Chapter 1

Background and Fundamentals of Mathematics

This chapter is fundamental, not just for algebra, but for all fields related to mathematics. The basic concepts are products of sets, partial orderings, equivalence relations, functions, and the integers. An equivalence relation on a set A is shown to be simply a partition of A into disjoint subsets. There is an emphasis on the concept of function, and the properties of surjective, injective, and bijective. The notion of a solution of an equation is central in mathematics, and most properties of functions can be stated in terms of solutions of equations. In elementary courses the section on the Hausdorff Maximality Principle should be ignored. The final section gives a proof of the unique factorization theorem for the integers.

Notation Mathematics has its own universally accepted shorthand. The symbol $\exists$ means "there exists" and $\exists!$ means "there exists a unique". The symbol $\forall$ means "for each" and $\Rightarrow$ means "implies". Some sets (or collections) are so basic they have their own proprietary symbols. Five of these are listed below.

$\mathbf{N} = \mathbf{Z}^+ =$ the set of positive integers $= \{1, 2, 3, ...\}$
$\mathbf{Z}$ = the ring of integers $= \{..., -2, -1, 0, 1, 2, ...\}$
$\mathbf{Q}$ = the field of rational numbers $= \{a/b : a, b \in \mathbf{Z}, b \neq 0\}$
$\mathbf{R}$ = the field of real numbers
$\mathbf{C}$ = the field of complex numbers $= \{a + bi : a, b \in \mathbf{R}\}$ $(i^2 = -1)$

Sets Suppose A, B, C,... are sets. We use the standard notation for intersection and union.

$A \cap B = \{x : x \in A \text{ and } x \in B\}$ = the set of all x which are elements of A and B.

$A \cup B = \{x : x \in A \text{ or } x \in B\}$ = the set of all x which are elements of A or B.

Any set called an index set is assumed to be non-void. Suppose T is an index set and for each $t \in T$, A_t is a set.

$$\bigcup_{t \in T} A_t = \{x : \exists\, t \in T \text{ with } x \in A_t\}$$

$$\bigcap_{t \in T} A_t = \{x : \text{if } t \in T, x \in A_t\} = \{x : \forall t \in T, x \in A_t\}$$

Let $\emptyset$ be the null set. If $A \cap B = \emptyset$, then A and B are said to be *disjoint.*

Definition Suppose each of A and B is a set. The statement that A is a subset of B $(A \subset B)$ means that if a is an element of A, then a is an element of B. That is, $a \in A \Rightarrow a \in B$. If $A \subset B$ we may say A is contained in B, or B contains A.

Exercise Suppose each of A and B is a set. The statement that A is not a subset of B means ________________________.

Theorem (De Morgan's laws) Suppose S is a set. If $C \subset S$ (i.e., if C is a subset of S), let C', the complement of C in S, be defined by $C' = S - C = \{x \in S : x \notin C\}$. Then for any $A, B \subset S$,

$$(A \cap B)' = A' \cup B' \quad \text{and}$$

$$(A \cup B)' = A' \cap B'$$

Cartesian Products If X and Y are sets, $X \times Y = \{(x, y) : x \in X \text{ and } y \in Y\}$. In other words, the Cartesian product of X and Y is defined to be the set of all ordered pairs whose first term is in X and whose second term is in Y.

Example $\mathbf{R} \times \mathbf{R} = \mathbf{R}^2$ = the plane.

Definition If each of $X_1, ..., X_n$ is a set, $X_1 \times \cdots \times X_n = \{(x_1, ..., x_n) : x_i \in X_i$ for $1 \leq i \leq n\}$ = the set of all ordered n-tuples whose i-th term is in X_i.

Example $\mathbf{R} \times \cdots \times \mathbf{R} = \mathbf{R}^n$ = real n-space.

Question Is $(\mathbf{R} \times \mathbf{R}^2) = (\mathbf{R^2} \times \mathbf{R}) = \mathbf{R^3}$?

Relations

If A is a non-void set, a non-void subset $R \subset A \times A$ is called a *relation* on A. If $(a, b) \in R$ we say that a is related to b, and we write this fact by the expression $a \sim b$. Here are several properties which a relation may possess.

1) If $a \in A$, then $a \sim a$. (reflexive)
2) If $a \sim b$, then $b \sim a$. (symmetric)
2′) If $a \sim b$ and $b \sim a$, then $a = b$. (anti-symmetric)
3) If $a \sim b$ and $b \sim c$, then $a \sim c$. (transitive)

Definition A relation which satisfies 1), 2′), and 3) is called a *partial ordering.* In this case we write $a \sim b$ as $a \leq b$. Then

1) If $a \in A$, then $a \leq a$.
2′) If $a \leq b$ and $b \leq a$, then $a = b$.
3) If $a \leq b$ and $b \leq c$, then $a \leq c$.

Definition A *linear ordering* is a partial ordering with the additional property that, if $a, b \in A$, then $a \leq b$ or $b \leq a$.

Example $A = \mathbf{R}$ with the ordinary ordering, is a linear ordering.

