Abstract Algebra 1 (MATH 3140)

Background on Sets, Relations, and Functions

In a rigorous mathematical theory, the definition of a new concept can involve only

- concepts that were defined earlier;
  - ∗ Note: the definitions of those concepts involve only concepts that were defined still earlier; etc.
- and a few undefined *basic concepts*
  - ∗ to make sure that 'untangling the meaning' in this step-by-step fashion terminates.

Similarly, in the proof of a new theorem we can only use rules of logic and

- theorems that were proved earlier;
  - ∗ Note: the proofs of those earlier theorems rely only theorems that were proved still earlier; etc.
- and some *axioms*, which describe our assumptions about the basic concepts.

Most of mathematics can be built up from the basic concepts 'set' and 'element' ($\in$), with the axiom system ZFC for set theory (Zermelo–Fraenkel set theory with the Axiom of Choice).[1] ZFC consists of 10 axioms/axiom schemes: 2 are statements about the nature of sets, 3 assert the existence of certain sets, and 5 are about set constructions.

The first 8 of them can be informally stated as follows:

Extensionality Axiom: Two sets are equal if they have the same elements.

The converse "If two sets are equal, they have the same elements." is true by logic.

Definitions 1.1.[2] For arbitrary sets A and B, we say that

1. *A is a subset of B*, in symbols: $A \subseteq B$, if every element of A is an element of B;
   A is a proper subset of B, in symbols: $A \subset B$ or $A \subsetneq B$, if $A \subseteq B$ but $A \neq B$.

Thus, the Extensionality Axiom together with its converse can be expressed as follows:

Theorem 1.2. *For any two sets A and B, we have*
(1) *$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Empty Set Axiom: There is a set with no elements.

By the Extensionality Axiom, there is only one such set.

Definitions 1.1.

3. This set is called *the empty set*, and is denoted by $\emptyset$.

[1] In ZFC it is assumed that every object is a set. In particular, the elements of sets are also sets.

[2] We follow the numbering used in the review version of this document. Definitions, theorems, etc. that also appear in the review version (possibly with slightly different wording) are in black.

Pairing Axiom: If A, B are sets, then $\{A, B\}$ is a set.

Union Axiom: If S is a set (of sets), then *the union* $\bigcup S = \{u : u \in X \text{ for some } X \in S\}$ *of all members of* S is a set.

In particular, if A, B are sets, then $S = \{A, B\}$ is a set by the Pairing Axiom, and hence $A \cup B = \{x : x \in A \text{ or } x \in B\}$ is a set by the Union Axiom; $A \cup B$ is called *the union of* A *and* B.[3]

Power Set Axiom: If A is a set, then *the power set* $\mathcal{P}(A) = \{X : X \subseteq A\}$ *of* A is a set.[4]

Subset Axioms: If A is a set and R is a property of sets (expressible using other sets and $\in$ only), then $\{x \in A : R(x)\}$ is a set.

The Subset Axioms imply that the 'sets' in parts 5–6. of Definition 1.1 below are indeed sets:

Definitions 1.1. Let A, B be arbitrary sets, and let S be a set of sets.

5. The *intersection of* A *and* B, denoted $A \cap B$, is the set
$$A \cap B := \{x : x \in A \text{ and } x \in B\} \left(\stackrel{!}{=} \{x \in A : x \in B\}\right),$$
and if $S \neq \emptyset$, say $A \in S$, then the *intersection* $\bigcap S$ *of all members of* S is the set
$$\bigcap S := \{u : u \in X \text{ for all } X \in S\} \left(\stackrel{!}{=} \{u \in A : u \in X \text{ for all } X \in S\}\right).$$
6. The *difference,* $A \setminus B$*, of* A *and* B is the set
$$A \setminus B := \{x \in A : x \notin B\}.$$
7. We say that A and B are *disjoint* if $A \cap B = \emptyset$.

Infinity Axiom: There exists an *inductive set*; that is, a set S (of sets) such that $\emptyset \in S$ and for every member X of S, we have that $X' := X \cup \{X\}$ (a set!) is also a member of S.

The set X' is called the *successor of* X.

Axiom of Choice: If S is a set of nonempty, pairwise disjoint sets, then there exists a set C such that $C \cap X$ has exactly one element for every $X \in S$.

1. MORE ABOUT SETS

The theorem below lists some of the familiar laws of computation for the set operations and for the relation $\subseteq$. All these laws can be proved directly from the definitions above and the Extensionality Axiom.

