SECTION 15

THE AXIOM OF CHOICE

For the deepest results about partially ordered sets we need a new set-theoretic tool; we interrupt the development of the theory of order long enough to pick up that tool.

We begin by observing that a set is either empty or it is not, and, if it is not, then, by the definition of the empty set, there is an element in it. This remark can be generalized. If X and Y are sets, and if one of them is empty, then the Cartesian product $X \times Y$ is empty. If neither X nor Y is empty, then there is an element x in X, and there is an element y in Y; it follows that the ordered pair (x, y) belongs to the Cartesian product $X \times Y$, so that $X \times Y$ is not empty. The preceding remarks constitute the cases $n = 1$ and $n = 2$ of the following assertion: if $\{X_i\}$ is a finite sequence of sets, for i in n, say, then a necessary and sufficient condition that their Cartesian product be empty is that at least one of them be empty. The assertion is easy to prove by induction on n. (The case $n = 0$ leads to a slippery argument about the empty function; the uninterested reader may start his induction at 1 instead of 0.)

The generalization to infinite families of the non-trivial part of the assertion in the preceding paragraph (necessity) is the following important principle of set theory.

Axiom of choice. *The Cartesian product of a non-empty family of non-empty sets is non-empty.*

In other words: if $\{X_i\}$ is a family of non-empty sets indexed by a non-empty set I, then there exists a family $\{x_i\}$, $i \in I$, such that $x_i \in X_i$ for each i in I.

Suppose that $\mathcal{C}$ is a non-empty collection of non-empty sets. We may regard $\mathcal{C}$ as a family, or, to say it better, we can convert $\mathcal{C}$ into an indexed set, just by using the collection $\mathcal{C}$ itself in the role of the index set and using the identity mapping on $\mathcal{C}$ in the role of the indexing. The axiom

of choice then says that the Cartesian product of the sets of $\mathcal{C}$ has at least one element. An element of such a Cartesian product is, by definition, a function (family, indexed set) whose domain is the index set (in this case $\mathcal{C}$) and whose value at each index belongs to the set bearing that index. Conclusion: there exists a function f with domain $\mathcal{C}$ such that if $A \in \mathcal{C}$, then $f(A) \in A$. This conclusion applies, in particular, in case $\mathcal{C}$ is the collection of all non-empty subsets of a non-empty set X. The assertion in that case is that there exists a function f with domain $\mathcal{P}(X) - \{\varnothing\}$ such that if A is in that domain, then $f(A) \in A$. In intuitive language the function f can be described as a simultaneous choice of an element from each of many sets; this is the reason for the name of the axiom. (A function that in this sense "chooses" an element out of each non-empty subset of a set X is called a *choice function* for X.) We have seen that if the collection of sets we are choosing from is finite, then the possibility of simultaneous choice is an easy consequence of what we knew before the axiom of choice was even stated; the role of the axiom is to guarantee that possibility in infinite cases.

The two consequences of the axiom of choice in the preceding paragraph (one for the power set of a set and the other for more general collections of sets) are in fact just reformulations of that axiom. It used to be considered important to examine, for each consequence of the axiom of choice, the extent to which the axiom is needed in the proof of the consequence. An alternative proof without the axiom of choice spelled victory; a converse proof, showing that the consequence is equivalent to the axiom of choice (in the presence of the remaining axioms of set theory) meant honorable defeat. Anything in between was considered exasperating. As a sample (and an exercise) we mention the assertion that every relation includes a function with the same domain. Another sample: if $\mathcal{C}$ is a collection of pairwise disjoint non-empty sets, then there exists a set A such that $A \cap C$ is a singleton for each C in $\mathcal{C}$. Both these assertions are among the many known to be equivalent to the axiom of choice.

As an illustration of the use of the axiom of choice, consider the assertion that if a set is infinite, then it has a subset equivalent to ω. An informal argument might run as follows. If X is infinite, then, in particular, it is not empty (that is, it is not equivalent to 0); hence it has an element, say x_0. Since X is not equivalent to 1, the set $X - \{x_0\}$ is not empty; hence it has an element, say x_1. Repeat this argument ad infinitum; the next step, for instance, is to say that $X - \{x_0, x_1\}$ is not empty, and, therefore, it has an element, say x_2. The result is an infinite sequence $\{x_n\}$ of distinct elements of X; q.e.d. This sketch of a proof at least has the virtue of being

honest about the most important idea behind it; the act of choosing an element from a non-empty set was repeated infinitely often. The mathematician experienced in the ways of the axiom of choice will often offer such an informal argument; his experience enables him to see at a glance how to make it precise. For our purposes it is advisable to take a longer look.

