NOTES: ZORN'S LEMMA AND BASES FOR VECTOR SPACES

MTH 443/543 FALL 2018

The following notes were cadged from Rotman's *Advanced Modern Algebra* and from Dummit and Foote's *Abstract Algebra*.

1. Axiom of Choice; Zorn's Lemma

What could be more reasonable than the following?

Theorem 1. The Axiom of Choice *The product of any nonempty collection of nonempty sets is nonempty.*

It is the accepted faith of most mathematicians that the Axiom of Choice is true. P. M. Cohen showed in 1964 that the consistency of the standard axioms of set theory (Zermelo-Frankel) remains unchanged if one adds the Axiom of Choice to them. (Unfortunately, we do not know if 'ZF' is consistent, only that 'ZFC' is no different with respect to this!)

Definition 1. A *partial ordering* on a nonempty set A is a relation $\preceq$ on A that is: reflexive; anti-symmetric ($x \preceq y$ and $y \preceq x$ implies that $x = y$); transitive. We say that A is *partially ordered* by a partial ordering.

You should be able to easily provide examples of partially ordered sets!

Definition 2. Let A be a nonempty set partially ordered by $\preceq$.

(1) A nonempty subset of $C \subset A$ is called a *chain* if $\forall x, y \in C$, either $x \preceq y$ or $y \preceq x$. A chain is called a *totally ordered* set.
(2) An upper bound for a subset $B \subset A$ is an element $u \in A$ such that $b \preceq u, \forall\, b \in B$.
(3) A *maximal element* of A is an element $m \in A$ such that $\forall x \in A$, if $m \preceq x$ then $x = m$.

Note that $\mathbb{R}$ with its usual partial ordering does not possess maximal elements.

Here is a very handy criterion to guarantee the existence of a maximal element.

Zorn's Lemma *If A is a nonempty partially ordered set in which every chain has an upper bound, then A has a maximal element.*

Template Almost all proofs invoking Zorn's Lemma have the following format:

(1) Define an appropriate nonempty partially ordered set;
(2) Show that all chains have upper bounds;
(3) Invoke Zorn; Show that existence of a maximal element implies result.

When checking properties of chains, the following lemma is often quite helpful.

Lemma 1. *Suppose that C is a chain in a nonempty partially ordered set, and $D \subset C$ is any* finite *subset. Then $\exists d \in D$ such that $\forall x \in D, x \preceq d$.*

Proof By induction on the cardinality of D, $n \geq 1$. The base case of $n = 1$ is obviously true.
Induction step: Suppose the lemma true for any D of cardinality $n = j$. Given $D_{j+1} = \{x_1, \ldots, x_{j+1}\}$ in C, consider $D_j = \{x_1, \ldots, x_j\}$. By our induction hypothesis, D_j admits an element x_i such that for all $x \in D_j$, $x \preceq x_i$. But, $x_i, x_{j+1} \in C$, hence either: $x_i \preceq x_{j+1}$ and we let $d = x_{j+1}$, in which case transitivity of partial ordering shows us that d does meet our conclusion; or, $x_{j+1} \preceq x_i$, and we let $d = x_i$. □

Definition 3. A *well-ordering* on a nonempty set A is a relation such that A is totally ordered and every nonempty subset of A has a minimum element.

Examples

(1) The standard ordering of $\mathbb{Z}$ is not a well-ordering. Why not?
(2) $0 \preceq -1 \preceq 1 \preceq -2 \preceq 2 \ldots$ is a well-ordering on $\mathbb{Z}$
(3) $\mathbb{N}$ is well-ordered in its usual ordering.

Well-Ordering Principle *Every nonempty set A admits a well-ordering.*

Theorem 2. *Under ZF, the following are equivalent.*

(1) *Axiom of Choice*
(2) *Zorn's Lemma*
(3) *Well-Ordering Principle*

2. Vector Space Bases

Definition 4. Let V be a vector space over a field k, and $S \subset V$ any set.

(1) S is *linearly independent* if every finite subset of S is linearly independent.
(2) S *spans* V if every vector of V can be expressed as a k-linear combination of *finitely* many elements of S.
(3) B is a *basis* of V if B both spans V and is linearly independent.

Example Consider the ring of all polynomials in one variable over k: $k[x]$. This is easily shown to be a k-vector space. Let $S = \{1, x, x^2, \dots, x^n, \dots\}$. Show that S is a basis for $k[x]$.

Theorem 3. *Every vector space V over a field k admits a basis. Furthermore, any linearly independent subset $S \subset V$ can be extended to a basis of V.*

Proof Since $\emptyset$ is linearly independent, the second statement implies the first. Thus, suppose that some linearly independent set $S \subset V$ is given. Let X be the family of all linearly independent subsets of V that contain S. Since S is in X, we have that X is nonempty. Check that inclusion of sets induces a partial ordering on X!

Now let $C = \{S_\alpha\}_{\alpha \in \mathcal{A}}$ be any nonempty chain of X. Let $S^* = \cup_{\alpha \in \mathcal{A}} S_\alpha$. Then clearly $S^* \supseteq S_\alpha$ for all S_α. We thus must only show that S^* belongs to X in order to conclude that C has an upper bound in X.

Of course, $S^* \supseteq S$. Thus, it only remains to show that S^* is linearly independent. Now, let $\{v_1, \dots, v_m\} \subset S^*$. Since S^* is the union of the S_α, for each i there is $\alpha(i) \in \mathcal{A}$ such that $v_i \in S_{\alpha(i)}$. By Lemma 1, $\exists j \in \{1, \dots, m\}$ such that $S_{\alpha(i)} \subseteq S_{\alpha(j)}$ for all $i \in \{1, \dots, m\}$. Thus, $\{v_1, \dots, v_m\} \subseteq S_{\alpha(j)}$. But, $S_{\alpha(j)}$ belongs to X and hence by definition is linearly independent. Therefore, $\{v_1, \dots, v_m\}$ is linearly independent. We have thus shown that S^* is linearly independent. Hence, C does admit an upper bound.

We now can invoke Zorn's Lemma: X has a maximal element, say B. By definition, B is linearly independent, and contains S. It suffices to show that B spans V.

Choose any nonzero vector $v \in V$; we aim to show that this is in the span of B. If $v \in B$, we are done. Thus suppose $v \notin B$, and let $B^* = B \cup \{v\}$. Clearly, $B^* \supset B$ and B^* also contains S. By the maximality of B, it follows that B^* is linearly dependent (for otherwise, $B^* \in X$ and contradicts the maximality of B).

Now, any finite subset of B is linearly independent. Of course the singleton $\{v\}$ is linearly independent. Hence there must exist some finite subset $\{v\} \cup \{b_1, \dots, b_m\} \subset B^*$ that is linearly dependent. To be precise, the zero vector can be expressed as a nontrivial linear combination of these elements in which the coefficients of v and at least one b_i being nonzero. We can then solve for v in terms of the various b_i. That is, we find that v must lie in the span of $\{b_1, \dots, b_m\}$. Thus, v lies in the span of B. We conclude that the linearly independent set B spans V, and thus B is indeed a basis. $\square$

Student suggestion: To show that B spans, suppose not and let v be an element not in the span. Then $B^* = B \cup \{v\}$ is linearly independent. But again, $B^* \supset B \supseteq S$ shows that B^* is in X and contradicts that maximality of B. From this contradiction, we find that B does span. This approach assumes the following

result: The union of any linearly independent set with a vector not in its span is still linearly independent. To prove this, you argue with linear combinations, in a way similar to the final paragraph above.