Math 425: Abstract Algebra I
Theorems from the Textbook - Chapter 0

Notation

Symbol	Description	Example
$\mathbb{N}$	Natural Numbers	{0,1,2,3,...}
$\mathbb{Z}$	Integers	{...,-2,-1,0,1,2,3,...}
$\mathbb{Q}$	Rational Numbers	Ratios of integers
$\mathbb{R}$	Real Numbers	The standard number line
$\mathbb{C}$	Complex Numbers	$\{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1,\ \text{and } si = is\ \forall\ s \in \mathbb{R}\}$
$\in$	element of	$2 \in \{1,2,3\}$
$\subseteq$	subset of	$\{2\} \subseteq \{1,2,3\}$ and $\{1,2,3\} \subseteq \{1,2,3\}$
$\subset$ or $\subsetneq$	proper subset of	$\{2\} \subset \{1,2,3\}$ but $\{1,2,3\} \not\subset \{1,2,3\}$
$\cap$	intersection	$\{1,2,3\} \cap \{2,3,4\} = \{2,3\}$
$\cup$	union	$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$
$\times$	Cartesian product	$\{1,2\} \times \{3,4\} = \{(1,3),(1,4),(2,3),(2,4)\}$
$A \xrightarrow{\alpha} B$	mapping α from A to B	$\alpha : \mathbb{Z} \to \mathbb{R}$ defined by $\alpha(n) = e^n$ for all $n \in \mathbb{Z}$
$1_A = \mathrm{id}_A$	identity map on A	$1_A : A \to A$ is defined by $1_A(a) = a$ for all $a \in A$
$\mathrm{im}(\alpha)$	the image of the map α	Given $\alpha : \mathbb{Z} \to \mathbb{R}$ defined by $\alpha(n) = e^n$ for all $n \in \mathbb{Z}$, $\mathrm{im}(\alpha) = \{e^n : n \in \mathbb{Z}\}$
$\beta\alpha$	composition of maps	Given $\alpha : \mathbb{Z} \to \mathbb{R}$ defined by $\alpha(n) = e^n$ and $\beta : \mathbb{R} \to \mathbb{C}$ defined by $\beta(x) = \sqrt{x}$, $\beta\alpha : \mathbb{Z} \to \mathbb{C}$ is defined by $\beta\alpha(n) = \beta(\alpha(n)) = \sqrt{e^n}$.
$\equiv$	relation	for $a, b \in \mathbb{Z}$ we say $a \equiv b$ if 5 divides $a - b$
$[\cdot]$	equivalence class	for the relation just above, $[1] = \{\cdots, -4, 1, 6, 11, \dots\}$
$A_{\equiv}$	quotient of A by $\equiv$	the collection of unique equivalence classes

Theorems

Theorem 0.3.3. *Let $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D$ be mappings on sets. Then*

1. *(identity) $\alpha 1_A = \alpha$ and $1_B \alpha = \alpha$*
2. *(associativity) $\gamma(\beta\alpha) = (\gamma\beta)\alpha$*
3. *If α and β are both one-to-one (resp. onto), then $\beta\alpha$ is one-to-one (resp. onto) too.*

Theorem 0.3.4. *If $\alpha : A \to B$ has an inverse, then the inverse mapping is unique.*

Theorem 0.3.5. *Let $\alpha : A \to B$ and $\beta : B \to C$ denote mappings.*

1. *The identity map, $1_A : A \to A$ is invertible and $1_A^{-1} = 1_A$.*
2. *If α is invertible, then α^{-1} is invertible and $(\alpha^{-1})^{-1} = \alpha$.*
3. *If α and β are both invertible, then $\beta\alpha$ is invertible with $(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$.*

Theorem 0.3.6 (Invertibility Theorem)**.** *A mapping $\alpha : A \to B$ is invertible if and only if α is a bijection.*

Theorem 0.4.1. *Let $\equiv$ be an equivalence on a set A and let a and b denote elements of A. Then*

1. *$a \in [a]$ for every $a \in A$.*
2. *$[a] = [b]$ if and only if $a \equiv b$.*
3. *If $a \in [b]$, then $[a] = [b]$.*
4. *If $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.*

Theorem 0.4.2 (Partition Theorem)**.** *If $\equiv$ is any equivalence on a nonempty set A, then the collection of all equivalence classes of A under $\equiv$ partitions A.*

Definitions

Definition (Principle of Set Equality)**.** If A and B are sets, then

$$A = B \quad \text{if and only if } A \subseteq B \text{ and } B \subseteq A.$$

Definition. If A has n-elements then we say the *cardinality* of A is n and we write $|A| = n$. Such sets are called *finite* sets. Sets with an infinite number of elements are *infinite* sets.