Example A = all subsets of $\mathbf{R}^2$, with $a \leq b$ defined by $a \subset b$, is a partial ordering.

Hausdorff Maximality Principle (HMP) Suppose S is a non-void subset of A and $\sim$ is a relation on A. This defines a relation on S. If the relation satisfies any of the properties 1), 2), 2′), or 3) on A, the relation also satisfies these properties when restricted to S. In particular, a partial ordering on A defines a partial ordering on S. However the ordering may be linear on S but not linear on A. The HMP is that any linearly ordered subset of a partially ordered set is contained in a maximal linearly ordered subset.

Exercise Define a relation on $A = \mathbf{R}^2$ by $(a, b) \sim (c, d)$ provided $a \leq c$ and $b \leq d$. Show this is a partial ordering which is linear on $S = \{(a, a) : a < 0\}$. Find at least two maximal linearly ordered subsets of $\mathbf{R}^2$ which contain S.

One of the most useful applications of the HMP is to obtain maximal monotonic collections of subsets.

Definition A collection of sets is said to be *monotonic* if, given any two sets of the collection, one is contained in the other.

Corollary to HMP Suppose X is a non-void set and A is some non-void collection of subsets of X, and S is a subcollection of A which is monotonic. Then $\exists$ a maximal monotonic subcollection of A which contains S.

Proof Define a partial ordering on A by $V \leq W$ iff $V \subset W$, and apply HMP.

The HMP is used twice in this book. First, to show that infinitely generated vector spaces have free bases, and second, in the Appendix, to show that rings have maximal ideals (see pages 87 and 109). In each of these applications, the maximal monotonic subcollection will have a maximal element. In elementary courses, these results may be assumed, and thus the HMP may be ignored.

Equivalence Relations A relation satisfying properties 1), 2), and 3) is called an *equivalence relation.*

Exercise Define a relation on $A = \mathbf{Z}$ by $n \sim m$ iff $n - m$ is a multiple of 3. Show this is an equivalence relation.

Definition If $\sim$ is an equivalence relation on A and $a \in A$, we define the *equivalence class* containing a by $cl(a) = \{x \in A : a \sim x\}$.

Theorem

1) If $b \in cl(a)$ then $cl(b) = cl(a)$. Thus we may speak of a subset of A being an equivalence class with no mention of any element contained in it.
2) If each of $U, V \subset A$ is an equivalence class and $U \cap V \neq \emptyset$, then $U = V$.
3) Each element of A is an element of one and only one equivalence class.

Definition A *partition* of A is a collection of disjoint non-void subsets whose union is A. In other words, a collection of non-void subsets of A is a partition of A provided any $a \in A$ is an element of one and only one subset of the collection. Note that if A has an equivalence relation, the equivalence classes form a partition of A.

Theorem Suppose A is a non-void set with a partition. Define a relation on A by $a \sim b$ iff a and b belong to the same subset of the partition. Then $\sim$ is an equivalence relation, and the equivalence classes are just the subsets of the partition.

Summary There are two ways of viewing an equivalence relation — one is as a relation on A satisfying 1), 2), and 3), and the other is as a partition of A into disjoint subsets.

Exercise Define an equivalence relation on $\mathbf{Z}$ by $n \sim m$ iff $n - m$ is a multiple of 3. What are the equivalence classes?

Exercise Is there a relation on $\mathbf{R}$ satisfying 1), 2), 2′) and 3) ? That is, is there an equivalence relation on $\mathbf{R}$ which is also a partial ordering?

Exercise Let $H \subset \mathbf{R}^2$ be the line $H = \{(a, 2a) : a \in \mathbf{R}\}$. Consider the collection of all translates of H, i.e., all lines in the plane with slope 2. Find the equivalence relation on $\mathbf{R}^2$ defined by this partition of $\mathbf{R}^2$.

Functions

Just as there are two ways of viewing an equivalence relation, there are two ways of defining a function. One is the “intuitive” definition, and the other is the “graph” or “ordered pairs” definition. In either case, *domain* and *range* are inherent parts of the definition. We use the “intuitive” definition because everyone thinks that way.

Definition If X and Y are (non-void) sets, a *function* or *mapping* or *map* with domain X and range Y, is an ordered triple (X, Y, f) where f assigns to each $x \in X$ a well defined element $f(x) \in Y$. The statement that (X, Y, f) is a function is written as $f : X \to Y$ or $X \xrightarrow{f} Y$.

Definition The *graph* of a function (X, Y, f) is the subset $\Gamma \subset X \times Y$ defined by $\Gamma = \{(x, f(x)) : x \in X\}$. The connection between the "intuitive" and "graph" viewpoints is given in the next theorem.

Theorem If $f : X \to Y$, then the graph $\Gamma \subset X \times Y$ has the property that each $x \in X$ is the first term of one and only one ordered pair in Γ. Conversely, if Γ is a subset of $X \times Y$ with the property that each $x \in X$ is the first term of one and only ordered pair in Γ, then $\exists!$ $f : X \to Y$ whose graph is Γ. The function is defined by "$f(x)$ is the second term of the ordered pair in Γ whose first term is x."

