Galois Theory (Michaelmas 2005): Handout on Zorn's lemma

a.j.scholl@dpmms.cam.ac.uk

In order to prove the existence of the algebraic closure of an arbitrary field, it is necessary to use an axiom of set theory known as *Zorn's lemma*. It is equivalent to the Axiom of Choice (but I won't prove the equivalence here: see Halmos's *Nave Set Theory* or any other book on set theory for a proof and discussion). Some believe that one should avoid the Axiom of Choice wherever possible, as it is less intuitive than the other axioms of set theory. However a lot of algebra (not to say analysis) would be very awkward without it (see Theorem A below for one reason why). If one is really concerned about its validity, it is worth pointing out that one can often avoid using Zorn's Lemma, at the expense of some notational complexity (for example, instead of the algebraic closure of a field one can often make do with the splitting field of a sufficiently large finite set of polynomials). The material in this handout (other than the statements of Zorn's Lemma and Theorem A) is not examinable.

Partial orders and Zorn's lemma

Let S be a set. A relation $\leqslant$ on S is said to be a *partial order* if it satisfies:

(i) For all $x \in S$, $x \leqslant x$;
(ii) For all $x, y, z \in S$, if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$;
(iii) For all $x, y \in S$, if $x \leqslant y$ and $y \leqslant x$ then $x = y$.

S is said to be *totally ordered* by $\leqslant$ if moreover:

(iv) For all $x, y \in S$, either $x \leqslant y$ or $y \leqslant x$.

A *chain* is a partially ordered set $(S, \leqslant)$ is a subset $T \subset S$ which is totally ordered by $\leqslant$. If $T \subset S$ is a chain then so is any subset of T.

Examples:

(a) $\mathbb{R}$ is a totally ordered set (with the usual order relation).

(b) Let $S = \{x \in \mathbb{Z} \mid x > 1\}$ ordered by reverse divisibility:

$$x \preccurlyeq y \quad \Leftrightarrow \quad x/y \in \mathbb{Z}.$$

Then $(S, \preccurlyeq)$ is a partially ordered set. Let $m > 1$ and $T = \{m^i \mid i > 1\}$. Then T is a chain in S. So is the subset $\{n! \mid n > 1\}$.

(c) Let X be any set, S the set of all subsets of X with inclusion as the order relation. Then S is a partially ordered set.

Let $(S, \leqslant)$ be a partially ordered set, and T any subset of S. An *upper bound* for T is an element $z \in S$ such that $x \leqslant z$ for all $x \in T$. (We don't require that $z \in T$.) An element $y \in S$ is said to be *maximal* if for any $x \in S$, $y \leqslant x$ iff $x = y$.
If S is totally ordered, then it can have at most one maximal element (easy). A general partially ordered set can have many maximal elements. In the above examples:

(a) In $\mathbb{R}$ an upper bound for a subset is an upper bound in the usual sense. There are no maximal elements.

(b) In $S = \{x \in \mathbb{Z} \mid x > 1\}$ an element $x \in S$ is a maximal element iff it is prime. Every chain has an upper upper bound (take the element which is smallest for the usual ordering on $\mathbb{N}$).

Zorn's Lemma. *Let S be a nonempty partially ordered set. Assume that every chain in S has an upper bound. Then S has a maximal element.*

As an example of the uses of Zorn's lemma, we prove:

Theorem A. *Let R be a ring (nonzero, with unit element). Then R has a maximal ideal.*

Proof. Let S be the set of all proper (i.e. different from R itself) ideals of R, ordered by inclusion. Since R is nonzero, $\{0\} \in S$ and so S is nonempty. The maximal elements of S are then precisely the maximal ideals of R. We need to check the hypothesis of Zorn's lemma. Let $T \subset S$ be a chain. Define $J = \bigcup_{I \in T} I$ – we claim J is an upper bound for T. The only thing which is not obvious is that $J \in S$. As J is a union of ideals, it is clearly an ideal of R. Moreover it is a proper ideal, for if not then $1 \in J$ which is true iff $1 \in I$ for some $I \in T$, which is impossible as I is a proper ideal. Therefore $J \in S$ and so J is an upper bound for T. By Zorn's lemma, S has maximal elements, hence R has maximal ideals. □

Corollary. *Let R be a ring, $I \subsetneqq R$ a proper ideal. Then there is a maximal ideal of R containing I.*

Proof. Apply Theorem A to R/I. □

Zorn's lemma is equivalent to two other axioms of Set Theory: the first of these is:

The Axiom of Choice. *Let X_i $(i \in I)$ be a collection of sets, indexed by a set I. If each X_i is nonempty then so is the Cartesian product $\prod_{i \in I} X_i$.*

The second requires a further definition. A totally ordered set is said to be *well-ordered* if every non-empty subset contains a least element. For example, the set $\mathbb{N}$ with its usual ordering is well-ordered.

The Well-Ordering Principle. *Every set can be well-ordered.*

Here is another application of Zorn's Lemma.

Theorem B. *Every vector space has a basis.*

Proof. (Sketch) Let V be a vector space. If $V = \{0\}$ there is nothing to prove, so we may assume V is nonzero. Let S be the set whose elements are the linearly independent subsets of V, ordered by inclusion. Then S is a nonempty partially ordered set. A basis of V is nothing other than a maximal element of S. One checks that if $T \subset S$ is a chain, then $\bigcup_{I \in T} I$ is also a linearly independent subset of V, hence is an upper bound for T. By Zorn's lemma we conclude. □