

# Abstract Algebra Summary

Xue Leyang

March 23, 2017

## 1 The System of Natural Number

### 1.1 Product Set

**Definition 1.1.1.** The product set  $S \times T$  of two arbitrary sets  $S$  and  $T$  is a set of pairs  $(s, t)$ ,  $s \in S, t \in T$ . In general  $\prod S_i = S_1 \times S_2 \times \cdots \times S_r$  is the collection of  $r$ -tuples  $(s_1, s_2, \cdots, s_r)$ , where  $s_i \in S_i$ . If  $(s_1, s_2, \cdots, s_r)$  and  $(s'_1, s'_2, \cdots, s'_r)$  are equal, we have  $s_1 = s'_1, s_2 = s'_2, \cdots, s_r = s'_r$ .

### 1.2 Mapping

**Definition 1.2.1.** A mapping  $\alpha$  of set  $S$  onto set  $T$  if  $\forall t \in T, \exists s \in S \Rightarrow \alpha(s) = t$ , we also write the image of  $s$  in  $T$  as  $s\alpha$  or  $s^\alpha$ . The image set of  $S$  is denoted as  $S\alpha$  or  $S^\alpha$ .

If  $\alpha$  is a one-to-one mapping,  $s$  is unique for every  $t$ , and we call an inverse mapping  $\alpha^{-1}$  which is one-to-one of  $T$  onto  $S$ .

**Definition 1.2.2.** Resultant or Product of mapping is denoted as  $\alpha\beta$ , where  $\alpha$  maps set  $S$  onto set  $T$  and  $\beta$  maps set  $T$  onto set  $U$ . Mapping of  $S$  onto  $U$  can be written as  $S(\alpha\beta) = (S\alpha)\beta$ , and same for each element.

*Remark.* Mapping of a set into itself is called *transformations* of sets, including Identity mapping that leave all element in  $S$  fixed.

**Definition 1.2.3.** Identity mapping, denoted  $\mathbb{1}_S$ , its product with any transformation  $\alpha$ ,  $\mathbb{1}_S\alpha = \alpha = \alpha\mathbb{1}_S$ .

**Theorem 1.2.1.** If  $\alpha$  is a one-to-one mapping of  $S$  onto  $T$  and has inverse  $\alpha^{-1}$ , then  $\alpha\alpha^{-1} = \mathbb{1}_S$  and  $\alpha^{-1}\alpha = \mathbb{1}_T$ . Conversely, if  $\alpha : S \mapsto T$  and  $\beta : T \mapsto S$  such that  $\alpha\beta = \mathbb{1}_S$  and  $\beta\alpha = \mathbb{1}_T$ , then  $\alpha, \beta$  are one-to-one mapping and  $\beta = \alpha^{-1}$ .

**Theorem 1.2.2.** Associative law holds for the resultant of transformation of one set.

*Proof.* Suppose we have for sets  $S, T, U, V$  and  $\alpha : S \mapsto T; \beta : T \mapsto U; \gamma : U \mapsto V$ . Then  $\forall x \in S$ ,  $x((\alpha\beta)\gamma) = (x(\alpha\beta))\gamma = ((x\alpha)\beta)\gamma$  and  $x(\alpha(\beta\gamma)) = (x\alpha)(\beta\gamma) = ((x\alpha)\beta)\gamma$ , hence  $x((\alpha\beta)\gamma) = x(\alpha(\beta\gamma))$   $\square$

## 1.3 Equivalence Relations

**Definition 1.3.1.** The equivalence relation  $\sim$  of a pair of element satisfies:

1.  $a \sim a$  (reflexive property).
2.  $a \sim b \Rightarrow b \sim a$  (symmetric property)
3.  $a \sim b$  and  $b \sim c \Rightarrow a \sim c$  (transitive property)

**Definition 1.3.2.** An equivalence class

**Theorem 1.3.1.** Two equivalence classes are either identical or mutually exclusive

*Proof.* Suppose we have an equivalence class  $[a]$  of element  $a$ , if  $b \in [a]$ , then  $[b] \subseteq [a]$ ; hence by maximality of  $[b]$ , we conclude  $[b] = [a]$ .  $\square$

**Corollary 1.3.1.1.** The collection of distinct equivalence classes gives a decomposition of the set  $S$  into mutually exculsive subsets. Conversely, suppose a set  $S = \cup S_i$ , where  $S_i$  are mutually exclusive, we can define relation  $\mathcal{R}$  as  $a \sim b \iff$  subsets  $S_i, S_j$  containing  $a, b$  are identical.

**Definition 1.3.3.** The quotient set of  $S$  with equivalence relation  $\mathcal{R}$ , denoted  $S \setminus \mathcal{R}$ , is the collection of all equivalence classes in  $S$ , where  $s \mapsto [s]$  and  $S \mapsto S \setminus \mathcal{R}$ , i.e. each element maps to its equivalence class.

## 2 Semi-Groups and Groups

### 2.1 Semi-Groups

**Definition 2.1.1.** A semi-group is a system consisting of a set  $\mathfrak{S}$  and an associative binary composition in  $\mathfrak{S}$ . i.e.  $\forall a, b, c \in \mathfrak{S}$ , we have  $(ab)c = a(bc)$ .