Example *Identity functions* Here $X = Y$ and $f : X \to X$ is defined by $f(x) = x$ for all $x \in X$. The identity on X is denoted by I_X or just $I : X \to X$.

Example *Constant functions* Suppose $y_0 \in Y$. Define $f : X \to Y$ by $f(x) = y_0$ for all $x \in X$.

Restriction Given $f : X \to Y$ and a non-void subset S of X, define $f \mid S : S \to Y$ by $(f \mid S)(s) = f(s)$ for all $s \in S$.

Inclusion If S is a non-void subset of X, define the inclusion $i : S \to X$ by $i(s) = s$ for all $s \in S$. Note that inclusion is a restriction of the identity.

Composition Given $W \xrightarrow{f} X \xrightarrow{g} Y$ define $g \circ f : W \to Y$ by $(g \circ f)(x) = g(f(x))$.

Theorem (The associative law of composition) If $V \xrightarrow{f} W \xrightarrow{g} X \xrightarrow{h} Y$, then $h \circ (g \circ f) = (h \circ g) \circ f$. This may be written as $h \circ g \circ f$.

Definitions Suppose $f : X \to Y$.

1) If $T \subset Y$, the *inverse image of* T is a subset of X, $f^{-1}(T) = \{x \in X : f(x) \in T\}$.

2) If $S \subset X$, the *image of* S is a subset of Y, $f(S) = \{f(s) : s \in S\} = \{y \in Y : \exists s \in S \text{ with } f(s) = y\}$.

3) The *image of* f is the image of X , i.e., image $(f) = f(X) = \{f(x) : x \in X\} = \{y \in Y : \exists x \in X \text{ with } f(x) = y\}$.

4) $f : X \to Y$ is *surjective* or *onto* provided image $(f) = Y$ i.e., the image is the range, i.e., if $y \in Y$, $f^{-1}(y)$ is a non-void subset of X.

5) $f : X \to Y$ is *injective* or *1-1* provided $(x_1 \neq x_2) \Rightarrow f(x_1) \neq f(x_2)$, i.e., if x_1 and x_2 are distinct elements of X, then $f(x_1)$ and $f(x_2)$ are distinct elements of Y.

6) $f : X \to Y$ is *bijective* or is a *1-1 correspondence* provided f is surjective and injective. In this case, there is function $f^{-1} : Y \to X$ with $f^{-1} \circ f = I_X : X \to X$ and $f \circ f^{-1} = I_Y : Y \to Y$. Note that $f^{-1} : Y \to X$ is also bijective and $(f^{-1})^{-1} = f$.

Examples

1) $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = \sin(x)$ is neither surjective nor injective.

2) $f : \mathbf{R} \to [-1, 1]$ defined by $f(x) = \sin(x)$ is surjective but not injective.

3) $f : [0, \pi/2] \to \mathbf{R}$ defined by $f(x) = \sin(x)$ is injective but not surjective.

4) $f : [0, \pi/2] \to [0, 1]$ defined by $f(x) = \sin(x)$ is bijective. ($f^{-1}(x)$ is written as $\arcsin(x)$ or $\sin^{-1}(x)$.)

5) $f : \mathbf{R} \to (0, \infty)$ defined by $f(x) = e^x$ is bijective. ($f^{-1}(x)$ is written as $\ln(x)$.)

Note There is no such thing as "the function $\sin(x)$." A function is not defined unless the domain and range are specified.

Exercise Show there are natural bijections from $(\mathbf{R}\times\mathbf{R}^2)$ to $(\mathbf{R}^2\times\mathbf{R})$ and from $(\mathbf{R}^2\times\mathbf{R})$ to $\mathbf{R}\times\mathbf{R}\times\mathbf{R}$. These three sets are disjoint, but the bijections between them are so natural that we sometimes identify them.

Exercise Suppose X is a set with 6 elements and Y is a finite set with n elements.

1) There exists an injective $f: X \to Y$ iff n ________________.
2) There exists a surjective $f: X \to Y$ iff n ________________.
3) There exists a bijective $f: X \to Y$ iff n ________________.

Pigeonhole Principle Suppose X is a finite set with m elements, Y is a finite set with n elements, and $f: X \to Y$ is a function.

1) If $m = n$, then f is injective iff f is surjective iff f is bijective.
2) If $m > n$, then f is not injective.
3) If $m < n$, then f is not surjective.

If you are placing 6 pigeons in 6 holes, and you run out of pigeons before you fill the holes, then you have placed 2 pigeons in one hole. In other words, in part 1) for $m = n = 6$, if f is not surjective then f is not injective. Of course, the pigeonhole principle does not hold for infinite sets, as can be seen by the following exercise.

Exercise Show there is a function $f: \mathbf{Z}^+ \to \mathbf{Z}^+$ which is injective but not surjective. Also show there is one which is surjective but not injective.

Exercise Suppose $f: [-2, 2] \to \mathbf{R}$ is defined by $f(x) = x^2$. Find $f^{-1}(f([1,2]))$. Also find $f(f^{-1}([3,5]))$.