Let f be a choice function for X; that is, f is a function from the collection of all non-empty subsets of X to X such that $f(A) \in A$ for all A in the domain of f. Let $\mathcal{C}$ be the collection of all finite subsets of X. Since X is infinite, it follows that if $A \in \mathcal{C}$, then $X - A$ is not empty, and hence that $X - A$ belongs to the domain of f. Define a function g from $\mathcal{C}$ to $\mathcal{C}$ by writing $g(A) = A \cup \{f(X - A)\}$. In words: $g(A)$ is obtained by adjoining to A the element that f chooses from $X - A$. We apply the recursion theorem to the function g; we may start it rolling with, for instance, the set $\varnothing$. The result is that there exists a function U from ω into $\mathcal{C}$ such that $U(0) = \varnothing$ and $U(n^+) = U(n) \cup \{f(X - U(n))\}$ for every natural number n. Assertion: if $v(n) = f(X - U(n))$, then v is a one-to-one correspondence from ω to X, and hence, indeed, ω is equivalent to some subset of X (namely the range of v). To prove the assertion, we make a series of elementary observations; their proofs are easy consequences of the definitions. First: $v(n) \in' U(n)$ for all n. Second: $v(n) \in U(n^+)$ for all n. Third: if n and m are natural numbers and $n \leqq m$, then $U(n) \subset U(m)$. Fourth: if n and m are natural numbers and $n < m$, then $v(n) \neq v(m)$. (Reason: $v(n) \in U(m)$ but $v(m) \in' U(m)$.) The last observation implies that v maps distinct natural numbers onto distinct elements of X; all we have to remember is that of any two distinct natural numbers one of them is strictly smaller than the other.

The proof is complete; we know now that every infinite set has a subset equivalent to ω. This result, proved here not so much for its intrinsic interest as for an example of the proper use of the axiom of choice, has an interesting corollary. The assertion is that a set is infinite if and only if it is equivalent to a proper subset of itself. The "if" we already know; it says merely that a finite set cannot be equivalent to a proper subset. To prove the "only if," suppose that X is infinite, and let v be a one-to-one correspondence from ω into X. If x is in the range of v, say $x = v(n)$, write $h(x) = v(n^+)$; if x is not in the range of v, write $h(x) = x$. It is easy to verify that h is a one-to-one correspondence from X into itself. Since the range of h is a proper subset of X (it does not contain $v(0)$), the proof of the corollary is complete. The assertion of the corollary was used by Dedekind as the very definition of infinity.

SECTION 16

ZORN'S LEMMA

An existence theorem asserts the existence of an object belonging to a certain set and possessing certain properties. Many existence theorems can be formulated (or, if need be, reformulated) so that the underlying set is a partially ordered set and the crucial property is maximality. Our next purpose is to state and prove the most important theorem of this kind.

Zorn's lemma. *If X is a partially ordered set such that every chain in X has an upper bound, then X contains a maximal element.*

DISCUSSION. Recall that a chain is a totally ordered set. By a chain "in X" we mean a subset of X such that the subset, considered as a partially ordered set on its own right, turns out to be totally ordered. If A is a chain in X, the hypothesis of Zorn's lemma guarantees the existence of an upper bound for A in X; it does not guarantee the existence of an upper bound for A in A. The conclusion of Zorn's lemma is the existence of an element a in X with the property that if $a \leqq x$, then necessarily $a = x$.

The basic idea of the proof is similar to the one used in our preceding discussion of infinite sets. Since, by hypothesis, X is not empty, it has an element, say x_0. If x_0 is maximal, stop here. If it is not, then there exists an element, say x_1, strictly greater than x_0. If x_1 is maximal, stop here; otherwise continue. Repeat this argument ad infinitum; ultimately it must lead to a maximal element.

The last sentence is probably the least convincing part of the argument; it hides a multitude of difficulties. Observe, for instance, the following possibility. It could happen that the argument, repeated ad infinitum, leads to a whole infinite sequence of non-maximal elements; what are we to do in that case? The answer is that the range of such an infinite sequence is a chain in X, and, consequently, has an upper bound; the thing to do is to start the whole argument all over again, beginning with that

upper bound. Just exactly when and how all this comes to an end is obscure, to say the least. There is no help for it; we must look at the precise proof. The structure of the proof is an adaptation of one originally given by Zermelo.

