Zorn's Lemma (Galois Theory 2018)

pmhw@dpmms.cam.ac.uk

In order to prove the existence and uniqueness of splitting fields for arbitrary sets of polynomials in $k[X]$ over an arbitrary field k, or equivalently the existence and uniqueness of the algebraic closure of k, we shall need to assume a form of the Axiom of Choice. Note however that this is not necessary for instance when k is a subfield of the complex numbers, since we can construct the complex numbers explicitly. The form of the Axiom of Choice which is most convenient is Zorn's Lemma, which we explain below. We'll not prove that it is equivalent to the axiom of choice (which it is). You may instead assume Zorn's Lemma if it is necessary for a particular problem, but should try to avoid its use when it is unnecessary.

Partially ordered sets

A relation $\leq$ on a set S is called a *partial ordering* if

(a) $x \leq x$ for all $x \in S$,

(b) if $x \leq y$ and $y \leq z$ in S, then $x \leq z$,

(c) if $x \leq y$ and $y \leq x$ in S, then $x = y$.

For example, if S is a collection of subsets of a set X, then we can partially order S by taking $\leq$ to be inclusion.

A partial ordering $\leq$ on a set S is a *total ordering* if for any elements $x, y \in S$, either $x \leq y$ or $y \leq x$. If S is a partially ordered set, a *chain* $\mathcal{C}$ of elements of S is just a non-empty subset of S which is totally ordered in the ordering inherited from S.

If T is a subset of a partially ordered set S, an element $x \in S$ is called an *upper bound* for T if $t \leq x$ for all $t \in T$. An upper bound of T may or may not exist; if it exists, it may or may not be in T itself, and it may or may not be unique.

An element x of a partially ordered set S is called *maximal* if, whenever $x \leq y$ for some $y \in S$, we have $x = y$. A maximal element of S is not necessarily an upper bound for S, and a partially ordered set S may have many maximal elements, or none at all.

Zorn's Lemma. *If a non-empty partially ordered set S has the property that every chain $\mathcal{C}$ in S has an upper bound, then S contains at least one maximal element.*

As an example of the use of Zorn's Lemma, let us prove the (apparently innocuous) statement that any non-zero commutative ring A has a maximal ideal — this is in fact the statement we'll need in our proof of the existence of algebraic closures.

Let S denote the set of proper ideals of A, with partial order $\leq$ given by inclusion. Recall that an ideal I of A is proper iff $1 \notin I$. For any chain $\mathcal{C}$ of proper ideals, an elementary check confirms that $\bigcup\{I \in \mathcal{C}\}$ is also a proper ideal of A, and hence is an upper bound for $\mathcal{C}$. Thus S has a maximal element, which is by definition a maximal ideal of A.