**MATHEMATICS 000**

Thomas Wieting
Reed College, 2001

**1 Introduction**
**2 Sets and Mappings**
**3 The Concept of Ring**
**4 Number Systems**
**5 Mathematical Induction**
**6 Problems**
**7 Reference**

## 1 Introduction

01° The object of these brief notes is to establish common ground for the discussion of elementary Mathematics. We first develop the basic properties of Sets and Mappings. We then describe the concept of Ring. This concept serves in general to set a context in which we may practice reading and writing mathematical arguments and serves in particular to organize our review of the familiar Number Systems of elementary Mathematics. Finally, under our review of the Ring of Integers, we describe the method of argument by Mathematical Induction.

We do not attempt to modulate the relentlessly formal tone of these notes. However, in any specific context of study, one would supplement the notes with motivational remarks and examples.

## 2 Sets and Mappings

*Axioms*

02° The language of Mathematics is based upon the term Set and upon the relations of Membership and Equality between sets. We present these ideas without formal definition, relying upon ordinary usage to supply them with intuitive meaning and relying upon the following discussion of their properties to refine that meaning for our purposes. We begin with notation. One generally denotes sets by the various letters of the English and other alphabets, for example by $a$, $B$, $\mathcal{Y}$, $\mathbf{Z}$, and $\epsilon$. One often uses the letters in modified form (such as $a_1$, $B^*$, $\mathcal{Y}_\circ$, $\hat{\mathbf{Z}}$, and $\bar{\epsilon}$) or in combinations (such as $A \times B$), and one sometimes uses more exotic symbols (such as $\emptyset$).

For any sets $a$ and $B$, one expresses the relation of membership between $a$ and $B$ by writing $a \in B$ and the denial of that relation by $a \notin B$. In practice,

we shall try to arrange notation so that if a set is denoted by an upper case letter then its members are denoted by lower case letters, if a set is denoted by a script letter then its members are denoted by upper case letters, and if a set is denoted by a boldface letter then its members are denoted by script letters (thus: $a \in B$, $B \in \mathcal{Y}$, and $\mathcal{Y} \in \mathbf{Z}$).

For any sets $A$ and $B$, one expresses the relation of equality between $A$ and $B$ by writing $A = B$ and the denial of that relation by $A \neq B$.

Given two sets $A$ and $B$, one says that $A$ is *included* in $B$ iff, for any set $x$, if $x \in A$ then $x \in B$. One might also say that $A$ is a *subset* of $B$. One expresses the relation of inclusion between $A$ and $B$ by writing $A \subseteq B$ and the denial of that relation by $A \not\subseteq B$.

The first axiom concerning sets states the intuitively evident fact that a set is entirely determined by its members, that is, that two sets are equal iff they have the same members.

(AXIOM 1) Axiom of Extension

For any sets $A$ and $B$, $A = B$ iff, for any set $x$, $x \in A$ iff $x \in B$.

Clearly, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

The second axiom introduces a substantial measure of flexibility. Informally, it provides for the formation of a subset of a given set by imposition of a condition for membership.

(AXIOM 2) Axiom of Specification

For any set $A$ and for any condition $\gamma$ applicable to the members of $A$, there is a set $B$ such that, for any set $x$, $x \in B$ iff $x \in A$ and $x$ satisfies $\gamma$.

By the Axiom of Extension, the set $B$ is unique. One refers to $B$ as the subset of $A$ *determined* by the condition $\gamma$ and one (sometimes) denotes it by:

$$\{\, x \in A \;:\; x \text{ satisfies } \gamma \,\}$$

Of course, in order to apply the Axiom of Specification, one must interpret the meaning of Condition. In point of fact, a proper discussion of this matter is subtle and would be at odds with the intent of this informal summary. In place of such a discussion, let us simply remark that in practice the meaning of Condition is clear. In subsequent developments, we shall describe instances of the Axiom of Specification which will suggest the manner in which the axiom is commonly used.

One might argue that the ambient set $A$ in the foregoing statement of the Axiom of Specification is irrelevant. Specifically, one might contend that the axiom should assert that, for any condition $\gamma$, there is a set $B$ such that,

for any set $x$, $x \in B$ iff $x$ satisfies $\gamma$. However, this unrestricted form of the axiom yields bald contradictions. Thus, from the particular condition:

($\bullet$) $\quad x \notin x$

one would obtain a set $B$ such that, for any set $x$, $x \in B$ iff $x \notin x$. It would follow that $B \in B$ iff $B \notin B$. In order to avoid this logical contradiction, called Russell's Paradox, one must restrict the naive correspondence between sets and conditions. At the same time, one must try to preserve the essential content of that correspondence. The compromise generally agreed upon by mathematicians is the Axiom of Specification as we have stated it.

The conventional form of the Axiom of Specification sidesteps Russell's Paradox in the following way. Given a set $A$ and the condition just stated, one would obtain a set $B$ such that, for any set $x$, $x \in B$ iff $x \in A$ and $x \notin x$. Now it would follow that $B \in B$ iff $B \in A$ and $B \notin B$, which while peculiar is not logically contradictory.

Let us emphasize that the efficacy of the Axiom of Specification is relative. For a given set, it provides an array of subsets; however, it does not by itself guarantee that sets exist. In due course, we shall present the Axiom of Infinity, which does provide for the existence of sets (in grand style). Until then, however, we shall proceed in good faith.

With the provisional assumption that sets do exist, we may apply the Axiom of Specification to produce a set of appealing simplicity. Thus, from a given set $A$ and from the condition:

($\bullet$) $\quad x \neq x$

we obtain a set $B$ such that, for any set $x$, $x \notin B$. One refers to this set as the *empty set* and denotes it by $\emptyset$.

The third axiom concerning sets provides for the formation of sets having two specified members.

(AXIOM 3) Axiom of Pairs

For any sets $a$ and $b$, there is a set $C$ such that, for any set $x$, $x \in C$ iff $x = a$ or $x = b$.

By the first axiom, the set $C$ is unique. One refers to it as the (unordered) *pair* determined by $a$ and $b$ and denotes it by $\{a, b\}$.

The next two axioms provide for the formation of unions and intersections of sets.

(AXIOM 4) Axiom of Unions

For any set $\mathcal{A}$, there is a set $E$ such that, for any set $x$, $x \in E$ iff there is some set $A$ such that $A \in \mathcal{A}$ and $x \in A$.

(AXIOM 5) Axiom of Intersections

For any set $\mathcal{A}$, if $\mathcal{A} \neq \emptyset$ then there is a set $F$ such that, for any set $x$, $x \in F$ iff, for each set $A$, if $A \in \mathcal{A}$ then $x \in A$.

The Axiom of Extension implies that the sets $E$ and $F$ just mentioned are unique. One refers to them as the *union* and the *intersection* of $\mathcal{A}$ and one denotes them by $\cup\mathcal{A}$ and $\cap\mathcal{A}$ respectively.

By elementary argument, one can show that the Axiom of Intersections is a consequence of the Axiom of Specification and the Axiom of Unions. In this context, however, we have opted for symmetry at the expense of economy. By the way, the hypothesis that $\mathcal{A}$ be nonempty in the statement of the Axiom of Intersections is crucial. In fact, if $\mathcal{A}$ were empty then the set $F$ indicated in the Axiom of Intersections would be *universal*, in that, for any set $x$, $x \in F$. Conjoined with the Axiom of Specification, such a set would reproduce Russell's Paradox.

Let us apply the foregoing axioms to a particular case. Thus, let $C$ and $D$ be any sets and let $\mathcal{A} = \{C, D\}$. Now, for any set $x$, $x \in \cup\mathcal{A}$ iff $x \in C$ or $x \in D$. Moreover, for any set $x$, $x \in \cap\mathcal{A}$ iff $x \in C$ and $x \in D$. In this context, one denotes $\cup\mathcal{A}$ by $C \cup D$ and $\cap\mathcal{A}$ by $C \cap D$, and one refers to them as the *union* and *intersection* of $C$ and $D$.

By conjoining the Axiom of Pairs and the Axiom of Unions, one can justify the formation of sets having three specified members. Thus, given any sets $a$, $b$, and $c$, one can form the sets $\{a, b\}$ and $\{c\} := \{c, c\}$; one can then form the set $\{a, b\} \cup \{c\}$. Obviously, the members of this set are $a$, $b$, and $c$ and nothing else. One denotes the set by $\{a, b, c\}$. In similar manner, one can obtain sets having any (finite) number of specified members.

In turn, one can form the union and intersection of any (finite) number of given sets, obtaining such sets as $C \cup D \cup X$ and $C \cap D \cap Y \cap Z$.

The sixth axiom provides for the formation of the set of all subsets of a given set.

(AXIOM 6) Axiom of Powers

For any set $A$, there is a set $\mathcal{B}$ such that, for any set $X$, $X \in \mathcal{B}$ iff $X \subseteq A$.