PROOF. The first step is to replace the abstract partial ordering by the inclusion order in a suitable collection of sets. More precisely, we consider, for each element x in X, the weak initial segment $\bar{s}(x)$ consisting of x and all its predecessors. The range $\mathcal{S}$ of the function $\bar{s}$ (from X to $\mathcal{P}(X)$) is a certain collection of subsets of X, which we may, of course, regard as (partially) ordered by inclusion. The function $\bar{s}$ is one-to-one, and a necessary and sufficient condition that $\bar{s}(x) \subset \bar{s}(y)$ is that $x \leqq y$. In view of this, the task of finding a maximal element in X is the same as the task of finding a maximal set in $\mathcal{S}$. The hypothesis about chains in X implies (and is, in fact, equivalent to) the corresponding statement about chains in $\mathcal{S}$.

Let $\mathfrak{X}$ be the set of all chains in X; every member of $\mathfrak{X}$ is included in $\bar{s}(x)$ for some x in X. The collection $\mathfrak{X}$ is a non-empty collection of sets, partially ordered by inclusion, and such that if $\mathcal{C}$ is a chain in $\mathfrak{X}$, then the union of the sets in $\mathcal{C}$ (i.e., $\bigcup_{A \in \mathcal{C}} A$) belongs to $\mathfrak{X}$. Since each set in $\mathfrak{X}$ is dominated by some set in $\mathcal{S}$, the passage from $\mathcal{S}$ to $\mathfrak{X}$ cannot introduce any new maximal elements. One advantage of the collection $\mathfrak{X}$ is the slightly more specific form that the chain hypothesis assumes; instead of saying that each chain $\mathcal{C}$ has some upper bound in $\mathcal{S}$, we can say explicitly that the union of the sets of $\mathcal{C}$, which is clearly an upper bound of $\mathcal{C}$, is an element of the collection $\mathfrak{X}$. Another technical advantage of $\mathfrak{X}$ is that it contains all the subsets of each of its sets; this makes it possible to enlarge non-maximal sets in $\mathfrak{X}$ slowly, one element at a time.

Now we can forget about the given partial order in X. In what follows we consider a non-empty collection $\mathfrak{X}$ of subsets of a non-empty set X, subject to two conditions: every subset of each set in $\mathfrak{X}$ is in $\mathfrak{X}$, and the union of each chain of sets in $\mathfrak{X}$ is in $\mathfrak{X}$. Note that the first condition implies that $\varnothing \in \mathfrak{X}$. Our task is to prove that there exists in $\mathfrak{X}$ a maximal set.

Let f be a choice function for X, that is, f is a function from the collection of all non-empty subsets of X to X such that $f(A) \in A$ for all A in the domain of f. For each set A in $\mathfrak{X}$, let $\hat{A}$ be the set of all those elements x of X whose adjunction to A produces a set in $\mathfrak{X}$; in other words, $\hat{A} = \{x \in X: A \cup \{x\} \in \mathfrak{X}\}$. Define a function g from $\mathfrak{X}$ to $\mathfrak{X}$ as follows: if $\hat{A} - A \neq \varnothing$, then $g(A) = A \cup \{f(\hat{A} - A)\}$; if $\hat{A} - A = \varnothing$, then $g(A) = A$. It follows from the definition of $\hat{A}$ that $\hat{A} - A = \varnothing$ if and only if A is maximal. In these terms, therefore, what we must prove is that there exists in $\mathfrak{X}$ a set A such that $g(A) = A$. It turns out that the crucial prop-

erty of g is the fact that $g(A)$ (which always includes A) contains at most one more element than A.

Now, to facilitate the exposition, we introduce a temporary definition. We shall say that a subcollection $\mathfrak{I}$ of $\mathfrak{X}$ is a *tower* if

(i) $\varnothing \in \mathfrak{I}$,

(ii) *if* $A \in \mathfrak{I}$, *then* $g(A) \in \mathfrak{I}$,

(iii) *if* $\mathfrak{C}$ *is a chain in* $\mathfrak{I}$, *then* $\bigcup_{A \in \mathfrak{C}} A \in \mathfrak{I}$.

Towers surely exist; the whole collection $\mathfrak{X}$ is one. Since the intersection of a collection of towers is again a tower, it follows, in particular, that if $\mathfrak{I}_0$ is the intersection of all towers, then $\mathfrak{I}_0$ is the smallest tower. Our immediate purpose is to prove that the tower $\mathfrak{I}_0$ is a chain.

