Abstract Algebra 1 (MATH 3140)

Background on Finite Sets and Infinite Sets

1. FINITE SETS

Now that we have introduced natural numbers, let's return to the question

What does it mean that *a set A is finite*?

Answer(s):

Example 1.1. Let

$$A = \big\{\{\emptyset\}, \mathcal{P}(\{\emptyset\}), \{\{\emptyset\}\}\big\}.$$

The theorem below can be proved by induction on n (i.e., by using the Induction Theorem).

Theorem 1.2. *Let A be a set, and let $n \in \mathbb{N}$. The following hold for every injective function $f\colon A \to n$.*

(1) *For some $m \in \mathbb{N}$,*

$$\text{there exists a bijection } A \to m. \tag{$*$}$$

(2) *For every m satisfying $(*)$ we have $m \leq n$.*
(3) *Moreover, if f is not surjective, then for every m satisfying $(*)$, we have $m < n$.*

Corollary 1.3. *Let A be a set, and let $m, n \in \mathbb{N}$.*

(1) *If $m > n$, then there is no injective function $m \to n$.*
(2) *If there exist bijections $A \to m$ and $A \to n$, then $m = n$.*
(3) *Every injective function $n \to n$ is surjective.*

Now we are ready to define what it means that 'a set is finite' and 'has n elements'.

Definition 1.4. A set A is called *finite* if there exists a bijection $A \to n$ for some natural number n. The unique such n (see Corollary 1.3(2)) is called *the number of elements* (or *the cardinality*) *of* A, and is denoted by $|A|$. A set that is not finite is called *infinite*.

So, writing $|A| = n$, where n is a natural number, means that A is a finite set which has n elements.

Corollary 1.5.

(1) *For every* $n \in \mathbb{N}$ *we have that* n *(as a set) is finite, and* $|n| = n$.
(2) *Every subset of a finite set is finite.*

Moreover, for arbitrary finite sets A *and* B*:*

(3) $|A| = |B|$ *if and only if there exists a bijection* $A \to B$.
(4) *If* $A \subseteq B$, *then* $|A| \leq |B|$.
(5) *If* $A \subseteq B$ *and* $|A| = |B|$, *then* $A = B$.
(6) *If* $|A| = |B|$ *and* f *is an injective function* $A \to B$, *then* f *is surjective (hence bijective).*
(7) *If* $A \neq \emptyset$, *then the following conditions are equivalent:*
   (i) $|A| \leq |B|$;
   (ii) *there exists an injective function* $A \to B$;
   (iii) *there exists a surjective function* $B \to A$.

Finally, the theorem below relates set operations on finite set to the arithmetic operations on the natural numbers.

Theorem 1.6. *Let A and B be finite sets.*

(1) *If $A \cap B = \emptyset$ (i.e., if A, B are disjoint), then $|A \cup B| = |A| + |B|$.*
(2) $|A \times B| = |A| \cdot |B|$.
(3) $|A^B| = |A|^{|B|}$.
(4) $|\mathcal{P}(A)| = 2^{|A|}$.

Idea of Proof. Statements (1)–(3) can be proved by induction on $n := |B|$, using the definitions of the operations on $\mathbb{N}$ (see Definition 3.1 in the lecture notes "Background on the Natural Numbers and Induction"), Corollary 1.5(3) above (possibly combined with earlier items in Theorem 1.6), and some elementary facts about the set operations involved. For example, for (3) it is useful to observe that for any element $b \in B$ the following map is a bijection:

$$A^B \to A^{B \setminus \{b\}} \times A^{\{b\}}, \quad f \mapsto (f|_{B\setminus\{b\}}, f|_{\{b\}}).$$

In more detail, this map assigns to every $f \colon B \to A$ the pair of functions $f|_{B\setminus\{b\}} \colon B \setminus \{b\} \to A$ and $f|_{\{b\}} \colon \{b\} \to A$ obtained by restricting f to the sets $B \setminus \{b\}$ and $\{b\}$, respectively. Note also that $|A^\emptyset| = 1$, because there is exactly one function $\emptyset \to A$, namely $\emptyset$.