Exercise Suppose $f: X \to Y$ is a function, $S \subset X$ and $T \subset Y$. Find the relationship between S and $f^{-1}(f(S))$. Show that if f is injective, $S = f^{-1}(f(S))$. Also find the relationship between T and $f(f^{-1}(T))$. Show that if f is surjective, $T = f(f^{-1}(T))$.

Strips We now define the vertical and horizontal strips of $X \times Y$.

If $x_0 \in X$, $\{(x_0, y) : y \in Y\} = (x_0 \times Y)$ is called a *vertical strip*.
If $y_0 \in Y$, $\{(x, y_0) : x \in X\} = (X \times y_0)$ is called a *horizontal strip*.

Theorem Suppose $S \subset X \times Y$. The subset S is the graph of a function with domain X and range Y iff each vertical strip intersects S in exactly one point.

This is just a restatement of the property of a graph of a function. The purpose of the next theorem is to restate properties of functions in terms of horizontal strips.

Theorem Suppose $f : X \to Y$ has graph Γ. Then

1) Each horizontal strip intersects Γ in at least one point iff f is ________.
2) Each horizontal strip intersects Γ in at most one point iff f is ________.
3) Each horizontal strip intersects Γ in exactly one point iff f is ________.

Solutions of Equations Now we restate these properties in terms of solutions of equations. Suppose $f : X \to Y$ and $y_0 \in Y$. Consider the equation $f(x) = y_0$. Here y_0 is given and x is considered to be a "variable". A *solution* to this equation is any $x_0 \in X$ with $f(x_0) = y_0$. Note that the set of all solutions to $f(x) = y_0$ is $f^{-1}(y_0)$. Also $f(x) = y_0$ has a solution iff $y_0 \in \text{image}(f)$ iff $f^{-1}(y_0)$ is non-void.

Theorem Suppose $f : X \to Y$.

1) The equation $f(x) = y_0$ has at least one solution for each $y_0 \in Y$ iff f is ____________________.
2) The equation $f(x) = y_0$ has at most one solution for each $y_0 \in Y$ iff f is ____________________.
3) The equation $f(x) = y_0$ has a unique solution for each $y_0 \in Y$ iff f is ____________________.

Right and Left Inverses One way to understand functions is to study right and left inverses, which are defined after the next theorem.

Theorem Suppose $X \xrightarrow{f} Y \xrightarrow{g} W$ are functions.

1) If $g \circ f$ is injective, then f is injective.

2) If $g \circ f$ is surjective, then g is surjective.
3) If $g \circ f$ is bijective, then f is injective and g is surjective.

Example $X = W = \{p\}$, $Y = \{p, q\}$, $f(p) = p$, and $g(p) = g(q) = p$. Here $g \circ f$ is the identity, but f is not surjective and g is not injective.

Definition Suppose $f : X \to Y$ is a function. A left inverse of f is a function $g : Y \to X$ such that $g \circ f = I_X : X \to X$. A right inverse of f is a function $h : Y \to X$ such that $f \circ h = I_Y : Y \to Y$.

Theorem Suppose $f : X \to Y$ is a function.

1) f has a right inverse iff f is surjective. Any such right inverse must be injective.
2) f has a left inverse iff f is injective. Any such left inverse must be surjective.

Corollary Suppose each of X and Y is a non-void set. Then $\exists$ an injective $f : X \to Y$ iff $\exists$ a surjective $g : Y \to X$. Also a function from X to Y is bijective iff it has a left inverse and a right inverse iff it has a left and right inverse.

Note The Axiom of Choice is not discussed in this book. However, if you worked 1) of the theorem above, you unknowingly used one version of it. For completeness, we state this part of 1) again.

The Axiom of Choice If $f : X \to Y$ is surjective, then f has a right inverse h. That is, for each $y \in Y$, it is possible to choose an $x \in f^{-1}(y)$ and thus to define $h(y) = x$.

Note It is a classical theorem in set theory that the Axiom of Choice and the Hausdorff Maximality Principle are equivalent. However in this text we do not go that deeply into set theory. For our purposes it is assumed that the Axiom of Choice and the HMP are true.

Exercise Suppose $f : X \to Y$ is a function. Define a relation on X by $a \sim b$ if $f(a) = f(b)$. Show this is an equivalence relation. If y belongs to the image of f, then $f^{-1}(y)$ is an equivalence class and every equivalence class is of this form. In the next chapter where f is a group homomorphism, these equivalence classes will be called cosets.

Projections If X_1 and X_2 are non-void sets, we define the projection maps $\pi_1 : X_1 \times X_2 \to X_1$ and $\pi_2 : X_1 \times X_2 \to X_2$ by $\pi_i(x_1, x_2) = x_i$.

Theorem If Y, X_1, and X_2 are non-void sets, there is a 1-1 correspondence between $\{$functions $f\colon Y \to X_1 \times X_2\}$ and $\{$ordered pairs of functions (f_1, f_2) where $f_1\colon Y \to X_1$ and $f_2 : Y \to X_2\}$.