Once again, the first axiom guarantees that the set $\mathcal{B}$ is unique. One refers to it as the *power set* of $A$ and denotes it by $\mathcal{P}(A)$.

For our purposes, there are two more axioms to be considered: the Axiom of Choice and the Axiom of Infinity. We shall describe the former in context of the following discussion of Mappings and the latter in the later section on Number Systems.

*Ordered Pairs*

03° Let us turn now to a discussion of Ordered Pairs of sets and of Cartesian Products of sets. These are the basic ideas underlying studies of Relations and of Mappings.

For any sets $a$ and $b$, one defines the *ordered pair* with first component $a$ and second component $b$ to be the set $\{\{a\}, \{a, b\}\}$. One denotes this ordered pair by $(a, b)$. By careful consideration of cases, one can prove the following fundamental property of ordered pairs:

(•) for any sets $a'$, $a''$, $b'$ and $b''$, if $(a', b') = (a'', b'')$ then $a' = a''$ and $b' = b''$

One should contrast this circumstance with that of (unordered) pairs, as described in the Axiom of Pairs. From the hypothesis $\{a', b'\} = \{a'', b''\}$, one may infer that $a' = a''$ or $a' = b''$ and one may infer that if $a' = a''$ then $b' = b''$ and that if $a' = b''$ then $b' = a''$; however, one cannot recover the order of appearance of the component sets $a$ and $b$ from the set $\{a, b\}$.

One can extend the foregoing discussion of ordered pairs to apply to the formation of ordered triples, quadruples, quintuples, and so forth. Thus, for any sets $a$, $b$, and $c$, one defines the *ordered triple* with first component $a$, with second component $b$, and with third component $c$ to be the set $(a, (b, c))$. Of course, one obtains the characteristic property that, for any sets $a_1$, $a_2$, $b_1$, $b_2$, $c_1$, and $c_2$, if $(a_1, b_1, c_1) = (a_2, b_2, c_2)$ then $a_1 = a_2$, $b_1 = b_2$, and $c_1 = c_2$. Similar comments apply to ordered quadruples, quintuples, and the like.

Now let $A$ and $B$ be any sets. We contend that there is a set $C$ the members of which are precisely the ordered pairs $(a, b)$, where $a$ is any member of $A$ and where $b$ is any member of $B$. Of course, the set $C$ in question would be unique. One refers to it as the *cartesian product* of $A$ and $B$ and denotes it by $A \times B$. To justify the formation of the cartesian product of $A$ and $B$, we apply the foregoing axioms and definitions. We note first that, for any member $a$ of $A$ and for any member $b$ of $B$, $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Of course, the set $\mathcal{P}(\mathcal{P}(A \cup B))$ will generally contain many other members than those of the form $(a, b)$. We obtain the desired set $C$ by applying the Axiom of Specification to the set $\mathcal{P}(\mathcal{P}(A \cup B))$ and to the condition:

(•) there are sets $a$ and $b$ such that $a \in A$, $b \in B$, and $x = (a, b)$

The resulting subset of $\mathcal{P}(\mathcal{P}(A \cup B))$ is the cartesian product of $A$ and $B$.

*Relations*

04° Let us describe the concept of Relation. Let $X$ be any set. By a *relation* on $X$, one means any subset $\Delta$ of $X \times X$. For any members $x'$ and $x''$ of $A$, one says that $x'$ is *related* to $x''$ relative to $\Delta$ iff $(x', x'') \in \Delta$. In deference to the conventional notations involving membership, equality, and the like, one generally writes $x' \,\Delta\, x''$ instead of $(x', x'') \in \Delta$ and $x' \not\Delta\, x''$ instead of $(x', x'') \notin \Delta$.

Two types of relations accur repeatedly in mathematical studies: Order Relations and Equivalence Relations. Let us give a brief description of these ideas. Let $X$ be any nonempty set. One says a relation $\Delta$ on $X$ is an *order relation* iff it satisfies the following conditions:

- (•) for any member $x$ of $X$, $x \,\Delta\, x$
- (•) for any members $x$ and $y$ of $X$, if $x \,\Delta\, y$ and $y \,\Delta\, x$ then $x = y$
- (•) for any members $x$, $y$, and $z$ of $X$, if $x \,\Delta\, y$ and $y \,\Delta\, z$ then $x \,\Delta\, z$

With reference to the first of the foregoing conditions, one says that the relation $\Delta$ on $X$ is *reflexive*; to the second, *antisymmetric*; to the third, *transitive*.

For example, one may introduce a set $A$ and then form the relation $\Delta$ on $\mathcal{X} := \mathcal{P}(A)$ consisting of all ordered pairs $(B', B'')$ in $\mathcal{P}(A) \times \mathcal{P}(A)$ for which $B' \subseteq B''$. Obviously, $\Delta$ is an order relation.

One says that the order relation $\Delta$ on $X$ is *linear* if (in addition to the foregoing three conditions) it satisfies the following condition:

- (•) for any members $x$ and $y$ of $X$, $x \,\Delta\, y$ or $y \,\Delta\, x$

Clearly, the order relation $\Delta$ on $\mathcal{P}(A)$ just described is not linear (unless $A$ is empty or contains just one member). The principal examples of linear order relations appear in the study of number systems, which we shall take up in due course.

Again let $X$ be any nonempty set. One says that a relation $\Delta$ on $X$ is an *equivalence relation* iff it satisfies the following conditions:

- (•) for any member $x$ of $X$, $x \,\Delta\, x$
- (•) for any members $x$ and $y$ of $X$, if $x \,\Delta\, y$ then $y \,\Delta\, x$
- (•) for any members $x$, $y$, and $z$ of $X$, if $x \,\Delta\, y$ and $y \,\Delta\, z$ then $x \,\Delta\, z$

With reference to the second of the foregoing conditions, one says that the relation $\Delta$ on $X$ is *symmetric*.

One can best understand the concept of equivalence relation through the corresponding idea of Partition. By a *partition* of $X$, one means any subset $\mathcal{Q}$ of $\mathcal{P}(X)$ which meets the following conditions:

($\bullet$) for any member $W$ of $\mathcal{Q}$, $W \neq \emptyset$

($\bullet$) for any members $W'$ and $W''$ of $\mathcal{Q}$, $W' = W''$ or $W' \cap W'' = \emptyset$

($\bullet$) $\cup \mathcal{Q} = X$

Given a partition $\mathcal{Q}$ of $X$, one often refers to the various members of $\mathcal{Q}$ as the *fibers* of the partition. Of course, the fibers are nonempty mutually disjoint subsets of $X$, the union of which equals $X$ itself. Thus, one may define a partition of $X$ by breaking $X$ into nonempty mutually disjoint subsets.

We contend that every equivalence relation $\Delta$ on $X$ defines a particular partition $\bar{\mathcal{Q}}$ of $X$ and that every partition $\mathcal{Q}$ of $X$ defines a particular equivalence relation $\bar{\Delta}$ on $X$. Moreover, we contend that these correspondences are inverse to one another. We mean to say that, for any equivalence relation $\Delta$ on $X$ and for any partition $\mathcal{Q}$ of $X$, if $\Delta$ defines $\mathcal{Q}$ (so that $\mathcal{Q} = \bar{\mathcal{Q}}$) then $\mathcal{Q}$ defines $\Delta$ (so that $\Delta = \bar{\Delta}$) and if $\mathcal{Q}$ defines $\Delta$ (so that $\Delta = \bar{\Delta}$) then $\Delta$ defines $\mathcal{Q}$ (so that $\mathcal{Q} = \bar{\mathcal{Q}}$). Let us begin with a partition $\mathcal{Q}$ of $X$. Let $\bar{\Delta}$ be the relation on $X$ consisting of all ordered pairs $(x', x'')$ in $X \times X$ for which there is some $W$ in $\mathcal{Q}$ such that $x' \in W$ and $x'' \in W$. Clearly, $\bar{\Delta}$ so defined is an equivalence relation on $X$.

In turn, let $\Delta$ be an equivalence relation on $X$. By a *fiber* following $\Delta$, one means any subset $W$ of $X$ which satisfies the following conditions:

($\bullet$) $W \neq \emptyset$

($\bullet$) for any members $x'$ and $x''$ of $X$, if $x' \in W$ and $x'' \in W$ then $x' \, \Delta \, x''$

($\bullet$) for any members $x'$ and $x''$ of $X$, if $x' \in W$ and $x'' \notin W$ then $x' \not\Delta x''$

Let $\bar{\mathcal{Q}}$ be the set of all such fibers. Now one can easily verify that $\bar{\mathcal{Q}}$ so defined is a partition of $X$. The basic step of the verification occurs in noting that, for any member $y$ of $X$, the subset:

$$\{ \, x \in X \, : \, x \, \Delta \, y \, \}$$

of $X$ is a fiber following $\Delta$.

By straightforward argument, one can show that the foregoing correspondences between equivalence relations on $X$ and partitions of $X$ are inverse to one another.

