I.C. Posets

I.C.1. DEFINITION. A **partial order** on a set S is a relation "$\leq$" such that

$$\begin{cases} x \leq x \\ x \leq y \text{ and } y \leq z \implies x \leq z \\ x \leq y \text{ and } y \leq x \implies x = y \end{cases}$$

for all $x, y, z \in S$. The pair $(S, \leq)$ is called a **poset**.

An easy example is $(\mathscr{P}(S), \subset)$.

I.C.2. DEFINITIONS. Let $(S, \leq)$ be a poset.
(i) $(S, \leq)$ is **totally ordered** $\iff$ $x \leq y$ or $y \leq x$ ($\forall x, y \in S$).
(ii) A **chain** is a subset $\mathcal{C} \subset S$ such that $(\mathcal{C}, \leq)$ is totally ordered.
(iii) An **upper bound**[6] for a subset $S' \subset S$ is $x \in S$ such that

$$y \in S' \implies y \leq x.$$

(iv) A **maximal** element[7] of S is $x \in S$ such that

$$x \leq y \text{ and } y \in S \implies x = y.$$

I.C.3. ZORN'S LEMMA. *If every chain in S has an upper bound, then S has a maximal element.*

This is needed for:

- $\exists$ of bases for ∞-dimensional vector spaces (i.e. a linearly independent subset contained by no proper linear subspace);
- $\exists$ and ! of the algebraic closure of a field;[8]
- $\exists$ of transcendence bases for arbitrary field extensions;
- $\exists$ of maximal (proper) ideals containing a given proper ideal (for rings with uncountably many elements); and
- (in analysis) stuff like the Hahn-Banach extension.

Zorn's Lemma follows from (indeed, is equivalent to) the

[6] These need not exist or be unique in general: consider various subsets $S' \subset \mathbb{R}$ of the reals.
[7] This need *not* satisfy $y \leq x$ $\forall y \in S$, unless of course S is totally ordered.
[8] In mathematics, the symbol "!" stands for "unique" (or uniqueness, or uniquely).

I.C.4. AXIOM OF CHOICE. *Given a family of nonempty sets* $\{X_i\}_{i\in I}$*, there exists a "choice function" f defined on I such that* $f(i) \in X_i$ $(\forall i)$*. Alternately,* $\exists f$ $(= \{f(i)\}_{i\in I}) \in \prod_{i\in I} X_i$ *– that is, the Cartesian product is nonempty.*

(Clearly, this is only needed when I is infinite.) People make a fuss about using it because it renders your argument nonconstructive.

SKETCH OF PROOF THAT AOC $\implies$ ZL. Let $(S, \leq)$ be a poset in which all chains have an upper bound (write "UB"). For each $x \in S$, set

$$\varphi(x) := \{y \in S \mid y > x\} \in \mathscr{P}(S)\,,$$

and *assume no x is maximal* (i.e. no $\varphi(x) = \emptyset$). By I.C.4, there exists a choice function f on $\varphi(S)$ (a subset of $\mathscr{P}(S)$), with $f(\varphi(x)) \in \varphi(x)$. Clearly $x < f(\varphi(x))$.

Now, *fixing* $x \in S$, define a "sequence" in S by transfinite[9] recursion:

$$\begin{cases} x_0 := x, \\ x_{\alpha+1} := f(\varphi(x_\alpha)) \ (> x_\alpha) & \text{for any ordinal number } \alpha \end{cases}$$

and more generally (since this won't work for limit ordinals)

$$x_\alpha := f(\varphi(\mathrm{UB}\{x_\beta \mid \beta < \alpha\})).$$

This "goes on forever", so that $\alpha \mapsto x_\alpha$ yields an injection $\underline{\mathrm{Ord}} \hookrightarrow S$ — which is impossible because $\underline{\mathrm{Ord}}$ is not a set. □

This was just to give an idea; if you want more than that, pick up Halmos's "Naive set theory" book.

[9]There are arguments that avoid transfinite induction, but they take longer to even partially understand. You can think of an ordinal number as an isomorphism class of well-ordered sets (which are totally ordered sets each of whose subsets has a least element). The class $\underline{\mathrm{Ord}}$ of ordinal numbers is not a set – it is "too big".