Let us say that a set C in $\mathfrak{I}_0$ is *comparable* if it is comparable with every set in $\mathfrak{I}_0$; this means that if $A \in \mathfrak{I}_0$, then either $A \subset C$ or $C \subset A$. To say that $\mathfrak{I}_0$ is a chain means that all the sets in $\mathfrak{I}_0$ are comparable. Comparable sets surely exist; $\varnothing$ is one of them. In the next couple of paragraphs we concentrate our attention on an arbitrary but temporarily fixed comparable set C.

Suppose that $A \in \mathfrak{I}_0$ and A is a proper subset of C. Assertion: $g(A) \subset C$. The reason is that since C is comparable, either $g(A) \subset C$ or C is a proper subset of $g(A)$. In the latter case A is a proper subset of a proper subset of $g(A)$, and this contradicts the fact that $g(A) - A$ cannot be more than a singleton.

Consider next the collection $\mathfrak{U}$ of all those sets A in $\mathfrak{I}_0$ for which either $A \subset C$ or $g(C) \subset A$. The collection $\mathfrak{U}$ is somewhat smaller than the collection of sets in $\mathfrak{I}_0$ comparable with $g(C)$; indeed if $A \in \mathfrak{U}$, then, since $C \subset g(C)$, either $A \subset g(C)$ or $g(C) \subset A$. Assertion: $\mathfrak{U}$ is a tower. Since $\varnothing \subset C$, the first condition on towers is satisfied. To prove the second condition, i.e., that if $A \in \mathfrak{U}$, then $g(A) \in \mathfrak{U}$, split the discussion into three cases. First: A is a proper subset of C. Then $g(A) \subset C$ by the preceding paragraph, and therefore $g(A) \in \mathfrak{U}$. Second: $A = C$. Then $g(A) = g(C)$, so that $g(C) \subset g(A)$, and therefore $g(A) \in \mathfrak{U}$. Third: $g(C) \subset A$. Then $g(C) \subset g(A)$, and therefore $g(A) \in \mathfrak{U}$. The third condition on towers, i.e., that the union of a chain in $\mathfrak{U}$ belongs to $\mathfrak{U}$, is immediate from the definition of $\mathfrak{U}$. Conclusion: $\mathfrak{U}$ is a tower included in $\mathfrak{I}_0$, and therefore, since $\mathfrak{I}_0$ is the smallest tower, $\mathfrak{U} = \mathfrak{I}_0$.

The preceding considerations imply that for each comparable set C the set $g(C)$ is comparable also. Reason: given C, form $\mathfrak{U}$ as above; the fact that $\mathfrak{U} = \mathfrak{I}_0$ means that if $A \in \mathfrak{I}_0$, then either $A \subset C$ (in which case $A \subset g(C)$) or $g(C) \subset A$.

We now know that $\varnothing$ is comparable and that g maps comparable sets onto comparable sets. Since the union of a chain of comparable sets is comparable, it follows that the comparable sets (in $\mathfrak{I}_0$) constitute a tower, and hence that they exhaust $\mathfrak{I}_0$; this is what we set out to prove about $\mathfrak{I}_0$.

Since $\mathfrak{I}_0$ is a chain, the union, say A, of all the sets in $\mathfrak{I}_0$ is itself a set in $\mathfrak{I}_0$. Since the union includes all the sets in $\mathfrak{I}_0$, it follows that $g(A) \subset A$. Since always $A \subset g(A)$, it follows that $A = g(A)$, and the proof of Zorn's lemma is complete.

EXERCISE. Zorn's lemma is equivalent to the axiom of choice. [Hint for the proof: given a set X, consider functions f such that $\operatorname{dom} f \subset \mathcal{P}(X)$, $\operatorname{ran} f \subset X$, and $f(A) \in A$ for all A in $\operatorname{dom} f$; order these functions by extension, use Zorn's lemma to find a maximal one among them, and prove that if f is maximal, then $\operatorname{dom} f = \mathcal{P}(X) - \{\varnothing\}$.] Consider each of the following statements and prove that they too are equivalent to the axiom of choice. (i) Every partially ordered set has a maximal chain (i.e., a chain that is not a proper subset of any other chain). (ii) Every chain in a partially ordered set is included in some maximal chain. (iii) Every partially ordered set in which each chain has a least upper bound has a maximal element.