*Mappings*

05° Let us now consider the fundamental concept of Mapping. By a *mapping*, one means any ordered triple $(A, f, B)$, where $A$ and $B$ are sets and where $f$ is a subset of $A \times B$ which meets the following condition:

($\bullet$) for each member $x$ of $A$, there is precisely one member $y$ of $B$ for which $(x, y) \in f$

One refers to $A$ as the *domain*, to $B$ as the *codomain*, and to $f$ as the *graph* of the mapping. For each member $x$ of $A$, one refers to corresponding member $y$ of $B$ (uniquely determined by the condition $(x, y) \in f$) as the *image* of $x$ under $f$, and one denotes it by $f(x)$.

We emphasize the fact that a mapping consists of three parts: the domain, the codomain, and the graph. In order to show that two mappings $(A_1, f_1, B_1)$ and $(A_2, f_2, B_2)$ are equal, one must show that $A_1 = A_2$, $B_1 = B_2$, and $f_1 = f_2$. The last of these conditions means that, for any member $x$ of the common domain, $f_1(x) = f_2(x)$.

Let us consider several examples of mappings. First, let $A$ be any set. Let $1_A$ be the subset of $A \times A$ consisting of all ordered pairs $(x, y)$ for which $x = y$. Clearly, $1_A$ meets condition characterizing graphs. One refers to the mapping $(A, 1_A, A)$ as the *identity mapping* on $A$. For each member $x$ of $A$, $1_A(x) = x$.

Now let $A$ and $B$ be any sets for which $A \subseteq B$. Let $1_A^B$ be the subset of $A \times B$ consisting of all ordered pairs $(x, y)$ in $A \times B$ for which $x = y$. Clearly, $1_A^B$ meets relevant condition. One refers to the mapping $(A, 1_A^B, B)$ as the *inclusion mapping* carrying $A$ to $B$. For each member $x$ of $A$, $1_A^B(x) = x$.

Obviously, for a given set $A$, the identity mapping on $A$ and the inclusion mapping carrying $A$ to itself are equal.

Again let $A$ be any set. Let $\delta_A$ be the subset of $A \times (A \times A)$ consisting of all ordered pairs $(x, (y, z))$ for which $y = x$ and $z = x$. It is clear that $\delta_A$ meets the condition characterizing graphs. The mapping $(A, \delta_A, A \times A)$ is called the *diagonal mapping* carrying $A$ to $A \times A$. For each member $x$ of $A$, $\delta_A(x) = (x, x)$.

Now let $A$ and $B$ be any sets. One obtains two mappings $(A \times B, p, A)$ and $(A \times B, q, B)$ by specifying $p$ and $q$ as follows:

$$p = \{\ ((x, y), z) \in (A \times B) \times A\ :\ z = x\ \}$$
$$q = \{\ ((x, y), z) \in (A \times B) \times B\ :\ z = y\ \}$$

One refers to $(A \times B, p, A)$ as the *first projection mapping* for $A \times B$ and to $(A \times B, q, B)$ as the *second projection mapping* for $A \times B$. Clearly, for any member $(x, y)$ of $A \times B$, $p((x, y)) = x$ and $q((x, y)) = y$.

To simplify notation, one often refers to a given mapping $(A, f, B)$ simply by mentioning its graph $f$. This practice is permissible only when the domain and codomain of the mapping have already been clearly established, or when they are described concurrently in some dependent phrase. For example, one often speaks of a 'mapping $f$ carrying $A$ to $B$'.

In practice, one defines a mapping by smoothly describing the sets $A$ and $B$ and by presenting the graph $f$ in terms of some sort of Formula. Let us consider a family of examples, involving the real number system $\mathbf{R}$. Thus, let $J$ be the closed finite interval $[\,0, 1\,]$ in $\mathbf{R}$. Let $c$ be any real number for which $0 \leq c \leq 4$. Let $f_c$ be the mapping carrying $J$ to itself defined as follows:

$$f_c(x) := cx(1 - x) \qquad (x \in J)$$

Of course, one ought to verify carefully that, for any number $x$ in $\mathbf{R}$, if $x \in J$ then $f_c(x) \in J$. To do so, one must apply the condition that $0 \leq c \leq 4$. In any case, one refers to the mapping $f_c$ as the *Verhulst mapping* with *parameter* $c$.

Let us draw attention to three special types of mappings. Thus, let $A$ and $B$ be any sets and let $f$ be any mapping carrying $A$ to $B$. One says that $f$ is *injective* iff, for any members $x'$ and $x''$ of $A$, if $x' \neq x''$ then $f(x') \neq f(x'')$. With reference to the foregoing examples, one should note that the various inclusion mappings and diagonal mappings are injective while the various projection mappings in general are not. Moreover, the various Verhulst mappings $f_c$ are not injective.

One says that $f$ is *surjective* iff, for any member $y$ of $B$, there is some member $x$ of $A$ such that $f(x) = y$. One should note that the various projection mappings are surjective while the various inclusion mappings and diagonal mappings in general are not. Moreover, the Verhulst mapping $f_4$ is surjective. However, for any real number $c$, if $0 \leq c < 4$ then the Verhulst mapping $f_c$ is not surjective.

Finally, one says that $f$ is *bijective* iff it is both injective and surjective.

By the *range* of a given mapping $f$ carrying $A$ to $B$, one means the subset of $B$ consisting of all members $y$ for which there is some member $x$ of $A$ such that $f(x) = y$. One denotes the range of $f$ by $f_*(A)$. Clearly, $f$ is surjective iff $f_*(A) = B$.

Now let $A$, $B$, and $C$ be any sets, let $f$ be any mapping carrying $A$ to $B$, and let $g$ be any mapping carrying $B$ to $C$. One may form the mapping $\kappa$ carrying $A$ to $C$ by applying $f$ and $g$ in sequence:

$$\kappa(x) := g(f(x)) \qquad (x \in A)$$

One refers to $\kappa$ as the *composition* of $f$ and $g$ and denotes it by $g \cdot f$. Thus:

$$(g \cdot f)(x) := g(f(x)) \qquad (x \in A)$$

Given any sets $A$ and $B$ and any mapping $f$ carrying $A$ to $B$, one can easily check that $f \cdot 1_A = f$ and $1_B \cdot f = f$. Hence, the various identity mappings play a neutral role for composition. Given any sets $A$, $B$, $C$, and $D$ and any mappings $f$, $g$, and $h$ carrying $A$ to $B$, $B$ to $C$, and $C$ to $D$, respectively, one can easily verify that $(h \cdot g) \cdot f = h \cdot (g \cdot f)$. Hence, the composition of mappings is associative.

In terms of composition, one obtains very sharp characterizations of injective and surjective mappings. Thus, let $A$ and $B$ be any nonempty sets and let $f$ be any mapping carrying $A$ to $B$. Let $g$ be any mapping carrying $B$ to $A$. One says that $g$ is a *left-inverse* of $f$ iff $g \cdot f = 1_A$, which is to say that, for any member $x$ of $A$, $g(f(x)) = x$. One says that $g$ is a *right-inverse* of $f$ iff $f \cdot g = 1_B$, which is to say that, for any member $y$ of $B$, $f(g(y)) = y$. We propose to prove that:

(1) $f$ is injective iff there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a left-inverse of $f$

(2) $f$ is surjective iff there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a right-inverse of $f$

Let us prove (1). We assume first that there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a left-inverse of $f$. We must prove that $f$ is injective. Let $x'$ and $x''$ be any members of $A$. We must prove that if $x' \neq x''$ then $f(x') \neq f(x'')$. In fact, we shall prove the contrapositive; that is, we shall prove that if $f(x') = f(x'')$ then $x' = x''$. Thus, if $f(x') = f(x'')$ then $x' = g(f(x')) = g(f(x'')) = x''$.• Now let us assume that $f$ is injective. We must define a mapping $g$ carrying $B$ to $A$ such that $g$ is a left-inverse of $f$. To that end, let us arbitrarily select some member $a$ of $A$. That done, let us introduce the subset $g$ of $B \times A$ consisting of all ordered pairs $(y, x)$ which satisfy one or the other of the following two logically exclusive conditions:

(1.1) $(x, y) \in f$ (in which case $y \in f_*(A)$)

(1.2) $y \notin f_*(A)$ and $x = a$

One can readily check that $g$ meets condition characterizing graphs. By design, the resulting mapping $g$ carrying $B$ to $A$ is a left-inverse of $f$.•

Let us prove (2). We first assume that there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a right-inverse of $f$. We must prove that $f$ is surjective. Let $y$ be any member of $B$. We must show that there is a member $x$ of $A$ for which $f(x) = y$. Obviously, $f(g(y)) = y$, so we may take $x$ to be $g(y)$.•

We should now complete the proof of (2) by showing that if $f$ is surjective then there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a right-inverse of $f$. However, for such purpose we require an axiom which we have not yet stated: the Axiom of Choice. We have postponed presentation of this axiom

until now because the statement of it employs the concept of mapping and because the immediate effect of the axiom (in completing the proof of (2)) is instructive.