Theorem 1.2. *The following hold for arbitrary sets* A, B, C *and for any set* S *of sets:*

(2) $\emptyset \subseteq A$, $A \subseteq A$*; moreover, if* $A \subseteq B$ *and* $B \subseteq C$*, then* $A \subseteq C$.

[3]This remark, along with the terminology and notation intruduced in the union axiom takes care of the definition and notation for *union* that appeared in **Definition 1.1.**4 in the revision version of this document.

[4]The terminology and notation introduced here takes care of the definition and notation for *power set* that appeared in **Definition 1.1.**2 in the revision version of this document.

(3) $A \cap B = A$ *if and only if* $A \subseteq B$ *if and only if* $A \cup B = B$.

(4)

$$A \cap A = A, \qquad A \cup A = A,$$

$$A \cap B = B \cap A, \qquad A \cup B = B \cup A, \qquad (\textit{commutative laws})$$

$$(A \cap B) \cap C = A \cap (B \cap C), \qquad (A \cup B) \cup C = A \cup (B \cup C), \qquad (\textit{associative laws})$$

$$(A \cup B) \cap A = A, \qquad (A \cap B) \cup A = A,$$

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C), \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C), \qquad (\textit{distributive laws})$$

$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B), \quad C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B). \qquad (\textit{De Morgan laws})$$

(5) $(\bigcup S) \cap C = \bigcup\{X \cap C : X \in S\}, \quad (\bigcap S) \cup C = \bigcap\{X \cup C : X \in S\}.$
(general distributive laws)

To be able to define relations and functions we need the concept of an 'ordered' pair. Recall that given sets x, y, the existence of the 'unordered' pair $\{x, y\}$ is ensured by the Pairing Axiom.

Definition 1.3. For arbitrary sets x and y, the *ordered pair* (x, y) is defined to be the set $\{\{x\}, \{x, y\}\}$. (How do we know that this is a set?)

Theorem 1.4. *For arbitrary ordered pairs* (x, y) *and* (u, v) *we have that*

$$(x, y) = (u, v) \quad \textit{if and only if} \quad x = u \text{ and } y = v.$$

Definition 1.5. The *Cartesian product*, $A \times B$, of two sets A and B is defined by

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

(which can be shown to be a set, using the axioms).

2. RELATIONS AND FUNCTIONS

Definition 2.1. Let A, B, and C be sets.

1. The subsets of $A \times B$ are called *relations from* A *to* B or *assignments from* A *to* B. A relation from A to A is called a *relation on* A. If ρ is a relation on A, then we may write $a \,\rho\, b$ to indicate that $(a, b) \in \rho$.
2. If ρ is a relation from A to B and σ is a relation from B to C, then
   - the *inverse* of ρ is the relation $\rho^{-1} := \{(b, a) \in B \times A : (a, b) \in \rho\}$ from B to A, and
   - the composition of ρ and σ is the relation

     $$\sigma \circ \rho := \{(a, c) \in A \times C : \text{there exists } b \in B \text{ such that } (a, b) \in \rho \text{ and } (b, c) \in \sigma\}$$

     from A to C.

Definitions 2.2. Let A, B be sets, and let f be a relation (or assignment) from A to B. We say that f is a *function mapping* A *to* B (or a *mapping of* A *to* B), in symbols: $f \colon A \to B$, if for every $a \in A$ there exists exactly one $b \in B$ such that $(a, b) \in f$. For each $a \in A$ the unique $b \in B$ with $(a, b) \in f$ is denoted by $f(a)$ and is called *the image of* a *under* f. Instead of $(a, b) \in f$ we usually write $b = f(a)$, but we may also write $a \overset{f}{\mapsto} b$.

The set of all functions from A to B is denoted by B^A.

Definitions 2.3. Let A, B be sets and let $f\colon A \to B$. We say that

1. f is *one-to-one* (or *injective* or an *injection*) if for all distinct elements $a_1, a_2 \in A$ we have that $f(a_1) \neq f(a_2)$;
2. f is *onto* (or *surjective* or a *surjection*) if for all $b \in B$ there exists $a \in A$ such that $b = f(a)$;
3. f is *bijective* (or a *bijection*) if f is both injective and surjective.

Examples 2.4.

