MA651 Topology. Lecture 2. Elements of Set Theory 2.

This text is based on the following books:

- *"Topology" by James Dugundgji*
- *"Introduction to real analysis" by A.N. Kolmogorov and S.V. Fomin*
- *"Introduction to set theory" by K. Hrbacek and T. Jech*

I have intentionally made several mistakes in this text. The first homework assignment is to find them.

10 Ordering

Certain types of binary relations are called ordering.

Definition 10.1. A binary relation R in a set A is called an *preorder* relation if it is reflexive and transitive; that is, if:

1. $\forall a \in A : aRa$ (reflexive)
2. $(aRb) \wedge (bRc) \Rightarrow (aRc)$ (transitive).

A set together with a definite preorder is called a preordered set.

We denote preorder R by $\prec$; $a \prec b$ is read "a precedes b", or b follows a. A preordered set A will also be written $(A, \prec)$ whenever it is necessary to indicate explicitly the preorder being used. If A is preordered and $B \subset A$, the induced relation on B is clearly a preordering; when we consider B itself as a preordered set, it will always be with the induced preordering.

Example 10.1. *In any set A, the relation $\{(a, b) \mid a = b\}$ is preordering. Note that we do* not *require each pair of elements $a, b \in A$ to be related; that is, to satisfy either $a \prec b$ or $b \prec a$.*

Example 10.2. *In E^1 (Euclidean line), the relation $\{(x, y) \mid x \leq y\}$ is a preordering, whereas $\{(x, y) \mid x < y\}$ is not.*

Example 10.3. *Let C be the set of complex numbers, and define $z_1 \prec z_2$ if and only if $|z_1| \leq |z_2|$. This is a preordering on C. Observe that we do* not *require that $(a \prec b) \wedge (b \prec a)$ imply $a = b$.*

Example 10.4. *In $\mathscr{P}(X)$, the relation $A \prec B$, defined by $A \prec B$ if and only if $A \subset B$, is a preordering. More generally, any family of sets preordered in this matter is said to be* preordered by inclusion.

There is a standard terminology pertaining to preordered sets:

Definition 10.2. Let $(A, \prec)$ be preordered:

1. $m \in A$ is called a maximal element in A if $\forall a : m \prec a \Rightarrow a \prec m$; that is, if neither no $a \in A$ follows m or each a that follows m also precedes m.

2. $a_0 \in A$ is called as upper bound for a subset $B \subset A$ if $\forall b \in B : b \prec a_0$.

3. $B \subset A$ is called a *chain* in A if each two elements in B are related

Example 10.5. *In Example (10.1), each element is maximal. No subset of A containing at least two elements has an upper bound. Thus a maximal element in A need not be an upper bound for A.*

Example 10.6. *In Example (10.2), there is no maximal element. Every bounded set has many upper bounds.*

Example 10.7. *In Example (10.3), $a_0 = 1$ is an upper bound for $B = \{z \mid |z| \leq 1\} \subset C$, but is not maximal in C. Note also that although a_0 is an upper bound for B, it is possible for some $b \in B$ also to satisfy $a_0 \prec b$. In the set B (with induced preorder!) each z with $|z| = 1$ is both maximal and upper bound for B.*

Placing additional requirements on preorderings gives other types of ordering relations.

Definition 10.3. A preordering in A with the additional property

$$(a \prec b) \wedge (b \prec a) \Rightarrow (a = b) \text{ (antisymmetry)}$$

is called a *partial ordering*. A set together with a definite partial ordering is called a partially ordered set. A partially ordered set that is also a chain is called a *totally ordered set*.

It is evident that partial (total) orders induce partial (total) orders on subsets.

Example 10.8. *Ordering by inclusion in $\mathscr{P}(X)$, or any family of sets, is always a partial ordering (but, clearly, need not be a total order).*

Example 10.9. *Let $(A, \prec)$ be a preordered set, and define a relation S in A by $aSb \Leftrightarrow (a \prec b) \wedge (b \prec a)$. It is easy to verify that S is an equivalence relation and that A/S is partially ordered by $Sa \prec Sb \Leftrightarrow a \prec b$.*

Note that in a partially ordered A, the statement "m is maximal" is equivalent to "each $a \in A$ is either not related to m or satisfies only $a \prec m$", and also that if a_0 is an upper bound for $B \subset A$, then there can be no $b \in B - \{a_0\}$ with $a_0 \prec b$.

Total ordering of the type in the following definition is very important, as we shall see.

Definition 10.4. A partially ordered set W is called well-ordered (or as ordinal) if each nonempty subset $B \subset W$ has a first element; that is, for each $B \neq \emptyset$, there exists a $b_0 \in B$ satisfying $b_0 \prec b$ for each $b \in B$.

Every well-ordered set W is in fact totally ordered, since each subset $\{a, b\} \subset W$ has a first element; furthermore, the induced order on a subset of a well-ordered set is a well-order on that subset.