(AXIOM 7) Axiom of Choice

For any sets $A$ and $B$ and for any mapping $G$ carrying $B$ to $\mathcal{P}(A)$, if, for any member $y$ of $B$, $G(y) \neq \emptyset$ then there is a mapping $g$ carrying $B$ to $A$ such that, for any member $y$ of $B$, $g(y) \in G(y)$.

Let us apply the Axiom of Choice to complete the proof of (2). Let $f$ be surjective. We must show that there exists a mapping $g$ carrying $B$ to $A$ such that $g$ is a right-inverse of $f$. Let $G$ be the mapping carrying $B$ to $\mathcal{P}(A)$ defined as follows:

$$G(y) := \{\ x \in A\ :\ f(x) = y\ \} \qquad\qquad (y \in B)$$

Since $f$ is surjective, $G$ meets the hypothesis in the Axiom of Choice. Hence, there is a mapping $g$ carrying $B$ to $A$ such that, for any member $y$ of $B$, $g(y) \in G(y)$, which is to say that $f(g(y)) = y$. It follows that $g$ is a right-inverse of $f$.•

Let us return to general considerations of left- and right-inverses. Again let $A$ and $B$ be any (nonempty) sets and let $f$ be any mapping carrying $A$ to $B$. One can readily prove that, for any mappings $g'$ and $g''$ carrying $B$ to $A$, if $g'$ is a left-inverse for $f$ and if $g''$ is a right-inverse for $f$ then $g' = g''$. It follows that there can be at most one mapping $g$ carrying $B$ to $A$ such that $g$ is both a left- and a right-inverse of $f$. When such a mapping $g$ does in fact exist, one says that $f$ is *invertible*. In that case, one refers to $g$ as the *inverse* of $f$ and denotes it by $f^{-1}$. By the foregoing assertions (1) and (2), it is plain that $f$ is invertible iff it is bijective.

*Sets of Mappings*

06° Let $A$ and $B$ be any nonempty sets. For many purposes, it is useful to know that the various mappings $(A, f, B)$ with domain $A$ and codomain $B$ themselves comprise a set. One denotes this set by $\mathcal{M}(A, B)$. One may say that $\mathcal{M}(A, B)$ is the set of all mappings $f$ carrying $A$ to $B$. We produce $\mathcal{M}(A, B)$ by the following baroque argument. Thus, for any such mapping $(A, f, B)$, we have:

$$f \subseteq A \times B$$

so that:

$$f \in \mathcal{P}(A \times B)$$

and hence:

$$\{f, B\} \subseteq \mathcal{P}((A \times B) \cup B)$$

Since:

$$(f, B) = \{\{f\}, \{f, B\}\}$$

we have:

$$(f, B) \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\ (A \times B) \cup B\ )))$$

Since:

$$(A, f, B) = \{\{A\}, \{A, (f, B)\}\}$$

we have:

$$(A, f, B) \in \mathcal{P}(\mathcal{P}(\ \mathcal{P}(A)\ \cup\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\ (A \times B) \cup B\ )))\ ))$$

Now one may apply the Axiom of Specification to define $\mathcal{M}(A, B)$ as a subset of:

$$\mathcal{P}(\mathcal{P}(\ \mathcal{P}(A)\ \cup\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\ (A \times B) \cup B\ )))\ ))$$

*Indexed Sets*

07° We shall consider now a useful variation in terminology and notation involving mappings. Thus, let $J$ and $Y$ be any (nonempty) sets and let $\mu$ be any mapping carrying $J$ to $Y$. One sometimes refers to the range of $\mu$ as an *indexed subset* of $Y$, with *index mapping* $\mu$. For each member $j$ of $J$, one writes $\mu_j$ instead of $\mu(j)$ and one writes $\{\mu_j\}_{j \in J}$ instead of $\mu$. The intent of this variation is to emphasize the members of the range of $\mu$, without losing sight of $\mu$ itself.

In turn, let $M$ be any mapping carrying $J$ to $\mathcal{X} := \mathcal{P}(Y)$. One sometimes refers to the range of $M$ as an *indexed family* of subsets of $Y$. As just noted, one writes the more elaborate symbol $\{M_j\}_{j \in J}$ in place of $M$, where, for any member $j$ of $J$, $M_j$ stands for $M(j)$. One writes $\cup_{j \in J} M_j$ in place of $\cup M_*(J)$ and $\cap_{j \in J} M_j$ in place of $\cap M_*(J)$.

Now let $\{M_j\}_{j \in J}$ be any indexed family of sets. Of course, one presumes that all the sets $M_j$ are included in some ambient set $Y$; for present purposes, we may (and shall) take $Y$ to be $\cup_{j \in J} M_j$. By suitable application of the Axiom of Specification to the set $\mathcal{M}(J, Y)$, we may form the set of all mappings $\mu$ carrying $J$ to $Y$ and meeting the following condition:

($\bullet$) for any member $j$ of $J$, $\mu(j) \in M_j$

One refers to this set as the *cartesian product* of the indexed family $\cup_{j \in J} M_j$ and denotes it by $\prod_{j \in J} M_j$. Recalling the Axiom of Choice, one can readily prove that the cartesian product $\prod_{j \in J} M_j$ is nonempty iff, for any member $j$ of $J$, $M_j$ is nonempty.

Finally, let $J$ contain just two members: $J = \{j', j''\}$. To develop mental toughness, one should describe the difference between the (new) cartesian

product $\prod_{j \in J} M_j$ and the (old) cartesian product $M_{j'} \times M_{j''}$; and one should argue that the distinction is unimportant.

*Operations*

08° Let us mention an important special case of mapping: the concept of Operation. Let $X$ be any set. By an *operation* on $X$, one means any mapping $\theta$ carrying $X \times X$ to $X$. Given any members $x'$ and $x''$ of $X$, one usually writes $x' \; \theta \; x''$ in place of $\theta(x', x'')$.

The operations of addition and multiplication on the basic number systems (involving the integers, the rational numbers, the real numbers, and the complex numbers) are important examples. We shall initiate studies of these and many other examples in the next section.

## 3 The Concept of Ring

*Basic Definitions*

09° Let $X$ be any set and let $A$ and $M$ be operations on $X$. Given any members $x$ and $y$ of $X$, let us write $x + y$ in place of $A(x, y)$ and let us write $x \cdot y$ in place of $M(x, y)$. Let us refer to $A$ as the operation of *addition* on $X$ and to $M$ as the operation of *multiplication* on $X$. One says that the set $X$ supplied with the operations $A$ and $M$ is a *ring* iff the following conditions are satisfied:

(•) for any members $x$, $y$, and $z$ of $X$, $(x + y) + z = x + (y + z)$

(•) there exists a member 0 of $X$ such that, for any member $x$ of $X$, $x + 0 = x$ and $0 + x = x$

(•) for any member $x$ of $X$, there exists a member $y$ of $X$ such that $x + y = 0$ and $y + x = 0$

(•) for any members $x$ and $y$ of $X$, $x + y = y + x$

(•) for any members $x$, $y$, and $z$ of $X$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(•) there exists a member 1 of $X$ such that, for any member $x$ of $X$, $x \cdot 1 = x$ and $1 \cdot x = x$

(•) for any members $x$, $y$, and $z$ of $X$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$

(•) $0 \neq 1$

With regard to the second and the sixth of the foregoing conditions, one can show that the indicated members 0 and 1 of $X$ are unique. One refers to 0

as the *neutral* member of $X$ under addition and to 1 as the *neutral* member of $X$ under multiplication. The eighth condition requires that 0 and 1 be distinct. With regard to third of the foregoing conditions, one can show that, for any member $x$ of $X$, the indicated member $y$ of $X$ is unique. One refers to $y$ as the *additive inverse* of $x$ and one usually denotes it by $-x$. Noting the symmetric relation between $x$ and $y$, one may infer that not only $-x = y$ but also $-y = x$, which is to say that $-(-x) = x$.

It may happen that a given ring $X$ satisfies the following additional condition:

($\bullet$) for any members $x$ and $y$ of $X$, $x \cdot y = y \cdot x$.

In that case, one says that $X$ is *commutative*.

For any ring $X$, one can prove the following elementary results:

(1) for any member $w$ of $X$, if $w + w = w$ then $w = 0$

(2) for any member $x$ of $X$, $0 \cdot x = 0$ and $x \cdot 0 = 0$

(3) for any member $x$ of $X$, $(-1) \cdot x = -x$ and $x \cdot (-1) = -x$

(4) for any members $x$ and $y$ of $X$, $-(x+y) = (-x) + (-y)$, $(-x) \cdot y = -(x \cdot y)$, $x \cdot (-y) = -(x \cdot y)$, and $(-x) \cdot (-y) = xy$

*Examples*

10° Of course, the set $\mathbf{Z}$ consisting of all integers (together with the usual operations of addition and multiplication) is a commutative ring. Similarly, the set $\mathbf{Q}$ consisting of all rational numbers, the set $\mathbf{R}$ consisting of all real numbers, and the set $\mathbf{C}$ consisting of all complex numbers are commutative rings. These are the basic number systems of elementary Mathematics. We shall review the distinctive properties of these rings in the following section. For the present, we shall make use of these rings to describe other examples of rings, the properties of which are less familiar. (See the section of Problems at the end of these notes.) Such examples compel us to pay attention to formal definitions and to careful arguments.

