldots q{\cdot}p_{i-1}\ q{\cdot}p$ or $p_1\ p_2 \ldots p_{i-1}\ p\ p{\cdot}q_2\ p{\cdot}q_3 \ldots p{\cdot}q_{i-1}\ p{\cdot}q$.
*the **shortest** addition chain($j+i-1 = i+j-1$) for $n=p{\cdot}q$*

$45 = 5 \times 9$

5: 1, 2, 3, 5

9: 1, 2, 4, 8, 9

45: 1, 2, 4, 8, 9, 18, 27, 45 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, $a \oplus H = \{a \oplus x | x \in H\}$.*
Right ***coset*** *of H w.r.t. $a \in T$, denoted as, $H \oplus a = \{x \oplus a | x \in H\}$.*

Thm*. 4 Let $a \oplus H$ and $H \oplus a$ be two cosets of H. Then*
$a \oplus H = H \oplus a$ *or* $a \oplus H \cap H \oplus a = \varnothing$.

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

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 **bihective** 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.* $p \circ q(i) = p(q(i))$

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

Consider $S_n = \{1, 2, \ldots, n\}$ *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 $A = (T, \oplus, c)$ and $A' = (T', \oplus', c')$ be algebra, and

$h: T \rightarrow T'$.ə. $h(a) \oplus' h(b) = h(a \oplus b)$, $h(c) = c'$. Then

Since we consider h that is **onto**, $|T| \geq |T'|$.

A' is a **homomorphic image**(or **abstract interpretation**) of A under h.

A is calles as a **concretization**(or **refinement**) of A' under h.

Exa. 1 A **group** $(\mathbf{Z}_n, \oplus_n, 0, \oplus_n^{-1})$ and a **monoid** $(\mathbf{Z}_n, \otimes_n, 1)$ are **abstract interpretations** of the **group** $(\mathbf{Z}, +, 0, -)$ and a **monoid** $(\mathbf{Z}, \times, 1)$ under $h_n(=[]_n)$.

Exa. 2 A **group** $(\{$홀, 짝$\}, \oplus,$ 짝$, \oplus_n^{-1})$ and a **monoid** $(\{$홀, 짝$\}, \otimes,$ 홀$)$ are **abstract interpretation** of $(\mathbf{Z}, +, 0, -)$ and $(\mathbf{Z}, \times, 1)$, **respectively** under $h_2(=[]_2)$.

Exa. 2.1 The **group** $(\{$홀, 짝$\}, \oplus,$ 짝$, \oplus_n^{-1})$ and a **monoid** $(\{$홀, 짝$\}, \otimes,$ 홀$)$ are isomorphic to $(\mathbf{Z}_2 = \{0, 1\}, +, 0, -)$ and $(\mathbf{Z}_2, \times, 1)$ under $i(=[]_2)$.

where $i(0) =$ 짝 and $i(1) =$ 홀 ; $i^{-1}($ 짝 $) = 0$ and$i^{-1}($ 홀 $) = 1$.

Def. 1 *Let $(T', \oplus', c')$ be a* ***homomorphic image*** *of $(T, \oplus, c)$ under h. Then we define a congruence relation $\sim \subseteq T \times T$ under h as $a \sim b$, if $h(a) = h(b)$.*

Col. 1 *The congruence relation $\sim$ is equivalent.*

Thm *3 Let $(T', \oplus', c')$ be a* ***homomorphic image*** *of $(T, \oplus, c)$ under h and the* ***(equivalent) congruence*** *relation under h w.r.t $\oplus$ is $\sim$. Then*

$$\forall a, b \in T, a \sim b \wedge c \sim d \Leftrightarrow h(a \oplus b) = h(c \oplus d).$$

Exa. 3 *Consider a* ***group*** *$(\boldsymbol{Z}, +, 0, -)$ and its* ***homomorphic image*** *$(\boldsymbol{Z}_n, \oplus_n, 0, \oplus_n^{-1})$ under $[]_n$. Then $3 \sim n+3 \wedge 2n+5 \sim 5 \Leftrightarrow [2n+8]_n = [n+8]_n$.*

(Eqivalent) Congruence Class	$a \in T$: $[a]_\sim = [a]_h = h(a) \in T'$.
(Eqivalent) Congruence Partition	$Par_\sim(T) \leftrightarrow T'$.

12.4 Rings, Integral Domain, and Fields

*The operation ⊗ is **distributes** over ⊕, if*

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

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

1. *(A, ⊕) is an **abelian group**,*
   - *1.5 $(A, \oplus, e, \oplus^{-1})$ is a **group**,*
2. *(A, ⊗) is a **semigroup**, and*
3. *The operation ⊗ is **distributive** over ⊕.*

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

Ex. (ℵ, +, 0, −, ×) is not a ring,

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

⊕: ***additive** operation of the ring* — *a ⊕ b: **sum** of a and b*

⊗: ***multiplicative** operation of the ring* — *a ⊗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* ***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* $a \in A-\{0\}$ *.*ə*.* $a \otimes a^{-1} = 1$.

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

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

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 $\Re$ *is the set of* ***real*** *numbers. Then* $(\Re, +, 0, -, \times, 1, /)$ *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 $(Z_n, \oplus_n, \otimes_n)$

$a \oplus_n b$ = the remainder of $a+b$ divided by n.

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

$(Z_n, \oplus_n)$ is an **abelian group**, and $\otimes$ is commutative.

$(Z_n - \{0\}, \otimes_n)$ is an **abelian group** iff n is **prime**.

proof If n is not prime, $n = ab$ for some $a, b \in Z_n - \{0\}$,

But $\exists a, b \in Z_p - \{0\}, a \otimes_n b = 0$ **not closed**

If $n=p$ is prime,

$\forall a, b \in Z_p - \{0\}, a \cdot b \neq 0 \therefore a \otimes_p b \in Z_p - \{0\}$.

$\therefore \otimes_p$ **is closed** under $Z_p - \{0\}$.

$\otimes_p$ is **associative** and **commutative**

1 is the **identity** for $\otimes_p$.

If $\forall a, b \neq c \in Z_p - \{0\}$, then $a \otimes_p b \neq a \otimes_p c$.

proof *assume* $a \otimes_p b = a \otimes_p c$

$ab = kp + r,\ ac = lp + r$

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

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

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

$\therefore\ a \otimes_p b \neq a \otimes_p c$

$\therefore\ {}^{\forall}a \in Z_n-\{0\}, {}^{\exists}b \in Z_n-\{0\}$.ə. $a \otimes b = 1.$

$${}^{\exists}{}_1 1/a (= \otimes^{-1} a) = b.$$

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

field of integers modulus n

12.6 Coding Theory

12.7 Polynomial Rings and Polynomial Codes