Example 10.10. *$\emptyset$ is a well-ordered set. In any set $\{a\}$ containing exactly one element, $a \prec a$ is well-ordering. The partial ordering by inclusion in $\mathscr{P}(X)$ is not a well-ordering if X has more than one element.*

Example 10.11. *The nonnegative integers are well-ordered: this is one of the ways to state the principle of mathematical induction. This well-ordered set is denoted by ω; that is, $\omega = (N, \leq)$.*

Let W be well-ordered, and $q \notin W$; in $W \bigcup \{q\}$ define an order that coincides with the given one on W, satisfies $q \prec q$, and $\forall w : (w \in W) \Rightarrow w \prec q$. Then $W \bigcup \{q\}$ is well-ordered, since for each nonempty $E \subset W \bigcup \{q\}$, either $E = \{q\}$ or $E \bigcap W \neq \emptyset$, and in the latter case, the first element in $E \bigcap W$ is the first in $E \subset W \bigcup \{q\}$. We say $W \bigcup \{q\}$ is formed from W by adjoining q as last element.

Each element w of a well-ordered set that has a successor in the set, has an immediate successor; that is, we can find as $s \neq w$ satisfying $w \prec s$ and such that no $c \neq s$, w satisfies $w \neq c \neq s$; we need only choose $s =$ first element in the nonempty set $\{x \in W \mid (w \prec x) \wedge (w \neq x)\}$. However, an element w need *not* have an immediate predecessor; for each $b \prec w$ there may always be some $c \neq b, w$ with $b \prec c \prec w$. In fact, adjoining to w a last element q, we note that q has no immediate predecessor.

11 Zorn's Lemma; Zermelo's Theorem

This fundamental theorem is presented without prove:

Theorem 11.1. *The following three statements are equivalent:*

1. *The axiom of choice: Given any nonempty family* $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ *of nonempty pairwise disjoint* sets, *there exists a* set S *consisting of exactly* one *element from each* A_α.
2. *Zorn's lemma: Let* X *be preordered set. If each chain in* X *has an upper bound, then* X *has at least one maximal element.*
3. *Zermelo's theorem: Every set can be well ordered.*

Remarks Though Zermelo's theorem assures that every set can be well-ordered, no specific construction for well-ordering any uncountable set (say, the real numbers) is known. Furthermore, there are sets for which no specific constructions of a total order (let alone a well-order) is known, for example, the set of real-valued functions of one variable. Note, also, that a well-ordering guaranteed by Zermelo's theorem is obviously not unique, and is not stated to have any relation to any given structure on the set. For example, a well-ordering of the reals cannot coincide with usual ordering.

Applications

1. Zorn's lemma is a particularly useful version of the axiom of choice. It is applicable for existence theorems whenever the underlying set is partially ordered and the required object is characterized by maximality. As a simple example of its use, we prove the existence of a Hamel basis B for the real numbers.

   A subset $B = \{b_\alpha \in \mathscr{A}\} \subset E^1$ is a Hamel basis if

   (a) each real x can be written as a finite sum

   $$x = \sum_1^n r_{\alpha_i} b_{\alpha_i}$$

   with rational r_{α_i}

   (b) the set $\{b_\alpha \mid \alpha \in \mathscr{A}\}$ is rationally independent, that is,

   $$\sum_1^n r_{\alpha_i} b_{\alpha_i} = 0 \Leftrightarrow r_{\alpha_i} = 0 \text{ for each } i = 1, \cdots, n.$$

   The rational independence assures that each x can be written as required by the first condition (1a) in exactly one way.

   To prove existence of B, let $\mathscr{A}$ be the family of all rationally independent sets of reals. $\mathscr{A} \neq \emptyset$, since, say, $\{1\} \in \mathscr{A}$. Partially order $\mathscr{A}$ by inclusion. Then any chain $\{A_\beta \mid \beta \in \mathscr{B}\}$

has an upper bound, $\bigcup_\beta A_\beta$, since any finite collection of elements in $\bigcup_\beta A_\beta$ lies in some one A_β and so is rationally independent. Thus there is a maximal $B \in \mathscr{A}$; B is a Hamel basis, since for each x, $B \bigcup \{x\}$ is not rationally independent and therefore there is a relation $zx + r_{\alpha_1} x_{\alpha_1} + \cdots + r_{\alpha_n} x_{\alpha_n} = 0$, which necessarily involves x and has $r \neq 0$ because B is rationally independent, so that

$$x = -\sum_1^n \frac{r_{\alpha_i}}{r} b_{\alpha_i}$$

as required.

Hamel bases arise in several connections: If $b_1 \in B$, then the set of reals generated by $B - b_1$ is not a Lebesgue measurable set. Similarly, the functional equation $f(x+y) = f(x) + f(y)$, which has $f(x) = cx$ as its only continuous solutions, has others also, none of which is a Lebesgue measurable function.

2. In a commutative ring R with unit, every ideal $\mathscr{I} \neq R$ is contained in a maximal ideal (Krull's theorem). The proof is immediate by verifying that the set of all ideals containing $\mathscr{I}$, and not containing 1, satisfies the requirement of Zorn's lemma.