Statement (4) follows from Theorem 1.6(3) by recalling[1] that the function

$$\mathcal{P}(A) \to 2^A \ (= \{0,1\}^A), \quad B \to \chi_B$$

is a bijection; here $\chi_B \colon A \to 2$ is *the characteristic function of* B defined for each $a \in A$ by $\chi_B(a) = 1$ if $a \in B$ and $\chi_B(a) = 0$ if $a \notin B$.

[1] If you have not seen this fact in an earlier course, take some time to prove it for yourself.

2. INFINITE SETS

Recall from Definition 1.4 that a set A is *infinite* if it is not finite, that is, if no bijection $A \to n$ exists for any natural number n.

It is intuitively clear that the set $\mathbb{N}$ of natural numbers is infinite. This fact can be deduced from Corollary 1.3(1).

Corollary 2.1 [to Corollary 1.3(1)]**.** *The set* $\mathbb{N}$ *of natural numbers is infinite.*

It follows from Corollary 1.5(2) that if for a set A there exists an injection $\mathbb{N} \to A$, then A is also infinite. Using the Axiom of Choice, one can prove that the converse of this statement is also true. Hence we get the next theorem.

Theorem 2.2 [Requires the Axiom of Choice]**.** *The following conditions on a set A are equivalent.*

(i) *A is infinite;*
(ii) *there exists an injective function* $\mathbb{N} \to A$*;*
(iii) *there exists an injective function $A \to A$ which is not surjective.*

The negations of conditions (i)–(iii) are also equivalent. Thus (i) $\Leftrightarrow$ (iii) yields the following characterization of finite sets (assuming the Axiom of Choice):

A is finite if and only if every injective function $A \to A$ is surjective.

(The forward implication here is the special case $A = B$ of Corollary 1.5(6).)

In modern set theory[2] — assuming the Axiom of Choice — the notion of natural numbers is extended to include 'infinite numbers' (special sets), called *cardinal numbers* or *cardinals*, such that

- there is a cardinal associated to every set A, called its *cardinality*, and denoted by $|A|$, so that
- for any two sets A and B, we have $|A| = |B|$ if and only if there exists a bijection $A \to B$;
- a $\leq$ relation can be defined for cardinals so that $|A| \leq |B|$ if and only if there exists an injective function $A \to B$;
- if both $|A| \leq |B|$ and $|B| \leq |A|$ hold, then $|A| = |B|$;
- for any two sets A and B we have $|A| \leq |B|$ or $|B| \leq |A|$;
- addition, multiplication, and exponention of natural numbers can be extended to cardinal numbers so that Theorem 1.6 remains valid for all sets.

By Theorem 2.2, $|\mathbb{N}|$ is the least infinite cardinal, so the following is an initial segment of the list of cardinals in increasing order:

$$0 < 1 < 2 < \cdots < n < n+1 < \cdots < |\mathbb{N}| < \ldots .$$

Sets of cardinality $|\mathbb{N}|$ are called *countably infinite*. Other examples of countably infinite sets are the set $2\mathbb{N}$ of even natural numbers, the set $\mathbb{Z}$ of integers, and the set $\mathbb{Q}$ if rational numbers.

Sets of cardinality $> |\mathbb{N}|$ (where $>$ means: $\geq$ and $\neq$) are called *uncountable.*

Cantor's Theorem. $|\mathcal{P}(A)| > |A|$ *holds for every set* A.

In particular, for the set $\mathbb{R}$ of real numbers we have $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$, so $\mathbb{R}$ is uncountable.

Another important consequence of Cantor's theorem is that there is no largest cardinal number.

[2] Founded by Georg Cantor (1845–1918).