# Abstract Algebra Summary

Xue Leyang

March 18, 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 $\alpha$ 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 a 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.** *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 $x((\alpha\beta)\gamma) = x(\alpha(\beta\gamma))$ □

### 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.** 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 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. $\square$

$\mathfrak{ABCDEFGHIJKLMNOPRSTUVWXYZ}$

$\mathfrak{abcdefghijklmnopqrstuvwxyz}$

## 3 Rings

## 4 Fields