Advanced Algebra I

Sep. 22, 2006 (Fri.)

1. Set Theory

We recall some set theory that will be frequently used in the sequel or that is not covered in the basic college course. However, we will keep this chapter as minimum as possible.

We assume the notion of "set" and some basic operation of sets without bothering their definition.

1.1. **Zorn's Lemma.**

Definition 1.1.1. *A set S is said to be* **partially ordered** *if there is a relation $\leq$ such that*

(1) *(reflexive)* $x \leq x$
(2) *(anti-symmetric) if* $x \leq y$ *and* $y \leq x$, *then* $x = y$.
(3) *(transitive) if* $x \leq y$ *and* $y \leq z$ *then* $x \leq z$.

We usually call a partially ordered set to be a POSET.

Definition 1.1.2. *A pair of elements in an POSET is said to be* **comparable** *if either $x \leq y$ or $y \leq x$. A set is said to be* **totally ordered** *(or linearly ordered) if every pair is comparable.*

We also need the following definition:

Definition 1.1.3. *A maximal element of an poset S is an element $m \in S$ such that if $m \leq x$ then $m = x$.*

Foe a given subset $T \subset S$, an upper bound of T is an element $b \in S$ such that $x \leq b$ for all $x \in T$.

One has the following

Theorem 1.1.4 (Zorn's lemma)**.** *Let S be a non-empty poset. If every non-empty totally ordered subset (usually called a "chain") has an upper bound, then there exists a maximal element in S.*

Zorn's Lemma could be taken as an axiom of set theory. It can be proved to be equivalent with the Axiom of Choice. It's also equivalent to the Well-ordering Principle. We simply give the statement of these. The reader can find the proof in most of the books on set theory.

An ordered set is said to be well-ordered if it is totally ordered and every non-empty subset B has a least element, i.e. an element $a \in B$ such that $a \leq x$ for all $x \in B$.

Theorem 1.1.5 (Well-ordered Principle)**.** *Every non-empty set can be well-ordered.*

One might wondering that $(\mathbb{Q}, \leq)$ equipped with the usual ordering is not well-ordered. So the statement says that there is another ordering which make the set $\mathbb{Q}$ well-ordered.

Example 1.1.6. *Let R be a non-zero commutative ring. One can prove that there exists a maximal ideal by using Zorn's lemma. The proof goes as following: Let $S = \{I \lhd R | I \neq R\}$ equipped with the $\subset$ as the partial ordering. $S \neq \emptyset$ because $0 \in S$. For a chain $\{I_j\}_{j \in J}$, one has a upper bound $I = \cup I_j$. Then we have a maximal element in S by Zorn's lemma. One can easily show that the maximal element corresponds to a maximal ideal.*

1.2. **cardinality.** In order to compare the "size of sets", we introduce the cardinality.

Definition 1.2.1. *Two sets A, B are said to have the same cardinality if there is a bijection between them, denoted $|A| = |B|$.*
And we say $|A| \leq |B|$ if there is a injection from A to B.

It's easy to see that the cardinality has the properties that $|A| \leq |A|$ and if $|A| \leq |B|, |B| \leq |C|$, then $|A| \leq |C|$. So It's likely that the "cardinality are partially ordered" or even totally ordered.

Lemma 1.2.2. *Given two set A, B, either $|A| \leq |B|$ or $|B| \leq |A|$.*

Sketch. Consider

$$S = \{(C, f) | C \subset A, f : C \to B \text{ is an injection}\}.$$

Apply Zorn's lemma to S, one has an maximal element (D, g), then one claim that either $D = A$ or $im(g) = B$.
We leave it as an exercise for the readers. □

Theorem 1.2.3 (Schroeder-Bernstein)**.** *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Sketch. Let $f : A \to B$ (resp. $g : B \to A$) be the given injections respectively. One needs to construct a bijection by using f and g.

Some parts of A use f and some parts not. So we consider the partition

$$A_1 := \{a \in A | a \text{ has parentless ancestor in } A\},$$
$$A_2 := \{a \in A | a \text{ has parentless ancestor in } B\},$$
$$A_3 := \{a \in A | a \text{ has infinite ancestor}\}.$$

And so does B.

Then we claim that f restricted to A_1, A_3 are bijections to B_1, B_3. And g restricted to B_2, B_3 are bijections to A_2, A_3. So the desired bijection can be constructed. □

We need some more properties of cardinality. If $|A| = |\{1, .., n\}|$, then we write $|A| = n$. And if $|A| = |\mathbb{N}|$ then we write $|A| = \aleph_0$.

Proposition 1.2.4. *If A is infinite, then $\aleph_0 \leq |A|$.*

Sketch. By Axiom of Choice. □

Definition 1.2.5.

$$|A| + |B| := |A \amalg B|,$$
$$|A| \cdot |B| := |A \times B|.$$

We have the following properties:

Proposition 1.2.6.

(1) *If $|A|$ is infinite and $|B|$ is finite, then $|A + B| = |A|$.*
(2) *If $|B| \leq |A|$ and $|A|$ is infinite, then $|A + B| = |A|$.*
(3) *If $|B| \leq |A|$ and $|A|$ is infinite, then $|A \times B| = |A|$.*

Proof. For (1), take a countable subset A_0 in A by Proposition 1.2.4. One sees that $|A_0| = |A_0| + |B|$ by shifting the index by $|B|$. Then we have

$$|A| = |A - A_0| + |A_0| = |A - A_0| + |A_0| + |B| = |A| + |B|.$$

For (2), it's enough to see that $|A + A| \leq |A|$ since clearly

$$|A| \leq |A + B| \leq |A + A|.$$

Pick an maximal subset $X \subset A$ having the property that $|X+X| \leq |X|$ by Zorn's Lemma. One claim that $A - X$ is finite, and then we are done by (1).

To see the claim, if $A-X$ is infinite, then there is a countable subset $A_0 \subset A-X$. One can construct an injective function $A \amalg X \amalg A \amalg X \to A \amalg X$ which contradicts to the maximality of X.

For (3), it suffices to show that $|A \times A| = |A|$. We sketch the proof. Let

$$S = \{(B, f) | B \text{ is an infinite subset of } A, f : B \to B \times B \text{ an bijection}\}.$$

S is non-empty because S contains an infinite countable subset. S can be equipped with natural partial ordering and by Zorn's Lemma, there exists a maximal element, say (M, g).

Let C be the complement of M in A. If $|C| \leq |M|$, then by (2), $|A| = |M|$. Hence there is a bijection $h : A \to M$. It follows that there is a bijection $A \xrightarrow{h} M \xrightarrow{G} M \times M \xrightarrow{(h^{-1}, h^{-1})} A \times A$.

Finally, if $|C| \geq |M|$, then there is a subset $M_1 \in C$ such that $|M_1| = |M|$. Let $M' = M \cup M_1$. One can construct a bijection from $M' \to M' \times M'$. This contradicts to the maximality of M. Hence we are done. □