   Since in R every maximal ideal is a prime ideal, this has an immediate consequence the following result: Let X be an infinite set. Then there exists a $\mu : \mathscr{P}(X) \to \{0\} \cup \{1\}$ such that $\mu(F) = 0$ if F is finite, $\mu(X) = 1$, and $\mu(A \bigcup B) = \mu(A) + \mu(B)$ whenever A, B, are disjoint. (In the Boolean ring, $\mathscr{P}(X)$ (see Remark, Lecture notes 1 p. 6), let $\mathscr{F}$ be a maximal ideal containing the ideal of all finite subsets, and set $\mu(A) = 0$ if $A \in \mathscr{F}$ and $\mu(A) = 1$ otherwise.)

12 Ordinals

Since every set can be well-ordered, we study ordinals in greater details.

Definition 12.1. Let W be a well-ordered set.

1. $S \subset W$ is an ideal in W if $\forall x : (x \in S) \wedge (y \prec x) \Rightarrow y \in S$.

2. For each $a \in W$, the set $W(a) = \{x \in W \mid (x \prec a) \wedge (x \neq a)\}$ is the initial interval determined by a.

Clearly, W and $\emptyset$ are ideals in W; $\emptyset$ is also an initial interval, but W is not. For the properties and interrelations of these concepts we have

Proposition 12.1.

1. Every intersection, and every union, of ideals in W is itself an ideal in W.
2. Let $I(W)$ be the set of all ideals in W and $J(W)$ the set of all initial intervals in W. Then $J(W) = I(W) - \{W\}$: the ideals $\neq W$ are the initial intervals.

Proof. 1. $(x \in \bigcap_\alpha S_\alpha) \wedge (y \prec x) \Rightarrow \forall\alpha : (x \in S_\alpha \wedge (y \prec x) \Rightarrow \forall\alpha : y \in S_\alpha \Rightarrow y \in \bigcap_\alpha S_\alpha$, and similarly the union.

2. Each interval is obviously an ideal. Conversely, let $S \neq W$ be an ideal; then $W - S \neq \emptyset$, it has a first element a. We prove $S = W(a)$.

   i $x \in W(a) \Rightarrow x \in S$, since a is the first element of W not in S.

   ii $x \notin W(a) \Leftrightarrow a \prec x \Rightarrow x \notin S$, since otherwise, because S is an ideal, we would have $a \in S$.

□

Definition 12.2. A map f of a well-ordered set $(W, \prec)$ into a well-ordered $(X, \prec')$ is called a *monomorphism* if it is an order-preserving injection [that is, $a \prec b \Rightarrow f(a) \prec f(b)$]; f is an *isomorphism* if it is a bijective monomorphism.

Clearly, the composition of two monomorphisms is also a monomorphism. It is easy to see that if $f : W \to A$ is an order-preserving bijection and W is well-ordered, then the order in A is also a well-ordering and f is an isomorphism.

Theorem 12.1.

1. *The set $I(W)$ of all ideals of a well-ordered set is well-ordered by inclusion.*
2. *The map $a \to W(a)$ is an isomorphism of W onto the set $J(W)$ of its initial intervals [$\emptyset$ included in $J(W) \subset I(W)$].*

Proof. (2) Clearly, $a \prec b \Rightarrow W(a) \subset W(b)$ and $a \neq b \Rightarrow W(a) \neq W(b)$; thus $a \to W(a)$ is bijective and [using order by inclusion in $J(W)$] order-preserving. It follows at once that $J(W)$ is well-ordered by inclusion and that $a \to W(a)$ is an isomorphism.

(1) Since

$$I(W) = J(W) \bigcup \{W\}$$

and since the ordering by inclusion in $I(W)$ is determined by adjoining $\{W\}$ as last element, $I(W)$ is also well-ordered.

□

One consequence is the extremely useful

Theorem 12.2. *Let W be well-ordered, and $\Sigma \subset I(W)$ any family with the following properties:*

(a) Any union of members of Σ belongs to Σ.

(b) If $W(a) \in \Sigma$, then also $W(a) \bigcup \{a\} \in \Sigma$.

Then $\Sigma = I(W)$ and, in particular, $W \in \Sigma$.

Proof. Assume $\Sigma \neq I(W)$; by the previous theorem there is a smallest ideal $S \notin \Sigma$. Either S has a last element, or it does not.

(i) If S has a last element, b, then $S = W(b) \bigcup \{b\}$; because $W(b) \subset S$, we would then have $W(b) \in \Sigma$ and, by using (b), that $S \in \Sigma$, which contradicts the definition of S.

(ii) If S does not have a last element, then $S = \bigcup \{W(a) \mid W(a) \subset S\}$; as before, each $W(a) \in \Sigma$, so by using (a), we conclude that $S \in \Sigma$, again contradicting the definition of S.