*Example: Boolean Rings*

11° Let us first consider examples based upon formation of Unions and Intersections of sets. Thus, let $Y$ be any (nonempty) set and let $\mathcal{X}$ be the family of

all subsets of $Y$. One may introduce operations of addition and multiplication on $\mathcal{X}$ as follows:

$$W' + W'' := (W' \backslash W'') \cup (W'' \backslash W') \qquad (W' \in \mathcal{X}, \quad W'' \in \mathcal{X})$$

$$W' \cdot W'' := W' \cap W''$$

(See article 25•.) One can easily verify that $\mathcal{X}$ (supplied with the indicated operations of addition and multiplication) is a commutative ring. In fact, the neutral members of $\mathcal{X}$ under addition and multiplication are $\emptyset$ and $Y$. Moreover, for any member $W$ of $\mathcal{X}$, $-W = W$. As a sidelight, we note that, for any member $W$ of $\mathcal{X}$, $W^2 := W \cdot W = W$. One refers to the ring $\mathcal{X}$ as the *boolean ring based on* $Y$.

*Example: Modular Arithmetic*

12° Second, let us consider examples based upon Modular Arithmetic. Thus, let $k$ be any integer for which $2 \leq k$. In terms of $k$, one defines a relation on $\mathbf{Z}$, as follows. For any members $j'$ and $j''$ of $\mathbf{Z}$, one says that $j'$ and $j''$ are *equivalent modulo* $k$ iff $j'' - j'$ is divisible by $k$, which is to say that there exists a member $j$ of $\mathbf{Z}$ such that $j'' - j' = j \cdot k$. To express this relation, we shall write $j' \equiv_k j''$. Clearly, the relation on $\mathbf{Z}$ just defined is an equivalence relation. Let $\mathbf{Z}_k$ stand for the family of all equivalence classes $J$ following this relation. We plan to show that (under suitable operations of addition and multiplication) $\mathbf{Z}_k$ proves to be a (commutative) ring.

Let $J'$ and $J''$ be any equivalence classes in $\mathbf{Z}_k$. Let $j'$ be any member of $J'$ and let $j''$ be any member of $J''$. One defines $J' + J''$ to be the equivalence class in $\mathbf{Z}_k$ which contains $j' + j''$ and $J' \cdot J''$ to be the equivalence class in $\mathbf{Z}_k$ which contains $j' \cdot j''$. Of course, one must check that the resulting equivalence classes $J' + J''$ and $J' \cdot J''$ are the same no matter which members $j'$ of $J'$ and $j''$ of $J''$ be chosen initially. That done, one may verify that $\mathbf{Z}_k$ (supplied with the operations of addition and multiplication just defined) is a commutative ring. In fact, the neutral member of $\mathbf{Z}_k$ under addition is the equivalence class containing 0 and the neutral member of $\mathbf{Z}_k$ under multiplication is the equivalence class containing 1. Moreover, for any member $j$ of $\mathbf{Z}$, the equivalence class containing $j$ and the equivalence class containing $-j$ are the additive inverses of one another. One refers to the ring $\mathbf{Z}_k$ as the *ring of integers modulo* $k$.

For any member $j$ of $\mathbf{Z}$, there are members $\hat{\jmath}$ and $\bar{\jmath}$ of $\mathbf{Z}$ such that $j = \hat{\jmath} \cdot k + \bar{\jmath}$ and $0 \leq \bar{\jmath} < k$. Moreover, $\hat{\jmath}$ and $\bar{\jmath}$ are determined by $j$ and $k$. One refers to $\bar{\jmath}$ as the *remainder* for $j$ *modulo* $k$. One can easily show that, for any members $j'$ and $j''$ of $\mathbf{Z}$, $j' \equiv_k j''$ iff $\bar{\jmath}' = \bar{\jmath}''$. Hence, for any member $j$ of $\mathbf{Z}$, the equivalence class $J$ in $\mathbf{Z}_k$ containing $j$ contains precisely one among the possible remainders:

$$0, \ \ 1, \ \ 2, \ldots, \ \ k-1$$

modulo $k$, namely, $\bar{\jmath}$. It follows that there are precisely $k$ equivalence classes in $\mathbf{Z}_k$, since they stand in bijective correspondence with the remainders just displayed. Now one may identify the equivalence classes in $\mathbf{Z}_k$ with the various remainders modulo $k$ and one may regard the operations of addition and multiplication on $\mathbf{Z}_k$ as operations on the remainders. Thus, for any remainders $\bar{\jmath}'$ and $\bar{\jmath}''$, one would have:

$$\bar{\jmath}' + \bar{\jmath}'' = \overline{\jmath' + \jmath''}$$
$$\bar{\jmath}' \cdot \bar{\jmath}'' = \overline{\jmath' \cdot \jmath''}$$

*Example: Matrix Rings*

13° Now let us consider examples based upon Matrix Arithmetic. Let $X$ be any commutative ring. One might take $X$ to be $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, or $\mathbf{C}$. Let $\mathbf{X}$ be the family of all (two by two) matrices having entries in $X$. Thus, the members of $\mathbf{X}$ have the form:

$$T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

where $a$, $b$, $c$, and $d$ are any members of $X$. One may introduce operations of addition and multiplication on $\mathbf{X}$ as follows:

$$T' + T'' := \begin{pmatrix} a' + a'' & c' + c'' \\ b' + b'' & d' + d'' \end{pmatrix}$$
$$T' \cdot T'' := \begin{pmatrix} a' \cdot a'' + c' \cdot b'' & a' \cdot c'' + c' \cdot d'' \\ b' \cdot a'' + d' \cdot b'' & b' \cdot c'' + d' \cdot d'' \end{pmatrix} \qquad (T' \in \mathbf{X}, \quad T'' \in \mathbf{X})$$

By patient computation, one can verify that $\mathbf{X}$ (supplied with the indicated operations of addition and multiplication) is a ring. The neutral members of $\mathbf{X}$ under addition and multiplication are the following:

$$0 := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Moreover, for any member $T$ of $\mathbf{X}$:

$$-T = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}$$

One refers to the ring $\mathbf{X}$ as the *ring of (two by two) matrices* with entries in $X$. It is definitely not commutative.

*Constructions*

14° Finally, let us consider the concepts of *subring* and *product ring*, from which many new examples can be derived. Let $X$ be any ring. Let $X_\circ$ be a subset of $X$ which meets the following conditions:

(•) for any members $x'$ and $x''$ of $X$, if $x' \in X_\circ$ and $x'' \in X_\circ$ then $x' + x'' \in X_\circ$

(•) for any members $x'$ and $x''$ of $X$, if $x' \in X_\circ$ and $x'' \in X_\circ$ then $x' \cdot x'' \in X_\circ$

(•) $0 \in X_\circ$ and $1 \in X_\circ$

Under these conditions, it is plain that $X_\circ$ itself is a ring. The operations of addition and multiplication on $X_\circ$ are in a sense *inherited* from $X$. One refers to $X_\circ$ as a *subring* of $X$.

In time, we shall see that $\mathbf{Z}$ is a subring of $\mathbf{Q}$, that $\mathbf{Q}$ is a subring of $\mathbf{R}$, and that $\mathbf{R}$ is a subring of $\mathbf{C}$.

Now let $X'$ and $X''$ be any rings. Let $X' \times X''$ be the cartesian product of (the sets) $X'$ and $X''$. One proceeds to define operations of addition and multiplication on $X' \times X''$ as follows:

$$\begin{aligned} (x', x'') + (y', y'') &:= (x' + y', x'' + y'') \\ & \qquad ((x', x''),\ \ (y', y'') \in X' \times X'') \\ (x', x'') \cdot (y', y'') &:= (x' \cdot y', x'' \cdot y'') \end{aligned}$$

Of course, the operations on $X' \times X''$ which appear on the left are defined in terms of the given operations on $X'$ and $X''$ (which appear on the right). One can easily verify that, under the operations just indicated, $X' \times X''$ is a ring. In particular, the neutral members of $X' \times X''$ are $(0', 0'')$ and $(1', 1'')$, where $0'$ and $1'$ are the neutral members of $X'$ and $0''$ and $1''$ are the neutral members of $X''$. Moreover, for any member $(x', x'')$ of $X' \times X''$, the additive inverse of $(x', x'')$ in $X' \times X''$ is $(-x', -x'')$, where $-x'$ is the additive inverse of $x'$ in $X'$ and where $-x''$ is the additive inverse of $x''$ in $X''$. One refers to $X' \times X''$ (supplied with the indicated operations) as the *product* of the given rings $X'$ and $X''$.

