Abstract Algebra Summary

Xue Leyang

March 25, 2017

1 The System of Natural Number

1.1 Prosuct Set

Definition 1.1.1. The product set $S \times T$ ofteo 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 α 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^α. The image set of S is denoted as $S\alpha$ or S^α.
If α is a one-to-one mapping, s is unique for every t, and we call a inverse mapping α^{-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 α maps set S onto set T and β 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 α, $\mathbb{1}_S\alpha = \alpha = \alpha\mathbb{1}_S$

Theorem 1.2.1. *If α is a one-to-one mapping of S onto T and has inverse α^{-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 α, β are one-to-one mapping and $\beta = \alpha^{-1}$*

Theorem 1.2.2. *Associaltive 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 (reflecive 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. We have a relation $\sim$ defined on a set S, an equivalence class is the subset of S of element b such that $b \sim a$.

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 multually exculsive subsets. Conversely, suppose a set $S = \cup S_i$, where S_i are multually 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 $S \backslash \mathcal{R}$, is the collection of all equivalence classes in S, where $s \mapsto [s]$ and $S \mapsto S \backslash \mathcal{R}$, 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. $\forall a, b, c \in \mathfrak{S}$, we have $ab = ac \Rightarrow b = c$ is called left cancellation and so is right cancellation that $\forall a, b, c \in \mathfrak{S}$, 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 $a^{-1}b$. Also $ya = b$ has solution ab^{-1}.*

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. □

Theorem 2.2.2. *The only idemponent ($\exists a \in \mathfrak{S}, a^2 = a$) 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. □

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

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 eqution $ya = a, \forall a \in \mathfrak{S}$, 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. □

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

Proof. Let $\mathfrak{S} = (a_1, a_2, \ldots, a_n)$ has n distinct element, take $a, b \in \mathfrak{S}$, and let $\mathfrak{T} = (aa_1, aa_2, \ldots, aa_n) \Rightarrow \mathfrak{T} \subset \mathfrak{S}$ 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 $ya = b$. □

2.3 Subgroups

Definition 2.3.1. If a set $\mathfrak{H}$ is a non-empty subset of (semi)group $\mathfrak{S}$ and has property

1. closure i.e. $a, b \in \mathfrak{H} \;\Rightarrow\; ab \in \mathfrak{H}$
2. Exist $e \in \mathfrak{H}$, $\forall a \in \mathfrak{H}$ such that $ae = a = ea$
3. $\forall a \in \mathfrak{H}$ exist a^{-1} such that $aa^{-1} = e = a^{-1}a$

determines a sub-(semi)group of $\mathfrak{S}$

Theorem 2.3.1. *Let $\mathfrak{H}$ to be the subgroup of $\mathfrak{G}$, the identity in $\mathfrak{G}$ is the identity in $\mathfrak{H}$, and $\forall a \in \mathfrak{H}$ the inverse in $\mathfrak{G}$ is also the inverse in $\mathfrak{H}$.*

Theorem 2.3.2. *A non-empty subset $\mathfrak{H}$ of a group $\mathfrak{G}$ is a subgroup iff $\forall a, b \in \mathfrak{H}, ab^{-1} \in \mathfrak{H}$.*

Proof. If $\mathfrak{H}$ is a subgroup, then proved from Theorem 2.2.1.
$\forall a \in \mathfrak{H}$, we have $e = aa^{-1} \in \mathfrak{H}$ and implies $a^{-1} = ea^{-1} \in \mathfrak{H}$, so that $\mathfrak{H}$ contains an element and its inverse, hence $ab = a(b^{-1})^{-1} \in \mathfrak{H}$ proves closure. □

Theorem 2.3.3. *If A is collection of any subgroup $\mathfrak{H}$ of $\mathfrak{G}$, then the intersection $\bigcap\limits_{A} \mathfrak{H}$ is a subgroup.*

Theorem 2.3.4. *The centralizer $\mathfrak{C}(S), S \subset \mathfrak{G}$ of $\mathfrak{G}$ (the set of elements of $\mathfrak{G}$ that commute with each element of S) is a subgroup of $\mathfrak{G}$*

Proof. We take $a, b \in \mathfrak{C}(S), x \in S$, so that $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \;\Rightarrow\; ab \in \mathfrak{C}(S)$. And for $\forall a \in \mathfrak{C}(S)$, we have $ax = xa \;\Rightarrow\; axa^{-1} = x \;\Rightarrow\; xa^{-1} = a^{-1}x \;\Rightarrow\; a^{-1} \in \mathfrak{C}(S)$. The identity exists, so the $\mathfrak{C}(S)$ is a subgroup of $\mathfrak{G}$. □

2.4 Isomorphism

Definition 2.4.1. Two groups $\mathfrak{G}$ and $\mathfrak{G}'$ are said to be isomorphic if there exists a 1-1 mapping $x \mapsto x'$ of $\mathfrak{G}$(Isomorphism) onto $\mathfrak{G}'$ such that $(xy)' = x'y'$. $\mathfrak{G}$ and $\mathfrak{G}'$ are said to be *abstractly equivalent*, written as $\mathfrak{G} \cong \mathfrak{G}'$.

Theorem 2.4.1. *Isomorphism is a equivalence relation (definition 1.3.1).*

Theorem 2.4.2. *If a mapping φ is an isomorphism of $\mathfrak{G}$ onto $\mathfrak{G}'$*

1. *$e \in \mathfrak{G}$ is the identity, so that $\varphi(e) = e' \in \mathfrak{G}$ is the identity of $\mathfrak{G}'$.*
2. *$a \in \mathfrak{G}$ has inverse a^{-1}, so that $\varphi(a^{-1}) = (\varphi(a))^{-1}$.*

2.5 Transformation Groups

Definition 2.5.1. For an arbitrary set S, let $\mathfrak{T}(S)$ to be semi-group of transformations (mapping) of S into itself. Generally, a transformation group (in S) is any subgroup of a group $\mathfrak{T}(S)$ in which the definition 2.2.1 holds.

Definition 2.5.2. The special case in which S is the set of n numbers, $\mathfrak{T}(S)$ is called symmetric group of degree n, donated S_n. For $\alpha \in S_n$, we write $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1\alpha & 2\alpha & \cdots & n\alpha \end{pmatrix}$ to represent the mapping order.

$\mathfrak{ABCDEFGHIJKLMNOPRSTUVXWYZ}$

$\mathfrak{abcdefghijklmnopqrstuvwxyz}$

3 Rings

4 Fields