Proof Given f, define $f_1 = \pi_1 \circ f$ and $f_2 = \pi_2 \circ f$. Given f_1 and f_2 define $f : Y \to X_1 \times X_2$ by $f(y) = (f_1(y), f_2(y))$. Thus a function from Y to $X_1 \times X_2$ is merely a pair of functions from Y to X_1 and Y to X_2. This concept is displayed in the diagram below. It is summarized by the equation $f = (f_1, f_2)$.

$$\begin{tikzcd}
 & Y \arrow[dl, "f_1"'] \arrow[d, "f"] \arrow[dr, "f_2"] & \\
X_1 & X_1 \times X_2 \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & X_2
\end{tikzcd}$$

One nice thing about this concept is that it works fine for infinite Cartesian products.

Definition Suppose T is an index set and for each $t \in T$, X_t is a non-void set. Then the *product* $\prod\limits_{t \in T} X_t = \prod X_t$ is the collection of all sequences $\{x_t\}_{t \in T} = \{x_t\}$ where $x_t \in X_t$. Formally these sequences are functions α from T to $\bigcup X_t$ with each $\alpha(t)$ in X_t and written as $\alpha(t) = x_t$. If $T = \{1, 2, \ldots, n\}$ then $\{x_t\}$ is the ordered n-tuple $(x_1, x_2, \ldots, x_n)$. If $T = \mathbf{Z}^+$ then $\{x_t\}$ is the sequence $(x_1, x_2, \ldots)$. For any T and any s in T, the *projection map* $\pi_s : \prod X_t \to X_s$ is defined by $\pi_s(\{x_t\}) = x_s$.

Theorem If Y is any non-void set, there is a 1-1 correspondence between $\{$functions $f : Y \to \prod X_t\}$ and $\{$sequences of functions $\{f_t\}_{t \in T}$ where $f_t : Y \to X_t\}$. Given f, the sequence $\{f_t\}$ is defined by $f_t = \pi_t \circ f$. Given $\{f_t\}$, f is defined by $f(y) = \{f_t(y)\}$.

A Calculus Exercise Let A be the collection of all functions $f : [0,1] \to \mathbf{R}$ which have an infinite number of derivatives. Let $A_0 \subset A$ be the subcollection of those functions f with $f(0) = 0$. Define $D : A_0 \to A$ by $D(f) = df/dx$. Use the mean value theorem to show that D is injective. Use the fundamental theorem of calculus to show that D is surjective.

Exercise This exercise is not used elsewhere in this text and may be omitted. It is included here for students who wish to do a little more set theory. Suppose T is a non-void set.

1) If Y is a non-void set, define Y^T to be the collection of all functions with domain T and range Y. Show that if T and Y are finite sets with m and n elements, then Y^T has n^m elements. In particular, when $T = \{1, 2, 3\}$, $Y^T = Y \times Y \times Y$ has n^3 elements. Show that if $n \geq 3$, the subset of $Y^{\{1,2,3\}}$ of all injective functions has $n(n-1)(n-2)$ elements. These injective functions are called permutations on Y taken 3 at a time. If $T = \mathbf{N}$, then Y^T is the infinite product $Y \times Y \times \cdots$. That is, $Y^{\mathbf{N}}$ is the set of all infinite sequences $(y_1, y_2, \ldots)$ where each $y_i \in Y$. For any Y and T, let Y_t be a copy of Y for each $t \in T$. Then $Y^T = \prod\limits_{t \in T} Y_t$.

2) Suppose each of Y_1 and Y_2 is a non-void set. Show there is a natural bijection from $(Y_1 \times Y_2)^T$ to $Y_1^T \times Y_2^T$. (This is the fundamental property of Cartesian products presented in the two previous theorems.)

3) Define $\mathcal{P}(T)$, the power set of T, to be the collection of all subsets of T (including the null set). Show that if T is a finite set with m elements, $\mathcal{P}(T)$ has 2^m elements.

4) If S is any subset of T, define its characteristic function $\chi_S : T \to \{0, 1\}$ by letting $\chi_S(t)$ be 1 when $t \in S$, and be 0 when $t \notin S$. Define $\alpha : \mathcal{P}(T) \to \{0, 1\}^T$ by $\alpha(S) = \chi_S$. Define $\beta : \{0, 1\}^T \to \mathcal{P}(T)$ by $\beta(f) = f^{-1}(1)$. Show that if $S \subset T$ then $\beta \circ \alpha(S) = S$, and if $f : T \to \{0, 1\}$ then $\alpha \circ \beta(f) = f$. Thus α is a bijection and $\beta = \alpha^{-1}$.

$$\mathcal{P}(T) \longleftrightarrow \{0, 1\}^T$$

5) Suppose $\gamma : T \to \{0, 1\}^T$ is a function and show that it cannot be surjective. If $t \in T$, denote $\gamma(t)$ by $\gamma(t) = f_t : T \to \{0, 1\}$. Define $f : T \to \{0, 1\}$ by $f(t) = 0$ if $f_t(t) = 1$, and $f(t) = 1$ if $f_t(t) = 0$. Show that f is not in the image of γ and thus γ cannot be surjective. This shows that if T is an infinite set, then the set $\{0, 1\}^T$ represents a "higher order of infinity than T".