One may generalize the foregoing construction, to obtain products of any (finite number) of given rings, such as $X_1 \times X_2 \times \times X_3 \times X_4$. In fact, one may form the product of any indexed family $\{X_j\}_{j \in J}$ of rings:

$$\prod_{j \in J} X_j$$

if that be useful.

*Ordered Rings*

15° Let $X$ be a ring and let $\leq$ be an order relation on $X$. Given any members $x$ and $y$ of $X$, we shall write $x < y$ to express the condition that $x \leq y$ but $x \neq y$.

One says that the ring $X$ supplied with the order relation $\leq$ is an *ordered ring* iff the following conditions are satisfied:

- (•) X is commutative
- (•) $\leq$ is linear
- (•) for any members $x$, $y$, and $z$ of $X$, if $x < y$ then $x + z < y + z$
- (•) for any members $x$, $y$, and $z$ of $X$, if $x < y$ and $0 < z$ then $x \cdot z < y \cdot z$
- (•) for any members $x$, $y$, and $z$ of $X$, if $x < y$ and $z < 0$ then $y \cdot z < x \cdot z$

In this context, one can readily show that:

- (5) for any members $x$ and $y$ of $X$, if $0 < x$ and $0 < y$ then $0 < x + y$
- (6) for any members $x$ and $y$ of $X$, if $0 < x$ and $0 < y$ then $0 < x \cdot y$
- (7) for any members $x$ and $y$ of $X$, $x < y$ iff $0 < y - x$
- (8) $-1 < 0 < 1$

By convention, one denotes the subset of $X$ consisting of all members $x$ for which $x < 0$ by $X^-$ and one refers to the members of $X^-$ as *negative*. Similarly, one denotes the subset of $X$ consisting of all members $x$ for which $0 < x$ by $X^+$ and one refers to the members of $X^+$ as *positive*. Clearly, the sets $X^-$, $\{0\}$, and $X^+$ comprise a partition of $X$:

$$X = X^- \cup \{0\} \cup X^+$$

Moreover, for any member $x$ of $X$, $x \in X^+$ iff $-x \in X^-$.

Now let $X$ be an ordered ring. Let $Y$ be any subset of $X$. One says that $Y$ admits a *smallest* member iff there is a member $a$ of $Y$ such that, for each member $y$ of $Y$, $a \leq y$. Such a member $a$ of $Y$ would be unique (if it exists). It would of course be the smallest member of $Y$. In turn, one says that $Y$ admits a *largest* member iff there is a member $b$ of $Y$ such that, for each member $y$ of $Y$, $y \leq b$. Such a member $b$ of $Y$ would be unique (if it exists). It would of course be the largest member of $Y$. Let $z$ be any member of $X$. One says that $z$ is a *lower bound* for $Y$ iff, for each member $y$ of $Y$, $z \leq y$. In turn, one says that $z$ is an *upper bound* for $Y$ iff, for each member $y$

of $Y$, $y \leq z$. We shall denote by $Y_*$ and by $Y^*$ the subsets of $X$ consisting of all lower bounds for $Y$ and of all upper bounds for $Y$, respectively. Of course, either $Y_*$ or $Y^*$ may be empty.

We are now prepared to state two fundamental conditions bearing upon the ordered ring $X$. Each of the conditions has two logically equivalent guises. We shall say that $X$ satisfies Condition (Z) iff it meets one or the other (and hence both) of the following two conditions:

(Z.1) for any subset $Y$ of $X$, if $Y \neq \emptyset$ and $Y_* \neq \emptyset$ then $Y$ admits a smallest member

(Z.2) for any subset $Y$ of $X$, if $Y \neq \emptyset$ and $Y^* \neq \emptyset$ then $Y$ admits a largest member

We shall say that $X$ satisfies Condition (R) iff it meets one or the other (and hence both) of the following two conditions:

(R.1) for any subset $Y$ of $X$, if $Y \neq \emptyset$ and $Y_* \neq \emptyset$ then $Y_*$ admits a largest member

(R.2) For any subset $Y$ of $X$, if $Y \neq \emptyset$ and $Y^* \neq \emptyset$ then $Y^*$ admits a smallest member

In terms of these conditions, we shall be able to characterize the basic rings $\mathbf{Z}$ and $\mathbf{R}$ among all possible rings.

*Fields*

16° By a *field*, one means any ring $X$ which satisfies the following conditions:

(•) X is commutative

(•) for any member $x$ of $X$, if $x \neq 0$ then $x$ is invertible

In this regard, see Problem 7.

Of course, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are fields but $\mathbf{Z}$ is not.

Let $X$ be a field and let $X_\circ$ be a subring of $X$. It may happen that, for any member $x$ of $X$, if $x \in X_\circ$ and $x \neq 0$ then $x^{-1} \in X_\circ$. In that case, $X_\circ$ would itself be a field, one would say a *subfield* of $X$.

*Ordered Fields*

17° By an *ordered field*, one means an ordered ring $X$ which is in fact a field. Given an ordered field $X$, one can easily prove that:

(9) for any members $x$ and $y$ of $X$, if $0 < x < y$ then $0 < y^{-1} < x^{-1}$

## 3 Number Systems

*The Ring of Integers*

18° By a *ring of integers*, one means an ordered ring $X$ which satisfies Condition (Z). In point of fact, any two such rings must be isomorphic. (See article $32^{\bullet}$.) However, the argument by which one justifies this assertion is far from trivial. In any case, for all mathematical purposes, all such rings are indistinguishable. One selects such a ring arbitrarily, denotes it by $\mathbf{Z}$, and calls it the Ring of Integers. One refers to the various members of $\mathbf{Z}$ as *integers*.

One often refers to Condition (Z.1) as the Least Integer Principle. In the following section, we shall show that Condition (Z.1) lies behind the widely applied method of Argument by Mathematical Induction.

*The Field of Real Numbers*

19° By a *field of real numbers*, one means an ordered field $X$ which satisfies Condition (R). In point of fact, any two such fields must be isomorphic. (See article $32^{\bullet}$.) However, the argument by which one justifies this assertion is far from trivial. In any case, for all mathematical purposes, all such fields are indistinguishable. One selects such a field arbitrarily, denotes it by $\mathbf{R}$, and calls it the Field of Real Numbers. One refers to the various members of $\mathbf{R}$ as *real numbers*.

One often refers to Condition (R.2) as the Least Upper Bound Principle. It lies behind all the major results of the Calculus.

Given the field $\mathbf{R}$ of real numbers, one may define a subring $X$ of $\mathbf{R}$ which satisfies Condition (Z). Naturally, one would identify $X$ as the ring $\mathbf{Z}$ of integers. The construction proceeds as follows. Let us say that a given subset $Y$ of $\mathbf{R}$ is *balanced* iff it meets the following conditions:

($\bullet$) $0 \in Y$

($\bullet$) for any member $x$ of $\mathbf{R}$, if $x \in Y$ then $x - 1 \in Y$ and $x + 1 \in Y$

Let $\mathcal{Z}$ be the set of all balanced subsets of $\mathbf{R}$. Since $\mathbf{R}$ itself is balanced, it is plain that $\mathcal{Z}$ is not empty. Let $X := \cap\mathcal{Z}$. Now one can prove that $X$ is a subring of $\mathbf{R}$ which meets Condition (Z).

Conversely, given the ring $\mathbf{Z}$ of integers, one may proceed to construct an ordered field $X$ which satisfies Condition (R). It turns out that $\mathbf{Z}$ is a subring of $X$. Naturally, one would identify $X$ as the field $\mathbf{R}$ of real numbers. The construction is both complicated and interesting. One first produces the field $\mathbf{Q}$ of rational numbers as the *quotient field* of $\mathbf{Z}$, then the field $\mathbf{R}$ as the *completion* of $\mathbf{Q}$.

*The Field of Rational Numbers*

20° Let the field $\mathbf{R}$ of real numbers be given and let the ring $\mathbf{Z}$ of integers be identified as a subring of $\mathbf{R}$. The Field $\mathbf{Q}$ of Rational Numbers may be identified as the subset of $\mathbf{R}$ consisting of all members of the following form:

$$x \cdot y^{-1}$$

where $x$ and $y$ are any members of $\mathbf{Z}$ such that $y \neq 0$. Clearly, $\mathbf{Q}$ is a subfield of $\mathbf{R}$. One refers to the various members of $\mathbf{Q}$ as *rational numbers*.