Thus, the assumption $\Sigma \neq I(W)$ is false, and the theorem has been proved. □

13 The concept of ordinal numbers

In the class of all ordinals, define $W = X$ if W is isomorphic to X. This is evidently an equivalence relation, so it divides the class of all ordinals into mutually exclusive subclasses. We wish to attach to each ordinal an object, called its *ordinal number*, so that two ordinals have the same ordinal number if and only if they are isomorphic. Following Frege, we could define the ordinal number of an ordinal to be the equivalence *class* of the ordinal. Though this definition is adequate for most mathematical purposes, it has the disadvantage that ordinal numbers are not *sets*: Without separate axiomatic for them, we could not, for example, legitimately consider any collection of ordinal numbers. To develop this axiomatics it is enough to show that there exist a uniquely defined well-ordered class $\mathscr{L}$ such that each well-ordered set is isomorphic to some initial interval of $\mathscr{L}$. The desired objective is attained by calling the members of $\mathscr{L}$ ordinals numbers and assigning to each ordinal W the $\alpha \in \mathscr{L}$ for which $W = \mathscr{L}(\alpha)$.
The basic idea is to use the sets postulated by the axiom of infinity. Then each $\alpha \in \mathscr{L}$ will be a set whose elements are all the sets in $\mathscr{L}$ that precede it; in other words, each $\alpha \in \mathscr{L}$ will be simply the initial interval $\mathscr{L}(\alpha)$ in $\mathscr{L}$. To illustrate the mechanics, we write down the first few members of $\mathscr{L}$:

$$\emptyset; \{\emptyset\}; \{\emptyset, \{\emptyset\}\}; \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

The ordinal number of $\{1, 2, 3\}$, in its natural order, is then $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
If the set is infinite, the ordinal number is said to be transfinite.

14 Comparison of ordinal numbers

If n_1 and n_2 are two finite ordinal numbers, then they either coincide or else one is large than the other. As we now show, the same is true of transfinite ordinal numbers. Given any two ordinal numbers α and β corresponding to the well-ordered sets W and V respectively. Then we can say that

- $\alpha = \beta$ if W and V are isomorphic;
- $\alpha < \beta$ if W is isomorphic to some initial interval of V;
- $\alpha > \beta$ if V is isomorphic to some initial interval od W

(note that this definition makes sense for finite α and β).

Lemma 14.1. *Let f be an isomorphism of a well-ordered set A onto some subset $B \subset A$. Then $f(a) \geq a$ for all $a \in A$.*

Proof. If there are elements $a \in A$ such that $f(a) \geq a$, then there is a least such element since A is well-ordered set. Let a_0 be this element and let $b_0 = f(a_0)$. Then $b_0 < a_0$, and hence $f(b_0) < f(a_0) = b_0$ since f is an isomorphism. But then a_0 is not the smallest element such that $f(a) < a$. Contradiction. □

It follows from this lemma that a well-ordered set A cannot be isomorphic to any of its initial intervals, since if A were isomorphic to the initial interval determined by a, then clearly $f(a) < a$. In other words, the two relations

$$\alpha = \beta, \quad \alpha < \beta$$

are incompatible, and so are

$$\alpha = \beta, \quad \alpha > \beta$$

Moreover, the two relations

$$\alpha < \beta, \quad \alpha > \beta$$

are incompatible, since otherwise we could use the transitivity to deduce $\alpha < \alpha$, which is impossible by the lemma. Therefore, if one of the three relations

$$\alpha < \beta, \quad \alpha = \beta \quad \alpha > \beta \tag{1}$$

holds, the other two are automatically excluded. We must still show that one of relations (1) always holds, thereby providing that any two ordinal numbers are compatible.

Theorem 14.1. *Two given ordinal numbers α and β satisfy one and only one of the relations*

$$\alpha < \beta, \quad \alpha = \beta, \quad \alpha > \beta$$

Proof. Let $W(\alpha)$ be the set of all ordinal numbers $< \alpha$. Any two numbers γ and γ' in $W(\alpha)$ are comparable and the corresponding ordering of $W(\alpha)$ makes it a well-ordered set with ordinal number α. In fact, if is a set

$$A = \{\dots, a, \dots, b, \dots\}$$

has ordinal number α, then by definition, the ordinals corresponding to the ordinal numbers less than α are isomorphic to some initial interval of A. Hence the ordinal numbers themselves are in one-to-one correspondence with the elements of A.
Now let α and β be any two ordinal numbers corresponding to well-ordered sets $W(\alpha)$ and $W(\beta)$ respectively. Moreover, let $C = A \bigcap B$ be the intersection of the sets A and B, i.e. sets of all ordinals less than both α and β. Then C is well-ordered with ordinal number γ, say. We now show that $\gamma \leq \alpha$. If $C = A$ then obviously $\gamma = \alpha$. On the other hand, if $C \neq A$, then C is an initial interval of A and hence $\gamma < \alpha$. In fact, let $\xi \in C$, $\eta \in A - C$. Then ξ and η are compatible, i.e., either $\xi < \eta$ or $\xi > \eta$. but $\eta < \xi\alpha$ is impossible, since then $\eta \in C$. Therefore $\xi < \eta$ and hence C is an initial interval of A, which implies $\gamma < \alpha$. Moreover, γ is the first element of the set $A - C$. Thus $\gamma \leq \alpha$, as asserted, and similarly $\gamma \leq \beta$. The case $\gamma < \alpha$, $\gamma < \beta$ is impossible, since then $\gamma \in A - C$, $\gamma \in B - C$. But then $\gamma \notin C$ on the one hand and $\gamma \in A \bigcap B = C$ on the other hand. It follows that there are only three possibilities

$$\gamma = \alpha,\ \gamma = \beta,\ \alpha = \beta$$
$$\gamma = \alpha,\ \gamma < \beta,\ \alpha < \beta$$
$$\gamma < \alpha,\ \gamma = \beta,\ \alpha > \beta$$