6) An infinite set Y is said to be *countable* if there is a bijection from the positive

integers $\mathbf{N}$ to Y. Show $\mathbf{Q}$ is countable but the following three collections are not.

i) $\mathcal{P}(\mathbf{N})$, the collection of all subsets of $\mathbf{N}$.
ii) $\{0,1\}^{\mathbf{N}}$, the collection of all functions $f : \mathbf{N} \to \{0,1\}$.
iii) The collection of all sequences $(y_1, y_2, \ldots)$ where each y_i is 0 or 1.

We know that ii) and iii) are equal and there is a natural bijection between i) and ii). We also know there is no surjective map from $\mathbf{N}$ to $\{0,1\}^{\mathbf{N}}$, i.e., $\{0,1\}^{\mathbf{N}}$ is uncountable. Finally, show there is a bijection from $\{0,1\}^{\mathbf{N}}$ to the real numbers $\mathbf{R}$. (This is not so easy. To start with, you have to decide what the real numbers are.)

Notation for the Logic of Mathematics

Each of the words "Lemma", "Theorem", and "Corollary" means "true statement". Suppose A and B are statements. A theorem may be stated in any of the following ways:

Theorem **Hypothesis** Statement A.
Conclusion Statement B.

Theorem Suppose A is true. Then B is true.

Theorem If A is true, then B is true.

Theorem $A \Rightarrow B$ (A implies B).

There are two ways to prove the theorem — to suppose A is true and show B is true, or to suppose B is false and show A is false. The expressions "$A \Leftrightarrow B$", "A is equivalent to B", and "A is true iff B is true " have the same meaning (namely, that $A \Rightarrow B$ and $B \Rightarrow A$).

The important thing to remember is that thoughts and expressions flow through the language. Mathematical symbols are shorthand for phrases and sentences in the English language. For example, "$x \in B$ " means "x is an element of the set B." If A is the statement "$x \in \mathbf{Z}^+$" and B is the statement "$x^2 \in \mathbf{Z}^+$", then "$A \Rightarrow B$" means "If x is a positive integer, then x^2 is a positive integer".

Mathematical Induction is based upon the fact that if $S \subset \mathbf{Z}^+$ is a non-void subset, then S contains a smallest element.

Theorem Suppose $P(n)$ is a statement for each $n = 1, 2, ...$. Suppose $P(1)$ is true and for each $n \geq 1$, $P(n) \Rightarrow P(n+1)$. Then for each $n \geq 1$, $P(n)$ is true.

Proof If the theorem is false, then $\exists$ a smallest positive integer m such that $P(m)$ is false. Since $P(m-1)$ is true, this is impossible.

Exercise Use induction to show that, for each $n \geq 1$, $1+2+\cdots+n = n(n+1)/2$.

The Integers

In this section, lower case letters $a, b, c, ...$ will represent integers, i.e., elements of $\mathbf{Z}$. Here we will establish the following three basic properties of the integers.

1) If G is a subgroup of $\mathbf{Z}$, then $\exists$ $n \geq 0$ such that $G = n\mathbf{Z}$.
2) If a and b are integers, not both zero, and G is the collection of all linear combinations of a and b, then G is a subgroup of $\mathbf{Z}$, and its positive generator is the greatest common divisor of a and b.
3) If $n \geq 2$, then n factors uniquely as the product of primes.

All of this will follow from long division, which we now state formally.

Euclidean Algorithm Given a, b with $b \neq 0$, $\exists!$ m and r with $0 \leq r < |b|$ and $a = bm + r$. In other words, b divides a "m times with a remainder of r". For example, if $a = -17$ and $b = 5$, then $m = -4$ and $r = 3$, $-17 = 5(-4) + 3$.

Definition If $r = 0$, we say that b *divides* a or a is a *multiple* of b. This fact is written as $b \mid a$. Note that $b \mid a \Leftrightarrow$ the rational number a/b is an integer $\Leftrightarrow$ $\exists!$ m such that $a = bm \Leftrightarrow a \in b\mathbf{Z}$.

Note Anything (except 0) divides 0. 0 does not divide anything.
$\pm$ 1 divides anything . If $n \neq 0$, the set of integers which n divides is $n\mathbf{Z} = \{nm : m \in \mathbf{Z}\} = \{..., -2n, -n, 0, n, 2n, ...\}$. Also n divides a and b with the same remainder iff n divides $(a - b)$.

Definition A non-void subset $G \subset \mathbf{Z}$ is a *subgroup* provided $(g \in G \Rightarrow -g \in G)$ and $(g_1, g_2 \in G \Rightarrow (g_1 + g_2) \in G)$. We say that G is closed under negation and closed under addition.

Theorem If $n \in \mathbf{Z}$ then $n\mathbf{Z}$ is a subgroup. Thus if $n \neq 0$, the set of integers which n divides is a subgroup of $\mathbf{Z}$.