*The Principle of Archimedes*

21° With reference to article 15°, let $\mathbf{Z}^*$ be the set of all upper bounds for $\mathbf{Z}$. We contend that $\mathbf{Z}^* = \emptyset$. If it were not so then, by Condition (R), we could introduce the smallest member $x$ of $\mathbf{Z}^*$. Since $x - 1 \notin \mathbf{Z}^*$, we could then introduce a member $k$ of $\mathbf{Z}$ such that $x - 1 < k$. It would follow that $k + 1 \in \mathbf{Z}$ and that $x < k + 1$, in contradiction to the definition of $x$. Hence, $\mathbf{Z}^* = \emptyset$. One calls this conclusion the Principle of Archimedes:

(A) for all $w$ in $\mathbf{R}$, there is some $j$ in $\mathbf{Z}$ such that $w < j$

*The Field of Complex Numbers*

22° From the field $\mathbf{R}$ of real numbers, one may proceed to construct the Field $\mathbf{C}$ of Complex Numbers. Let $\mathbf{C} := \mathbf{R} \times \mathbf{R}$. One refers to the various members $z := (x, y)$ of $\mathbf{C}$ as *complex numbers*. When $y = 0$ one says that $z$ is *purely real*; when $x = 0$ one says that $z$ is *purely imaginary*

The operations of addition and multiplication on $\mathbf{C}$ are defined in the following way:

$$z' + z'' := (x' + x'', y' + y'')$$

$$(z' := (x', y'), \;\; z'' := (x'', y'') \in \mathbf{C})$$

$$z' \cdot z'' := (x' \cdot x'' - y' \cdot y'', x' \cdot y'' + y' \cdot x'')$$

By straightforward computation, one can check that $\mathbf{C}$ is a field. In particular, the neutral members of $\mathbf{C}$ are $0 := (0, 0)$ and $1 := (1, 0)$. Of course, for any member $z := (x, y)$ of $\mathbf{C}$, $-z = (-x, -y)$. Moreover, for any member $z := (x, y)$ of $\mathbf{C}$, if $z \neq 0$ then:

$$z^{-1} = (r^{-2}x, -r^{-2}y)$$

where $r := \sqrt{x^2 + y^2}$.

For any members $x'$ and $x''$ of $\mathbf{R}$, we have:

$$(x', 0) + (x'', 0) = (x' + x'', 0)$$
$$(x', 0) \cdot (x'', 0) = (x' \cdot x'', 0)$$

By these relations, the field $\mathbf{R}$ and the subfield $X$ of $\mathbf{C}$ consisting of all purely real complex numbers are isomorphic. (See Problem 8.) We are led to identify each real number $x$ with the corresponding (purely real) complex number $(x, 0)$. Under this identification, $\mathbf{R}$ appears as a subfield of $\mathbf{C}$. Now one may express the various complex numbers $z := (x, y)$ as follows:

$$z = (x, 0) + (0, 1) \cdot (y, 0) = x + i \cdot y$$

where $i$ stands for the (purely imaginary) complex number $(0, 1)$. The number $i$ satisfies the critical relation:

$$i \cdot i = -1$$

At this point, one may treat complex numbers as *expressions* of the form $x + iy$ (where $x$ and $y$ are any real numbers), to be added and multiplied according to the usual rules but with the proviso that $i^2 = -1$.

*The Axiom of Infinity*

23° We have described the Ring $\mathbf{Z}$ of Integers and the Fields $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ of Rational, Real, and Complex Numbers. We have also noted some of the relations among these number systems. In particular, $\mathbf{Z}$ is a subring of $\mathbf{Q}$, $\mathbf{Q}$ is a subfield of $\mathbf{R}$, and $\mathbf{R}$ is a subfield of $\mathbf{C}$. Moreover, given $\mathbf{Z}$, we may apply the foregoing axioms of Set Theory to construct ($\mathbf{Q}$ and) $\mathbf{R}$. Conversely, given $\mathbf{R}$, we may reconstruct $\mathbf{Z}$ and $\mathbf{Q}$. In any case, from $\mathbf{R}$ we may construct $\mathbf{C}$. However, these lines of development *presume* the existence of $\mathbf{Z}$ or $\mathbf{R}$ as a point of departure. One may naturally inquire whether such number systems as $\mathbf{Z}$ and $\mathbf{R}$ do in fact exist.

In fact, the axioms stated in the first section are not sufficient to guarantee the existence of the basic number systems of Mathematics. (Indeed, they do not guarantee the existence of any set!) We must introduce an axiom which asserts the existence of some sort of set adequate to serve as the foundation for constructing the basic number systems. Since the sets underlying these systems are *infinite*, the axiom in question must have substantial force. The following traditional axiom serves the purpose.

(AXIOM 8) Axiom of Infinity

There exists an infinite set.

We mean to say that there exists a set $X$ together with a mapping $f$ carrying $X$ to itself which is injective but not surjective. The mapping $f$ serves to express the condition that $X$ be infinite. Remarkably, such a set $X$ and such a mapping $f$ are sufficient to support the construction of a ring of integers.

A person who is troubled by the idea that one may cause a set to exist simply by saying that it is so, is not alone. The issue turns upon questions of Consistence and Inconsistence for Axiomatic Systems, and upon the philosophical positions of the Platonists and the Formalists.

## 5 Mathematical Induction

24° As usual, let $\mathbf{Z}$ be the ring of integers. Let us explain the relation between Condition (Z.1) and the widely applied method of argument called Mathematical Induction.

To that end, we must first show that 1 is the smallest member of $\mathbf{Z}^+$. We argue as follows. By Condition (Z.1), $\mathbf{Z}^+$ must admit a smallest member. Let it be denoted by $x$. Obviously, $0 < x \leq 1$. We claim that $x = 1$. Let us suppose to the contrary that $0 < x < 1$. Then $0 < x \cdot x < x$. Now $x \cdot x$ is a positive integer smaller than $x$. This contradiction entails that $x = 1$.

Now we are prepared to describe a Sharp Characterization of $\mathbf{Z}^+$. Thus, let $Y$ be any subset of $\mathbf{Z}$ which meets the following conditions:

(ZP.1) for any member $y$ of $Y$, $0 < y$

(ZP.2) $1 \in Y$

(ZP.3) for any member $y$ of $Y$, $y + 1$ is also a member of $Y$

Under these conditions, we contend that $Y$ must in fact equal $\mathbf{Z}^+$. By the first of the foregoing conditions, $Y \subseteq \mathbf{Z}^+$. Let $X := \mathbf{Z}^+ \backslash Y$. Of course, $X \cap Y = \emptyset$ and $\mathbf{Z}^+ = X \cup Y$. We shall prove that $X = \emptyset$, from which it will follow that $Y = \mathbf{Z}^+$. Let us suppose to the contrary that $X \neq \emptyset$. By Condition (Z.1), it is plain that $X$ admits a smallest member. Let it be denoted by $x$. Of course, $x \neq 1$ because (by the second of the foregoing conditions) $1 \in Y$. By the preceding remarks, it follows that $1 < x$. Now the positive integer $y := x - 1$ must be a member of $Y$ (because it cannot be a member of $X$). However, the third of the foregoing conditions entails that $y + 1$ (which equals $x$) must also be a member of $Y$. This contradiction forces the conclusion that $X = \emptyset$.•

Now let us describe argument by Mathematical Induction.

Typically, one begins with some sort of assertion $\gamma_k$ depending upon a positive integer $k$. For example:

($\gamma_k$) the sum of the first $k$ positive integers equals $\frac{1}{2}k(k+1)$

One then proceeds to show that the infinitely many assertions:

$$\gamma_1,\ \gamma_2,\ \gamma_3,\ \gamma_4,\ \ldots$$

can be proved, all at once, by Mathematical Induction. To that end, one proves the following two assertions:

(MI.1) $\gamma_1$

(MI.2) for any positive integer $k$, if $\gamma_k$ then $\gamma_{k+1}$

One then states that (by Mathematical Induction) all the foregoing assertions have been proved. Justification for this statement depends upon the foregoing Sharp Characterization of $\mathbf{Z}^+$. Thus, one imagines the set $Y$ of all positive integers $k$ for which the assertion $\gamma_k$ can be proved. Given that the assertions (MI.1) and (MI.2) have been proved, one can immediately check that $Y$ must meet the conditions (ZP.1), (ZP.2), and (ZP.3) characteristic of $\mathbf{Z}^+$. Hence, $Y$ must equal $\mathbf{Z}^+$, which is to say that, for any positive integer $k$, $\gamma_k$ can be proved.

## 6 Problems

*The Rules of DeMorgan*

25$^\bullet$ Let $Y$ be any set. For any subsets $U$ and $V$ of $Y$, one denotes by $U\backslash V$ the subset of $Y$ comprised of all elements $y$ which lie in $U$ but not in $V$. For any subset $W$ of $Y$, let us denote $Y\backslash W$ by $W^\circ$. Prove that, for any subsets $U$ and $V$ of $Y$, $(U \cup V)^\circ = U^\circ \cap V^\circ$ and $(U \cap V)^\circ = U^\circ \cup V^\circ$. These relations are the Rules of DeMorgan.