□

15 Transfinite induction

Mathematical propositions are very often proved by using the following familiar

Theorem 15.1. Mathematical induction *Given a proposition $P(n)$ formulated for every positive integer n, suppose that*

(1) $P(1)$ is true;

(2) The validity of $P(k)$ for all $k \leq n$ implies the validity of $P(n+1)$.

Then $P(n)$ is true for all $n = 1, 2, \dots$

Proof. Suppose $P(n)$ fails to be true for all $n = 1, 2, \dots$, and let n_1 be smallest integer for which $P(n)$ is false (the existence of n_1 follows from the well-ordering of the positive integers). Clearly $n_1 > 1$, so that $n_1 - 1$ is a positive integer. Therefore $P(n)$ is valid for all $k \leq n_1 - 1$ but not for n_1. Contradiction. □

Replacing the set of all integers by an arbitrary well-ordered set, we get

Theorem 15.2. Transfinite induction *Given a well ordered set A, let $P(a)$ be a proposition formulated for every element $a \in A$. Suppose that*

(1) $P(1)$ is true for the smallest element of A;

(2) The validity of $P(a)$ for all $a < a^*$ implies the validity of $P(a^*)$.

Then $P(a)$ is true for all $a \in A$.

Proof. Suppose $P(a)$ fails to be true for all $a \in A$. Then $P(a)$ is false for all a in some nonempty subset $A^* \subset A$. By the well-ordering, A^* has a smallest element a^*. Therefore $P(a)$ is valid for all $a < a^*$ but not for a^*. Contradiction. □

Remark Since any set can be well-ordered by Zermelo's theorem, transfinite induction can in principle can be applied to any set M whatsoever. In practice, however, Zorn's lemma is a more useful tool, requiring only that M be partially ordered.

16 Cardinality of Sets

The ordinals are associated with counting: to count, one counts some elements first and thus tacitly induced a well-ordering. The concept of cardinal is related simply to size: we wish to determine if one of two given sets has more members than the other. Counting is not needed for this purpose: we need only pair off each member of one set with a member of the other and see if any elements are left over. "Same size" is thus formalized in

Definition 16.1. Two sets, X and Y, are equipotent (or have the same cardinal) if a bijective map of X onto Y exists. We denote "X equipotent to Y" by "card X = card Y".

The next simple theorem shows that equipotence is an equivalence relation in the class of all sets, so it decomposes this class into mutually exclusive subclasses, called *equipotence classes.*

Theorem 16.1. *Let A, B, and C be sets, then*

1. *A is equipotent to A*
2. *If A is equipotent to B, then B is equipotent to A*
3. *If A is equipotent to B and B is equipotent to C, then A is equipotent to C*

Proof.

1. The identity function (Id_A) which returns the same value that was used as its argument ($f(x) = x$) for all elements of A is a bijective map of A onto A.

2. If f is a bijective map of A onto B then f^{-1} is a bijective map of B onto A.

3. If f is a bijective map of A onto B and g is a bijective map of B onto C, then $f \circ g$ is a bijective map of A onto C

$\square$

Example 16.1. *Let* $X = \{2n \mid n \in N\} \subset N$. *Then card* X = *card* N, *since* $n \to 2n$ *is a bijective of* N *onto* X. *Note that a set may be equipotent with a proper subset.*

Example 16.2. *Any open interval* $]a, b[\subset E^1$ *is equipotent to* $\mathscr{J} =]-1, +1[$, *since* $x \to \frac{b-a}{2}x + \frac{b+a}{2}$ *is a bijection* $\mathscr{J} \to]a, b[$. *Furthermore,* $\mathscr{J}$ *is equipotent with* E^1, *as* $x \to \frac{x}{1+|x|}$ *shows. Thus, by transitivity, card* $]a, b[$ = *card* E^1: *each open interval in* E^1 *has "just as many points" as* E^1 *itself.*

Definition 16.2. For two sets X, Y, the cardinality of X is less than or equal to the cardinality of Y, and we write card $X \leq$ card Y if an injection $X \to Y$ exists.

Note that we use "$\leq$" rather than "smaller": The existence of an injection $X \to Y$ does not exclude the possibility that there is also a bijection $X \to Y$.
The next evident proposition and the following theorem show that the property card $X \leq$ card Y behaves like an ordering on the "equivalence classes" under equipotence.

Proposition 16.1. Let X, Y, and Z be sets, then

1. If card $X \leq$ card Y and card X = card Z, then card $Z \leq$ card Y

2. If card $X \leq$ card Y and card Y = card Z, then card $X \leq$ card Z

3. card $X \leq$ card X

4. If card $X \leq$ card Y, and card $Y \leq Z$, then card $X \leq$ card Z

We see that $\leq$ is reflexive and transitive. It remains to establish antisymmetry.

