Zorn's lemma and examples of its application

Zorn's lemma is an extremely handy tool for dealing with constructions that require infinitely many steps to be done. Consider, for example, the following theorem:

Theorem 1. *Any vector space V has an (algebraic) basis* (that is, a linearly independent set of vectors such that any other vector in V is their finite linear combination).

One can try to naively prove this theorem this way: "Take a nonzero vector $v_1 \in V$. If v_1 spans V, then it forms a basis; otherwise there exists a vector $v_2 \in V$ that is linearly independent from v_1. If v_1, v_2 span V, then $\{v_1, v_2\}$ is a basis; otherwise there exists $v_3 \in V$ linearly independent from v_1, v_2. And so on, until no more linearly independent vectors remain in V. What we get is a basis of V." Of course, this argument does not work because the process described above may never end, – even after infinitely, uncountably many steps, – so that we will never get the maximal linearly independent subset of V. Zorn's lemma is designed to convert arguments like above into rigorous proofs. Here is its standard formulation:

Zorn's lemma. *Let S be a partially ordered set in which every chain has an upper bound. Then S has a maximal element.*

(Terminology: A set S is partially ordered if *a partial order* "$<$" is introduced on it, that is, for some pairs $a, b \in S$ one has $a < b$, so that it never happens that both $a < b$ and $b < a$, and so that $a < b < c$ implies $a < c$. *A chain* in S is a totally ordered subset $C \subseteq S$, which means that any two elements of S are comparable: for any distinct $a, b \in S$, either $a < b$ or $b < a$. *An upper bound* of a set $C \subseteq S$ is an element $c \in S$ such that $a \leq c$ for all $a \in C$. An element $m \in S$ is *maximal* in S if there is no $b \in S$ such that $b > m$.)

Zorn's lemma does the following: Is any chain bounded in S? Ok then, you MAY assume that you are already given a maximal chain C in S – maximal in the sense that it cannot be extended further, that is, there is no element $c \in S$ such that $c > a$ for all $a \in C$. Take an upper bound m of C (which is the maximal element of C in this case), then m is a maximal element of S.

Often the following version of Zorn's lemma applies:

Zorn's lemma 2. *Let X be a set and let $\mathcal{S}$ be a family of subsets of X such that for any chain $\mathcal{C}$ in $\mathcal{S}$ one has $\bigcup_{A \in \mathcal{S}} A \in \mathcal{S}$. Then $\mathcal{S}$ has a maximal element.*

(In this formulation, the order on $\mathcal{S}$ is given by the strict inclusion "$\subset$" relation, so that a chain in $\mathcal{S}$ is a subfamily $\mathcal{C} \subseteq \mathcal{S}$ such that for any distinct $A, B \in \mathcal{C}$ either $A \subset B$ or $B \subset A$, and M is a maximal element of $\mathcal{S}$ if there is no $B \in \mathcal{S}$ such that $M \subset B$.)

We may now prove Theorem 1:

Proof of Theorem 1. Let $\mathcal{S}$ be the family of all linearly independent subsets of V. If $\mathcal{C}$ is a chain in $\mathcal{S}$, then the set $D = \bigcup_{A \in \mathcal{C}} A$ is linearly independent. (Indeed, for any $u_1, \ldots, u_n \in D$ we have $u_i \in A_i$ for some $A_i \in \mathcal{C}$, $i = 1, \ldots, n$, and since all A_i are comparable, one of them, say A_n, contains all others; so $u_1, \ldots, u_n \in A_n$ and so, $u_1, \ldots, u_n$ are linearly independent.) Thus, $D \in \mathcal{S}$. Hence, Zorn's lemma applies to $\mathcal{S}$ and guarantees that there is a maximal linearly independent set M in V. Then M spans V; indeed, if there existed an element $v \in V$ which were not a linear combination of elements of B, then v could be added to B. Hence, M is a basis in V. ■

Here is another example:

Theorem 2. *Let R be a commutative ring with* 1*; then R has a maximal proper ideal.*

Proof. Let $\mathcal{S}$ be the set of all proper ideals in R. For any chain $\mathcal{C} \subseteq \mathcal{S}$, $J = \bigcup_{I \in \mathcal{C}} \mathcal{C} \in \mathcal{S}$. (Indeed, if $a, b \in J$, then $a \in I_1$, $b \in I_2$ for some $I_1, I_2 \in \mathcal{C}$. Assume, w.l.o.g., that $I_1 \subseteq I_2$; then $a_1, a_2 \in I_2$, so $r_1 a_1 + r_2 a_2 \in I_2 \subseteq J$ for any $r_1, r_2 \in R$. So, J is an ideal. Also, $J \neq R$ since $1 \notin I$ for all $I \in C$, so $1 \notin J$.) So, Zorn's lemma applies and says that R has a maximal ideal. ■

In the following example we use the inverse order: $A < B$ if $A \supset B$.

Theorem 3. *Let X be a compact metric space and let T be a continuous transformation of X (a continuous mapping $X \longrightarrow X$). Then there exists a minimal closed nonempty T-invariant (that is, with $T(B) \subseteq B$) subset B of X, and for such B, $T(B) = B$.*

Proof. Let $\mathcal{S}$ be the set of all closed nonempty T-invariant subsets of X. If $\mathcal{C}$ is a chain in $\mathcal{S}$, then $\bigcap_{A \in \mathcal{C}} A \in \mathcal{S}$. ($\bigcap_{A \in \mathcal{C}} A$ is T-invariant, and is nonempty by compactness.) So, by Zorn's lemma, $\mathcal{S}$ has a "maximal" element (that is, a minimal set) B. We have $T(B) \subseteq B$; if $T(B) \neq B$, then $T(B)$ is "larger" than B and is also T-invariant, contradiction. So, $T(B) = B$. ■