(1) For any set A the equality relation $\{(a, a) \in A \times A : a \in A\}$ on A is a function: $\mathrm{id}_A\colon A \to A$, $a \mapsto a$, called *the identity function on* A. Clearly, id_A is a bijection $A \to A$.
(2) For any set A, the function $A \to \mathcal{P}(A)$, $a \mapsto \{a\}$ is injective, but not surjective.
(3) For any nonempty sets A, B, the function $A \times B \to A$, $(a, b) \mapsto a$ is surjective; it is injective if and only if $B = \{b\}$ for some b.

Theorem 2.5. *Let $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$. Then*

(1) *$g \circ f$ is a function $A \to C$; namely, $g \circ f\colon A \to C$, $a \mapsto g(f(a))$.*
(2) *$h \circ (g \circ f) = (h \circ g) \circ f$; both are the function $A \to D$, $a \mapsto h(g(f(a)))$.*
(3) *$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$.*
(4) *If f, g are both injective, then so is $g \circ f$.*
If f, g are both surjective, then so is $g \circ f$.
If f, g are both bijective, then so is $g \circ f$.
(5) *If $g \circ f$ is injective, then so is f.*
If $g \circ f$ is surjective, then so is g.
If $g \circ f$ is bijective, then f is injective and g is surjective.
(6) *The relation f^{-1} from B to A is a function $B \to A$ if and only if f is a bijection.*
(7) *If f is a bijection, then*
- *f^{-1} is also a bijection, and $f = (f^{-1})^{-1}$;*
- *f^{-1} is the unique function $\varphi\colon B \to A$ satisfying the two equalities $\varphi \circ f = \mathrm{id}_A$ and $f \circ \varphi = \mathrm{id}_B$.*

(8) *If f, g are both bijections, then for the bijection $g \circ f$ (see item (4)) we have that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Definition 2.6. If $f\colon A \to B$ is a bijection, then $f^{-1}\colon B \to A$ is called *the inverse function* (or just *the inverse*) *of* f.

Definitions 2.7. Let A be a set, let ρ a relation on A, and let $\Pi \subseteq \mathcal{P}(A)$. We say that

1. ρ is *reflexive (on A)* if for all $a \in A$ we have $(a, a) \in \rho$;
2. ρ is *symmetric* if for all $(a, b) \in \rho$ we have $(b, a) \in \rho$;
3. ρ is *antisymmetric* if for all $(a, b) \in \rho$ with $a \neq b$ we have $(b, a) \notin \rho$;
4. ρ is *transitive* if for all $(a, b), (b, c) \in \rho$ we have $(a, c) \in \rho$;
5. ρ obeys the *dichotomy law* if for all $a, b \in A$ we have $(a, b) \in \rho$ or $(b, a) \in \rho$ (or both).
6. ρ is an *equivalence relation on A* if ρ is reflexive (on A), symmetric, and transitive;
7. ρ is a *partial order on A* if ρ is reflexive (on A), antisymmetric, and transitive;

8. ρ is a *linear order on* A (or *total order on* A) if ρ is a partial order on A that obeys the dichotomy law;
9. Π is a *partition of* A if
   - every member of Π is nonempty,
   - any two distinct members of Π are disjoint, and
   - $\bigcup \Pi = A$.

Examples 2.8.

(1) For any set A the equality relation $\varepsilon_A := \{(a, a) : a \in A\}$ on A is an equivalence relation as well as a partial order on A.
(2) For any set A, the relation $\subseteq$ is a partial order on $\mathcal{P}(A)$.
(3) For any function $f\colon A \to B$ the relation $\ker(f) := \{(a_1, a_2) \in A \times A : f(a_1) = f(a_2)\}$ is an equivalence relation on A.

Definition 2.9. The equivalence relation $\ker(f)$ is called *the kernel of* f.

Theorem 2.10. *Let A be a set. The following function is a bijection between the set* $\mathrm{Eq}(A)$ *of all equivalence relations on A and the set* $\mathrm{Part}(A)$ *of all partitions of A:*

$$\mathrm{Eq}(A) \to \mathrm{Part}(A), \quad \rho \mapsto A/\rho$$

where $A/\rho := \{[a]_\rho : a \in A\}$ and $[a]_\rho := \{b \in A : a \,\rho\, b\}$ is the ρ-equivalence class of a for all $a \in A$. The inverse of this function is

$$\mathrm{Part}(A) \to \mathrm{Eq}(A), \quad \Pi \mapsto \rho_\Pi$$

where $\rho_\Pi := \{(a, b) \in A \times A : a, b \in C$ for some $C \in \Pi\}$.