Theorem 16.2. Cantor-Bernstein

If card $X \leq$ *card* Y *and card* $Y \leq$ *card* X, *then card* X = *card* Y.

Proof. If card $X \leq$ card Y, then there is an injection f that maps X into Y; if card $Y \leq$ card X, then there is an injection g that maps Y into X. To show that card $X =$ card Y we have to exhibit a one-to-one function which maps X onto Y.

Let us apply first f and then g; the function $g \circ f$ maps X into X and is an injection. Clearly, $g(f(X)) \subset g(Y) \subset X$; moreover, since f and g are one-to-one, we have card $X =$ card $g(f(X))$.

Then to prove this theorem we should prove the following equivalent proposition (which is also sometimes called "Cantor-Bernstein theorem"): *Given any two sets A and B, suppose A contains a subset A_1 equipotent to B, while B contains a subset B_1 equivalent to A. Then A and B are equipotent."*

By hypothesis there is one-to-one function f mapping A into B_1 and one-to-one function g mapping B into A_1:

$$f(A) = B_1 \subset B,\ g(B) = A_1 \subset A$$

therefore

$$A_2 = gf(A) = g(f(A)) = g(B_1)$$

is a subset of A_1 equipotent to A. Similarly

$$B_2 = fg(B) = f(g(B)) = f(A_1)$$

is a subset of B_1 equipotent to B. Let A_3 be the subset of A into which the mapping gf carries the set A_1, and let A_4 be the subset of A into which gf carries A_2. More generally, let A_{k+2} be the set into which A_k $(k = 1, 2, ...)$ is carried by gf. Then clearly

$$A \supset A_1 \supset A_2 \supset \cdots \supset A_k \supset A_{k+1} \cdots$$

Setting

$$D = \bigcap_{k=1}^{\infty} A_k$$

we can represent A as the following union of pairwise disjoint sets:

$$A_1 = (A - A_1) \bigcup (A_1 - A_2) \bigcup (A_2 - A_3) \bigcup \cdots \bigcup (A_k - A_{k+1}) \bigcup \cdots \bigcup D$$

Clearly, A and A_1 can be represented as

$$A = D \bigcup M \bigcup N$$
$$A_1 = D \bigcup M \bigcup N_1$$

where

$$M = (A_1 - A_2)\bigcup(A_3 - A_4)\bigcup\cdots$$
$$N = (A - A_1)\bigcup(A_2 - A_3)\bigcup\cdots$$
$$N_1 = (A_2 - A_3)\bigcup(A_4 - A_5)\bigcup\cdots$$

But $A - A_1$ is equipotent to $A_2 - A_3$ (the former is carried into the later by the one-to-one function gf), $A_2 - A_3$ is equipotent to $A_4 - A_5$. and so on. Therefore N is equipotent to N_1 and therefore the one-to-one correspondence can be set up between the sets A and A_1. But A_1 is equipotent to B, by hypothesis. Therefore A is equivalent to B. $\square$

Remark. Here we can even "afford the unnecessary luxury" of explicitly writing down a one-to-one function carrying A into B, i.e.,

$$\varphi(a) = \begin{cases} g^{-1} & \text{if } a \in D\bigcup M \\ f(a) & \text{if } a \in D\bigcup N \end{cases}$$

17 Finite, Countable and Uncountable Sets

In this section we list some basic facts concerning finite, countable and uncountable sets. We do not prove them, but students are encouraged to read the first chapter of the James Munkres's book, where some proofs are given. For the comprehensive theory of sets we refer to "Introduction to set theory" by K. Hrbacek and T. Jech.

Definition 17.1. A set S is *finite* if it is equipotent to some natural number $n \in N$. We then define card $S = n$ and say that S has n *elements*. A set is *infinite* if it not finite.

Finite sets

Proposition 17.1. If $n \in N$, then there is no one-to-one mapping of n onto a proper subset $X \subsetneq n$

Corollary 17.1.

- *If $n \neq m$, then there is no mapping of n onto m.*
- *If card $S = n$ and card $S = m$, then $n = m$.*
- *N is infinite.*

Proposition 17.2. If X is a finite set and $Y \subset X$, then Y is finite. moreover card $Y \leq$ card X.

Proposition 17.3. If X is a finite set and f is a function, then $f(X)$ is finite. Moreover card $f(X) \leq$ card X.

Proposition 17.4. If X and Y are finite, then $X \bigcup Y$ is finite. Moreover card $X \bigcup Y \leq$ card X + card Y, and if X and Y are disjoint, then card $X \bigcup Y$ = card X + card Y.

Proposition 17.5. If X is finite then $\mathscr{P}(X)$ is finite.

Proposition 17.6. If X is infinite, then card $X > n$ for all $n \in N$.

Countable sets

Definition 17.2. A set S is countable if card S = card N.

Proposition 17.7. An infinite subset of a countable set is countable.