The next theorem states that every subgroup of $\mathbf{Z}$ is of this form.

Theorem Suppose $G \subset \mathbf{Z}$ is a subgroup. Then

1) $0 \in G$.
2) If g_1 and $g_2 \in G$, then $(m_1g_1 + m_2g_2) \in G$ for all integers m_1, m_2.
3) $\exists!$ non-negative integer n such that $G = n\mathbf{Z}$. In fact, if $G \neq \{0\}$ and n is the smallest positive integer in G, then $G = n\mathbf{Z}$.

Proof Since G is non-void, $\exists\ g \in G$. Now $(-g) \in G$ and thus $0 = g + (-g)$ belongs to G, and so 1) is true. Part 2) is straightforward, so consider 3). If $G \neq 0$, it must contain a positive element. Let n be the smallest positive integer in G. If $g \in G$, $g = nm + r$ where $0 \leq r < n$. Since $r \in G$, it must be 0, and $g \in n\mathbf{Z}$.

Now suppose $a, b \in \mathbf{Z}$ and at least one of a and b is non-zero.

Theorem Let G be the set of all linear combinations of a and b, i.e., $G = \{ma + nb : m, n \in \mathbf{Z}\}$. Then

1) G contains a and b.
2) G is a subgroup. In fact, it is the smallest subgroup containing a and b. It is called the subgroup generated by a and b.
3) Denote by (a, b) the smallest positive integer in G. By the previous theorem, $G = (a, b)\mathbf{Z}$, and thus $(a, b) \mid a$ and $(a, b) \mid b$. Also note that $\exists\ m, n$ such that $ma + nb = (a, b)$. The integer (a, b) is called the *greatest common divisor* of a and b.
4) If n is an integer which divides a and b, then n also divides (a, b).

Proof of 4) Suppose $n \mid a$ and $n \mid b$ i.e., suppose $a, b \in n\mathbf{Z}$. Since G is the smallest subgroup containing a and b, $n\mathbf{Z} \supset (a, b)\mathbf{Z}$, and thus $n \mid (a, b)$.

Corollary The following are equivalent.

1) a and b have no common divisors, i.e., $(n \mid a \text{ and } n \mid b) \Rightarrow n = \pm 1$.

2) $(a,b)=1$, i.e., the subgroup generated by a and b is all of $\mathbf{Z}$.
3) $\exists\ m,n \in \mathbf{Z}$ with $ma+nb=1$.

Definition If any one of these three conditions is satisfied, we say that a and b are *relatively prime.*

This next theorem is the basis for unique factorization.

Theorem If a and b are relatively prime with a not zero, then $a|bc \Rightarrow a|c$.

Proof Suppose a and b are relatively prime, $c \in \mathbf{Z}$ and $a \mid bc$. Then there exist m,n with $ma+nb=1$, and thus $mac+nbc=c$. Now $a \mid mac$ and $a \mid nbc$. Thus $a \mid (mac+nbc)$ and so $a \mid c$.

Definition A *prime* is an integer $p>1$ which does not factor, i.e., if $p=ab$ then $a=\pm 1$ or $a=\pm p$. The first few primes are 2, 3, 5, 7, 11, 13, 17,... .

Theorem Suppose p is a prime.

1) If a is an integer which is not a multiple of p, then $(p,a)=1$. In other words, if a is any integer, $(p,a)=p$ or $(p,a)=1$.
2) If $p \mid ab$ then $p \mid a$ or $p \mid b$.
3) If $p \mid a_1 a_2 \cdots a_n$ then p divides some a_i. Thus if each a_i is a prime, then p is equal to some a_i.

Proof Part 1) follows immediately from the definition of prime. Now suppose $p \mid ab$. If p does not divide a, then by 1), $(p,a)=1$ and by the previous theorem, p must divide b. Thus 2) is true. Part 3) follows from 2) and induction on n.

The Unique Factorization Theorem Suppose a is an integer which is not 0,1, or -1. Then a may be factored into the product of primes and, except for order, this factorization is unique. That is, $\exists$ a unique collection of distinct primes $p_1, p_2, ..., p_k$ and positive integers $s_1, s_2, ..., s_k$ such that $a=\pm p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$.

Proof Factorization into primes is obvious, and uniqueness follows from 3) in the theorem above. The power of this theorem is uniqueness, not existence.

Now that we have unique factorization and part 3) above, the picture becomes transparent. Here are some of the basic properties of the integers in this light.

Theorem (Summary)

1) Suppose $|a| > 1$ has prime factorization $a = \pm p_1^{s_1} \cdots p_k^{s_k}$. Then the only divisors of a are of the form $\pm p_1^{t_1} \cdots p_k^{t_k}$ where $0 \le t_i \le s_i$ for $i = 1, ..., k$.

2) If $|a| > 1$ and $|b| > 1$, then $(a, b) = 1$ iff there is no common prime in their factorizations. Thus if there is no common prime in their factorizations, $\exists\ m, n$ with $ma + nb = 1$, and also $(a^2, b^2) = 1$.