26$^\bullet$ Let $X$ be any nonempty set and let $\Delta$ be any linear order relation on $X$. Let $X^*$ stand for the set of all *ordered k-tuples* $\xi := (x_1, x_2, \ldots, x_k)$, where $k$ is any positive integer and where $x_1$, $x_2$, ... , and $x_k$ are any members of $X$. Show that $X^*$ is in fact a well-defined set. Let $\Delta^*$ be the relation on $X^*$ consisting of all ordered pairs $(\xi', \xi'')$ which meet one or the other of the following two conditions:

($\bullet$) $k' \leq k''$ and, for any integer $j$, if $1 \leq j \leq k'$ then $x'_j = x''_j$

($\bullet$) there is an integer $k$ such that $0 \leq k < k'$ and $0 \leq k < k''$, such that, for any integer $j$, if $1 \leq j \leq k$ then $x'_j = x''_j$, and such that $(x'_{k+1}, x''_{k+1}) \in \Delta$ but $x'_{k+1} \neq x''_{k+1}$

In this context, one refers to $X$ as the *alphabet*, to $X^*$ as the *lexicon*, and to $\Delta^*$ as the *lexicographic order* on $X^*$. Prove that $\Delta^*$ is a linear order relation on $X^*$.

*Groups of Mappings*

27• Let $X$ be any nonempty set. Let $\mathcal{F}$ be any set of bijective mappings carrying $X$ to itself such that:

- (•) $1_X$ is a member of $\mathcal{F}$
- (•) for any member $f$ of $\mathcal{F}$, $f^{-1}$ is also a member of $\mathcal{F}$
- (•) for any members $g$ and $h$ of $\mathcal{F}$, $g \cdot h$ is also a member of $\mathcal{F}$

One refers to such a set $\mathcal{F}$ as a *group* of mappings on $X$. In turn, let $\Delta$ be the relation on $X$ consisting of all ordered pairs $(x, y)$ such that:

- (•) there is some member $f$ of $\mathcal{F}$ for which $y = f(x)$

Prove that $\Delta$ is an equivalence relation on $X$. In this context, we may say that the group $\mathcal{F}$ *determines* the relation $\Delta$. Now show that, for any equivalence relation $\Delta$ on $X$, there exists a group $\mathcal{F}$ of mappings on $X$ such that $\mathcal{F}$ determines $\Delta$.

28• Let $c$ be a real number for which $0 \leq c \leq 4$. Let $f_c$ be the Verhulst mapping (carrying the interval $[\,0, 1\,]$ to itself) with parameter value $c$. Find all real numbers $x$ in $[\,0, 1\,]$ for which $f_c(f_c(x)) = x$. Of course, the answers will depend upon $c$.

29• Let $X$ be any ring. Let $x$ and $y$ be any members of $X$. Prove that there is precisely one member $z$ of $X$ such that $z + y = x$. One refers to $z$ as the *difference* between $x$ and $y$ and denotes it by $x-y$. Of course, $x-y = x+(-y)$.

30• Let $X$ be any ring. Let $x$ be any member of $X$. One says that $x$ is *invertible* iff there is some member $y$ of $X$ such that $x \cdot y = 1$ and $y \cdot x = 1$. Prove that such a member $y$ of $X$ (if it exists) must be unique. One refers to $y$ as the *inverse* of $x$ and denotes it by $x^{-1}$. Note that, for any member $x$ of $X$, if $x$ is invertible then $x^{-1}$ is also invertible and $(x^{-1})^{-1} = x$. Prove that, for any members $x$ and $y$ of $X$, if both $x$ and $y$ are invertible then $x \cdot y$ is also invertible and $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. Prove that the neutral member 0 of $X$ is not invertible. The last assertion formalizes the folk-theorem that "division by zero is impossible."

31• Let $X'$ and $X''$ be any rings. Let $H$ be a mapping carrying $X'$ to $X''$. One says that $H$ is an *isomorphism* iff the following conditions are satisfied:

- (•) $H$ is bijective
- (•) for any members $x$ and $y$ of $X'$, $H(x+y) = H(x) + H(y)$
- (•) for any members $x$ and $y$ of $X'$, $H(x \cdot y) = H(x) \cdot H(y)$

Given that $H$ is an isomorphism, verify that $H(0) = 0$ and $H(1) = 1$. In general, one says that $X'$ and $X''$ are *isomorphic* iff there exists an isomorphism $H$ carrying $X'$ to $X''$. Given that $X'$ and $X''$ are isomorphic, explain the sense in which $X'$ and $X''$ would be *Mathematically Indistinguishable*. Describe examples of rings $X'$ and $X''$ which are not isomorphic.

32• Let $X'$ and $X''$ be any ordered rings. Let $H$ be a mapping carrying $X'$ to $X''$. One says that $H$ is an *isomorphism* iff the following conditions are satisfied:

- (•) $H$ is bijective
- (•) for any members $x$ and $y$ of $X'$, $H(x+y) = H(x) + H(y)$
- (•) for any members $x$ and $y$ of $X'$, $H(x \cdot y) = H(x) \cdot H(y)$
- (•) for any members $x$ and $y$ of $X'$, $x \leq y$ iff $H(x) \leq H(y)$

In general, one says that $X'$ and $X''$ are *isomorphic* iff there exists an isomorphism $H$ carrying $X'$ to $X''$. Given that $X'$ and $X''$ are isomorphic, explain the sense in which $X'$ and $X''$ would be *Mathematically Indistinguishable*. Describe examples of ordered rings $X'$ and $X''$ which are not isomorphic.

33• Let $X$ be a ring. One says that $X$ is an *integral domain* iff it meets the following conditions:

- (•) $X$ is commutative
- (•) for any members $x$ and $y$ of $X$, if $x \neq 0$ and $y \neq 0$ then $x \cdot y \neq 0$

Prove that if $X$ is an ordered ring then it is an integral domain.

34• Let $X$ be any ring. For any members $x$ and $y$ of $X$, one says that $x$ is a *square root* for $y$ iff $x \cdot x = y$. Given a boolean ring $\mathcal{X}$, note that, for any $W'$ and $W''$ in $\mathcal{X}$, $W'$ is a square root for $W''$ iff $W' = W''$. For such a ring, every member $W$ admits precisely one square root, namely, itself. Now let $p$ be an odd prime positive integer. For the ring $\mathbf{Z}_p$ of integers modulo $p$, prove that there are precisely $(p+1)/2$ members which admit square roots. Note that

$\bar{0}$ admits just one square root (namely, itself), while the rest admit precisely two square roots. List the members of $\mathbf{Z}_{13}$ which admit square roots. In turn, let $\mathbf{X}$ be the ring of (two by two) matrices with entries in $\mathbf{Z}$. Let $T$ be any member of $\mathbf{X}$ of the form:

$$T = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

where $x$ is any nonzero integer. Prove that $T$ admits square roots (in fact, precisely two) iff $x$ is even. Find the (four) square roots of the identity matrix $I$. Finally, invent a (commutative) ring $X$ for which the neutral member 1 admits precisely eight square roots.

35• Let $X$ be an integral domain. Prove that, for any members $y'$ and $y''$ of $X$, if $y' \cdot y' = y'' \cdot y''$ then $y' = y''$ or $y' = -y''$. Conclude that, for any member $x$ of $X$, $x$ can have at most two square roots.

36• Let $k$ be any positive integer. Prove that:

($\gamma_k$) for any set $A$, if $A$ contains precisely $k$ members then $\mathcal{P}(A)$ contains precisely $2^k$ members.

*Complete Mathematical Induction*

37• See **Section 5**. For arguments by Mathematical Induction, one sometimes proves not conditions (MI.1) and (MI.2) but the following condition:

(MI.C) for any positive integer $k$, if [*for any positive integer $j$, if $j < k$ then $\gamma_j$*] then $\gamma_k$

Show that condition (MI.C) is equivalent to the conjunction of conditions (MI.1) and (MI.2). Arguments based upon condition (MI.C) are called arguments by Complete Mathematical Induction.

*The Principle of Archimedes: Second Form*

38• Prove that, for any $w$ in $\mathbf{R}^+$, there is some $j$ in $\mathbf{Z}^+$ such that $(1/j) < w$.

*Integral and Fractional Parts*

39• Let $x$ be any member of $\mathbf{R}$. Prove that there are members $k$ of $\mathbf{Z}$ and $z$ of $\mathbf{R}$ such that $x = k + z$ and $0 \leq z < 1$. Check that, so defined, $k$ and $z$ are "unique." One refers to $k$ as the *integral part* of $x$ and denotes it by $[x]$; one refers to $z$ as the *fractional part* of $x$ and denotes it by $(x)$. Of course, $x = [x] + (x)$.

## 7 Reference

For the development of the theory of Ordinal and of Cardinal Numbers, one requires two new axioms in addition to the eight described above, namely, the Axiom of Regularity and the Axiom of Comprehension. See the following reference.

Halmos, P. R., *Naive Set Theory*, Van Nostrand Reinhold, New York, 1960