Proposition 17.8. The union of a finite family of countable sets is countable.

Proposition 17.9. If A and B are countable, then $A \times B$ is uncountable.

Corollary 17.2. *The cartesian product of a finite number of countable sets is countable. Consequently, N^m is countable, for every $m > 0,\ m \in N$.*

Proposition 17.10. If A is countable, then the set $Seq(A)$ of all finite sequences of elements of A is countable.

Corollary 17.3. *The set of all finite subsets of a countable set is countable.*

Proposition 17.11. The set of all integers Z and the set of all rational numbers Q are countable.

Proposition 17.12. An equivalence relation on a countable set has at most countably many equivalence classes (i.e. finite or countable number).

Uncountable sets

Definition 17.3. The infinite set S is an uncountable set if it is not countable.

Proposition 17.13. Uncountable sets exist.

Proposition 17.14. The set of real numbers R is uncountable.

Corollary 17.4. *The following sets are uncountable:*

1. *The set of all real numbers in any closed interval $[a, b]$.*

2. *The set of all real numbers in any open interval (a, b).*

3. *The set of all integer points in the plane or in space.*

4. *The set of all points on a sphere or inside a sphere.*

5. *The set of all lines in the plane.*

6. *The set of all* continuous *real functions of one or several variables.*

Proposition 17.15. The set of all sets of natural numbers is uncountable, in fact card $\mathscr{P}(N) >$ card N, and card $\mathscr{P}(N) =$ card R

Infinite sets

Proposition 17.16. Every infinite set has a countable subset.

Proposition 17.17. Every infinite set is equivalent to one of its proper subsets.

The proof of Proposition (17.17) is a homework assignment.

18 General Cartesian Products

In this section the concept of cartesian product is extended to any family of sets. this extension is based on the observation that the elements of $A_1 \times A_2$ can be considered to be those maps f of the index set $\{1, 2\}$ into $A_1 \bigcup A_2$ having the property $f(1) \in A_1$, $f(2) \in A_2$.

Definition 18.1. Let $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ be a family of sets. The cartesian product $\prod\limits_\alpha A_\alpha$ is the set of all maps $c : \mathscr{A} \to \bigcup\limits_\alpha A_\alpha$ having the property $\forall \alpha \in \mathscr{A} : c(\alpha) \in A_\alpha$.

That $\prod\limits_\alpha A_\alpha$ is indeed a *set* follows from Propositions (9.3), (9.7). The notations $\prod\limits_\alpha A_\alpha$ and $\prod\limits_\alpha \{A_\alpha \mid \alpha \in \mathscr{A}\}$ are used interchangeably. An element $c \in \prod\limits_\alpha A_\alpha$ is generally written $\{a_\alpha\}$, indicating that $c(\alpha) = a_\alpha$ for each α; with this notation, $a_\alpha \in A_\alpha$ is called the αth coordinate of $\{a_\alpha\}$. The set A_α is called the αth factor of $\prod\limits_\alpha A_\alpha$; for each $\beta \in \mathscr{A}$, the map

$$p_\beta : \prod_\alpha A_\alpha \to A_\beta$$

given by $\{a_\alpha\} \to a_\beta$ [or, equivalently, by $c \to c(\beta)$] ie termed "projection onto the βth factor".

Example 18.1. *If each A_α has exactly one element, $\prod\limits_\alpha A_\alpha$ consists of a single element. If $\mathscr{A} = \emptyset$, then again $\prod\limits_\alpha A_\alpha$ has exactly one element, the null set. If $\mathscr{A} \neq \emptyset$ and some one $A_\alpha = \emptyset$, then $\prod\limits_\alpha A_\alpha = \emptyset$.*

Example 18.2. *If each $A_\alpha = A$ is a fixed set, then $\prod_\alpha A_\alpha$ is simply a set of all maps $\mathscr{A} \to A$.*

Example 18.3. *Let $A_i = \{0, 2\}$ for each $i \in Z^+$; $\prod_\alpha A_\alpha$ is then the set of all sequences of 0's and 2's: $\{\{n_i \mid n_i = 0 \text{ or } 2;\ i = 1, 2, \cdots\}$. The map $f : \prod_\alpha A_\alpha \to [0, 1] \subset E^1$, defined by*

$$f(\{n_i\}) = \sum_{i=1}^{\infty} \frac{n_i}{3^i}$$

is easily seen to be injective; the image is called the Cantor set, and can be described geometrically as follows: Divide $[0, 1]$ into three equal parts and remove the middle-third open interval $]\frac{1}{3}, \frac{2}{3}[$; this removes all real numbers in $[0, 1]$ that require $n_1 = 1$ in their triadic expansion. At the second stage, remove the middle third of each of the two remaining intervals, $[0, \frac{1}{3}]$, $[\frac{2}{3}, 1]$, thus eliminating all real numbers in $[0, 1]$ requiring $n_2 = 1$ in their triadic expansion. Proceeding analogously, removing at the nth stage the union M_n of the middle thirds of the 2^{n-1} intervals present, $C = [0, 1] - \bigcup_1^\infty M_n$ is the Cantor set. It consists of all real numbers in $[0, 1]$ that do not require the use of "1" in their triadic expansion. Since the expansion (using no 1's) of each number of C is unique, f is a bijection of $\prod_\alpha A_\alpha$ on C. In view of Example (18.2), there is a bijection of all maps $Z^+ \to \{0, 2\}$ onto the Cantor set.