Definition. The *power set* of a set A is the set $P(A)$ consisting of all subsets of A.

Definition. The *Cartesian Product* of the sets A and B is the set

$$A \times B := \{(a, b) : a \in A \text{ and } b \in B\}.$$

Note that the elements, (a, b), are ordered pairs.

Definition. A *mapping* or *function* α from A to B is a rule that assigns to every input $a \in A$ exactly one output $\alpha(a) \in B$. The notation here is

$$\alpha : A \to B \text{ or } A \xrightarrow{\alpha} B.$$

Once we have verified that each input maps to exactly one output then we say the mapping is *well-defined.*

Definition. Assume $\alpha : A \to B$ is a mapping.

- We call A the *domain* of α and B the *codomain* of α.
- If $C \subseteq A$, then the *image* of C is

$$f(C) = \{b \in B : b = f(c) \text{ for some } c \in C\}.$$

– The *range* of α is the image of the domain,

$$\mathrm{im}(\alpha) = f(A) = \{f(a) \in B : a \in A\}.$$

Definition. We will call two maps $\alpha : A \to B$ and $\beta : A \to B$ equal if $\alpha(a) = \beta(a)$ for all $a \in A$.

Definition. Let $\alpha : A \to B$ be a mapping.

(a) We call α *one-to-one* or *injective* if for all $a_1, a_2 \in A$ if $\alpha(a_1) = \alpha(a_2)$, then $a_1 = a_2$.

(b) We call α *onto* or *surjective* if for all $b \in B$ there is an $a \in A$ such that $\alpha(a) = b$.

(c) We call α a *bijection* or *bijective* if α is both one-to-one and onto.

Definition. The *identity map* for the set A is the map $1_A : A \to A$ defined by $1_A(a) = a$ for all $a \in A$.

If $\alpha : A \to B$ and $\beta : B \to C$ are mappings, we can write

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C,$$

and the *composition* of the maps is the mapping $\beta\alpha : A \to C$ defined by

$$\beta\alpha(a) = \beta[\alpha(a)] \text{ for all } a \in A.$$

Definition. If $\alpha : A \to B$ is a mapping of sets, then we call $\beta : B \to A$ an *inverse* of α if

$$\beta\alpha = 1_A \text{ and } \alpha\beta = 1_B.$$

Definition. If A is a set, any subset of $A \times A$ is called a *relation* on A.

Definition. A relation $\equiv$ on a set A is called an *equivalence relation* if it satisfies all of the following conditions for all $a, b, c \in A$,

1. $a \equiv a$ (*reflexivity*),

2. If $a \equiv b$ then $b \equiv a$ (*symmetric*),

3. If $a \equiv b$ and $b \equiv c$, then $a \equiv c$ (*transitive*).

Definition. An equivalence relation $\mathcal{R}$ on a set S partitions S into disjoint pieces S_i such that

$$S = S_1 \cup S_2 \cup \cdots .$$

Each S_i is called an *equivalence class* - see next definition.

We can pick any member of each class to be a *representative* of the class S_i. We denote this class by square brackets or overbar.

Definition. Given an equivalence relation $\equiv$ on a set A, we define the *equivalence class* of a to be the set

$$[a] = \{x \in A \mid x \equiv a\}.$$

Definition. Two sets are *disjoint* if their intersection is empty.

A collection of sets $\mathcal{P}$ is *pairwise disjoint* if $X \cap Y = \emptyset$ for all $X \neq Y$ in $\mathcal{P}$.

Definition. A *partition* of the set A is a collection $\mathcal{P}$ of subsets of A such that

1. $\emptyset \notin \mathcal{P}$.

2. $\mathcal{P}$ is pairwise disjoint.

3. Every element of A is in some element of $\mathcal{P}$.

Definition. The mapping $\phi : A \to A_{\equiv}$ given by $\phi(a) = [a]$ for all $a \in A$ is called the *natural mapping*.