**Definition 2.1.2.** Element  $a$  and  $b$  are said to be commute if  $ab = ba, a, b \in \mathfrak{S}$ . If it holds for any pair  $a, b$  in  $\mathfrak{S}$  then  $\mathfrak{S}$  is called commutative.

**Definition 2.1.3.** An element  $e_l \in \mathfrak{S}$  is called left identity if  $\forall a \in \mathfrak{S}, e_l a = a$ . Similarly,  $e_r$  is right identity if  $\forall a \in \mathfrak{S}, e_r a = a$ .

**Theorem 2.1.1.** If  $e_l, e_r$  both exists in  $\mathfrak{S}$ , then  $e_l = e_r$ , i.e. if two side identity exists then it is unique.

*Proof.* We have  $e_r = e_r e_l = e_l$ , from the definition of identity looking from two sides.  $\square$

**Definition 2.1.4.** A right regular(unit)  $a$  and right inverse  $a'$ , if  $a, a' \in \mathfrak{S}, aa' = e$ , two side inverse  $a^{-1}$

**Theorem 2.1.2.** If right inverse and left inverse both exists, they are identical.

*Proof.* We set  $a, a', a'' \in \mathfrak{S}$ , that  $aa' = e, a''a = e$ , conclude that  $a' = (a''a)a' = a''(aa') = a''$   $\square$

## 2.2 Groups

**Definition 2.2.1.** A group  $\mathfrak{G}$  is a semi-group that has an identity  $e$  and in which every element is a unit.

1. associativity
2. Exist  $e \in \mathfrak{G}, \forall a \in \mathfrak{G}$  such that  $ae = a = ea$
3.  $\forall a \in \mathfrak{G}$  exist  $a^{-1}$  such that  $aa^{-1} = e = a^{-1}a$

**Definition 2.2.2.**  $\forall a, b, c \in \mathfrak{G}$ , we have  $ab = ac \Rightarrow b = c$  is called left cancellation and so is right cancellation that  $\forall a, b, c \in \mathfrak{G}$ , we have  $ba = ca \Rightarrow b = c$ .

**Theorem 2.2.1.** With  $a, b \in \mathfrak{G}$ , the linear equation  $ax = b$  the only solution  $a^{-1}b$ .

*Proof.* If the solution is not unique, we set another solution to be  $x'$ , so that  $ax = ax'$ , contrasting to the result of left cancellation.  $\square$

**Theorem 2.2.2.** The only idempotent ( $\exists a \in \mathfrak{G}, a^2 = a$ ) in a group is the identity (unity).

*Proof.* From  $a \circ a = a$  we can observe  $a$  hold both the property of left and right unit, the  $a$  is a unit and unit is unique.  $\square$

**Theorem 2.2.3.** A semi-group  $\mathfrak{S}$  with left unit  $e_L$  and left inverse  $a_L^{-1}, \forall a \in \mathfrak{S}$ , then it is a group. Also with right unit and right inverse.

*Proof.* We take  $\forall a \in \mathfrak{S}, aa_L^{-1} = e_L aa_L^{-1} = [(a_L^{-1})_L^{-1} a_L^{-1}] aa_L^{-1} = (a_L^{-1})_L^{-1} (a_L^{-1} a) a_L^{-1} = e_L$   
 $ae_L = a(a_L^{-1} a) = e_L a = a$ , so that we have equivalence property of right and left.  $\square$

**Theorem 2.2.4.** If  $\mathfrak{S}$  is a semi-group and linear equation  $ya = b; ax = b, \forall a, b \in \mathfrak{S}$  is solvable, then  $\mathfrak{S}$  is a group.

*Proof.* We suppose  $e$  is the solution for equation  $ya = a, \forall a \in \mathfrak{S}$ , and that the solution for  $ax = b$  is  $g$ . Then  $eb = e(ag) = ag = b$ ,  $e$  is proved to be a left identity. Also,  $yb = e$  is always solvable, so  $\mathfrak{S}$  has right inverse and right identity, thus is a group.  $\square$

**Theorem 2.2.5.** A finite semi-group with cancellation laws hold is a group.

*Proof.* Let  $\mathfrak{S} = (a_1, a_2, \dots, a_n)$  has  $n$  distinct element, take  $a, b \in \mathfrak{S}$ , and let  $\mathfrak{T} = (aa_1, aa_2, \dots, aa_n) \Rightarrow \mathfrak{T} \subset \mathfrak{S}$  according to the self-mapping of  $\mathfrak{S}$ .  $aa_i = aa_j \Rightarrow a_i = a_j$  by cancellation law, hence  $\mathfrak{T}$  also have  $n$  distinct elements  $\Rightarrow \mathfrak{T} = \mathfrak{S}$ . So that the linear equation  $ax = b$  is solvable in  $\mathfrak{S}$ , so as  $ya = b$ .  $\square$

**Definition 2.2.3.**

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
abcdefghijklmnopqrstuvwxyz

### **3 Rings**

### **4 Fields**