Example (18.3) is analogous to the Russell example of pairs of shoes, in that each A_n has distinctive elements. In the general case where the A_α are abstractly given sets, the possibility remains open that, even though each $A_\alpha \neq \emptyset$ still $\prod_\alpha A_\alpha = \emptyset$; to show that it is not empty requires that we exhibit a $c : \mathscr{A} \to \bigcup_\alpha A_\alpha$ having property required in Definition (18.1), and this requires appeal to the axiom of choice. In fact,

Theorem 18.1. *The following three properties are equivalent:*

1. *Let $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ be nonempty family of sets. If each $A_\alpha \neq \emptyset$, then $\prod\{A_\alpha \mid \alpha \in \mathscr{A}\} \neq \emptyset$.*
2. *The axiom of choice*
3. *If $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ be a family of nonempty sets (not necessarily pairwise disjoint!), then there exists a map $c : \mathscr{A} \to \bigcup_\alpha A_\alpha$ such that $\forall \alpha \in \mathscr{A} : c(\alpha) \in A_\alpha$. (c is called a "choice function" for the family $\{A_\alpha \mid \alpha \in \mathscr{A}\}$).*

Proof.

- (1) $\Rightarrow$ (2). Let $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ be a family of nonempty pairwise disjoint sets. Since $\prod_\alpha A_\alpha \neq \emptyset$, we can exhibit an element $c = \{a_\alpha\}$; then $S = c(\mathscr{A})$ is a set satisfying the requirements in the axiom of choice.

- (2) $\Rightarrow$ (3). For each $\alpha \in \mathscr{A}$, let $A'_\alpha = \alpha \times A_\alpha$; each A'_α is a nonempty set and the family $\{A'_\alpha \mid \alpha \in \mathscr{A}\}$ is pairwise disjoint. By the axiom of choice, there is a set S consisting of exactly one member from each A'_α; that is, for each α there is a unique $(\alpha, a_\alpha) \in S$ with $a_\alpha \in A_\alpha$. Since
$$S \subset \bigcup_\alpha (\{\alpha\} \times A_\alpha) \subset \bigcup_\alpha (\mathscr{A} \times A_\alpha) = \mathscr{A} \times \bigcup_\alpha A_\alpha,$$
S is indeed a map $\mathscr{A} \to bigcup_\alpha A_\alpha$ as required. Observe that the "chosen" elements may be the same for distinct α.

- (3) $\Rightarrow$ (1). If $c : \mathscr{A} \to \bigcup_\alpha A_\alpha$ is a choice function, it is an element of $\prod_\alpha A_\alpha$.

$\square$

We can now define some future properties of cartesian products.

Theorem 18.2. *Let $\{A_\alpha \mid \alpha \in \mathscr{A}\}$ be a family of nonempty sets, let $\mathscr{B} \subset \mathscr{A}$, and define $P : \prod_\alpha \{A_\alpha \mid \alpha \in \mathscr{A} \to \prod_\alpha A_\alpha \mid \alpha \in \mathscr{B}\}$ by $P(c) = c \mid \mathscr{B}$. Then P is surjective; in particular, each projection $p_\beta : \prod_\alpha A_\alpha \to A_\beta$ is surjective.*

Proof. Let $f \in \prod\{A_\alpha \mid \alpha \in \mathscr{B}\}$ be any given element; we are to find a $c \in \prod\{A_\alpha \mid \alpha \in \mathscr{A}\}$ with $P(c) = f$. By Theorem (16.2) (3) there is a choice function $\bar{c} : \mathscr{A} - \mathscr{B} \to \bigcup\{A_\alpha \mid \alpha \in \mathscr{A} - \mathscr{B}\}$; then the map $c : \mathscr{A} \to \bigcup\{A_\alpha \mid \alpha \in \mathscr{A}\}$ given by $c \mid \mathscr{B} = f$, $c \mid \mathscr{A} - \mathscr{B} = \bar{c}$ (by Corollary (7.1) is an element of
$$\prod\{A_\alpha \mid \alpha \in \mathscr{A}\}$$
and $P(c) = c \mid \mathscr{B} = f$. If $\mathscr{B}$ consists of a single element $\beta \in \mathscr{A}$, it is clear that the map P will be p_β, which proves the second part. $\square$

Corollary 18.1. *If $A_\alpha \subset B_\beta$, for each $\alpha \in \mathscr{A}$, then $\prod_\alpha A_\alpha \subset \prod_\alpha B_\alpha$. Conversely, if each $A_\alpha \neq \emptyset$ and $\prod_\alpha A_\alpha \subset \prod_\alpha B_\alpha$, then $A_\alpha \subset B_\alpha$ for each α.*

Proof. The first assertion is trivial. The proof of the second is left as a homework. $\square$