3) Suppose $|a| > 1$ and $|b| > 1$. Let $\{p_1, \ldots, p_k\}$ be the union of the distinct primes of their factorizations. Thus $a = \pm p_1^{s_1} \cdots p_k^{s_k}$ where $0 \le s_i$ and $b = \pm p_1^{t_1} \cdots p_k^{t_k}$ where $0 \le t_i$. Let u_i be the minimum of s_i and t_i. Then $(a, b) = p_1^{u_1} \cdots p_k^{u_k}$. For example $(2^3 \cdot 5 \cdot 11,\ 2^2 \cdot 5^4 \cdot 7) = 2^2 \cdot 5$.

3′) Let v_i be the maximum of s_i and t_i. Then $c = p_1^{v_1} \cdots p_k^{v_k}$ is the *least* (positive) *common multiple* of a and b. Note that c is a multiple of a and b, and if n is a multiple of a and b, then n is a multiple of c. Finally, if a and b are positive, their least common multiple is $c = ab/(a, b)$, and if in addition a and b are relatively prime, then their least common multiple is just their product.

4) There is an infinite number of primes. (Proof: Suppose there were only a finite number of primes $p_1, p_2, ..., p_k$. Then no prime would divide $(p_1 p_2 \cdots p_k + 1)$.)

5) Suppose c is an integer greater than 1. Then $\sqrt{c}$ is rational iff $\sqrt{c}$ is an integer. In particular, $\sqrt{2}$ and $\sqrt{3}$ are irrational. (Proof: If $\sqrt{c}$ is rational, $\exists$ positive integers a and b with $\sqrt{c} = a/b$ and $(a, b) = 1$. If $b > 1$, then it is divisible by some prime, and since $cb^2 = a^2$, this prime will also appear in the prime factorization of a. This is a contradiction and thus $b = 1$ and $\sqrt{c}$ is an integer.) (See the fifth exercise below.)

Exercise Find (180,28), i.e., find the greatest common divisor of 180 and 28, i.e., find the positive generator of the subgroup generated by {180,28}. Find integers m and n such that $180m + 28n = (180, 28)$. Find the least common multiple of 180 and 28, and show that it is equal to $(180 \cdot 28)/(180, 28)$.

Exercise We have defined the greatest common divisor (gcd) and the least common multiple (lcm) of a pair of integers. Now suppose $n \geq 2$ and $S = \{a_1, a_2, .., a_n\}$ is a finite collection of integers with $|a_i| > 1$ for $1 \leq i \leq n$. Define the gcd and the lcm of the elements of S and develop their properties. Express the gcd and the lcm in terms of the prime factorizations of the a_i. When is the lcm of S equal to the product $a_1 a_2 \cdots a_n$? Show that the set of all linear combinations of the elements of S is a subgroup of $\mathbf{Z}$, and its positive generator is the gcd of the elements of S.

Exercise Show that the gcd of $S = \{90, 70, 42\}$ is 2, and find integers n_1, n_2, n_3 such that $90n_1 + 70n_2 + 42n_3 = 2$. Also find the lcm of the elements of S.

Exercise Show that if each of $G_1, G_2, ..., G_m$ is a subgroup of $\mathbf{Z}$, then $G_1 \cap G_2 \cap \cdots \cap G_m$ is also a subgroup of $\mathbf{Z}$. Now let $G = (90\mathbf{Z}) \cap (70\mathbf{Z}) \cap (42\mathbf{Z})$ and find the positive integer n with $G = n\mathbf{Z}$.

Exercise Show that if the nth root of an integer is a rational number, then it itself is an integer. That is, suppose c and n are integers greater than 1. There is a unique positive real number x with $x^n = c$. Show that if x is rational, then it is an integer. Thus if p is a prime, its nth root is an irrational number.

Exercise Show that a positive integer is divisible by 3 iff the sum of its digits is divisible by 3. More generally, let $a = a_n a_{n-1} \ldots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0$ where $0 \leq a_i \leq 9$. Now let $b = a_n + a_{n-1} + \cdots + a_0$, and show that 3 divides a and b with the same remainder. Although this is a straightforward exercise in long division, it will be more transparent later on. In the language of the next chapter, it says that $[a] = [b]$ in $\mathbf{Z}_3$.

Card Trick Ask friends to pick out seven cards from a deck and then to select one to look at without showing it to you. Take the six cards face down in your left hand and the selected card in your right hand, and announce you will place the selected card in with the other six, but they are not to know where. Put your hands behind your back and place the selected card on top, and bring the seven cards in front in your left hand. Ask your friends to give you a number between one and seven (not allowing one). Suppose they say three. You move the top card to the bottom, then the second card to the bottom, and then you turn over the third card, leaving it face up on top. Then repeat the process, moving the top two cards to the bottom and turning the third card face up on top. Continue until there is only one card face down, and this will be the selected card. Magic? Stay tuned for Chapter 2, where it is shown that any non-zero element of $\mathbf{Z}_7$ has order 7.