CONTENTS

Module 1: Elements 1

Module 2: The Fundamental Theorem of Algebra 11

Module 3: The Fundamental Theorem of Calculus 20

Module 4: The Fundamental Theorem of Arithmetic 31

Module 5: The Central Limit Theorem 38

Module 6: The Five Famous Formulas of College Mathematics 50

Elements

1.1 What are Sets?

The most primitive entities in mathematics are called *sets*. Intuitively, a set can be likened to a physical "collection" of distinct things. The things that make up a set are called its *members*. It might come to you as a surprise to learn that some words like "set" and "member" actually are undefined in mathematics. To define these words, reference would have to be made to mathematical entities of a more primitive order, which in turn would have to be defined in terms of mathematical entities of a still more primitive order, and so on. Evidently, the process must terminate at some stage. The language of mathematics terminates at the words "set" and "member".

1.2 The Symbolism of Sets

Typically, sets are denoted by upper case letters. The names of the members are enclosed in curly braces. For example:

$A = \{\text{All positive even integers}\}$
$B = \{\text{All even integers between 7 and 17}\}$
$C = \{\text{All real numbers greater than -2 and less than or equal to 5}\}$

In many cases it is possible to display all the members of a set by way of a sequential list. If so, the names of the members are separated by commas. Examples:

$A = \{2, 4, 6, 8, 10, \ldots\}$
$B = \{6, 8, 10, 12, 14, 16\}$

The members of the set C in the first example are too many (and too crowded) to permit being displayed as a sequential list. In this case we can employ "set-builder notation" to identify the set:

$C = \{x \mid x \text{ is a real number and } -2 < x \leq 5\}$

Similarly, the set A above can be displayed using set-builder notation as follows:

$A = \{x \mid x = 2n \text{ where } n \text{ is a positive integer}\}$

A set (like a club) is determined completely by its membership, without regard to order. Thus, two sets are equal if and only if they have the same members. Examples:

$\{1, 2, 3\} = \{3, 1, 2\}$
$\{x \mid x \text{ is a real number and } x^2 = 25\} = \{-5, 5\}$

The symbol $\in$ is used to denote membership. Thus

$2 \in \{3, 1, 2\}$
$5 \notin \{3, 1, 2\}$
$2000 \in \{2, 4, 6, 8, 10, \ldots\}$
$\sqrt{7} \in \{x \mid x \text{ is a real number and } -2 < x \leq 5\}$
$-2 \notin \{x \mid x \text{ is a real number and } -2 < x \leq 5\}$

We say that the set S is a *subset* of the set T, symbolized by $S \subseteq T$, if and only if every member of S is a member of T. For instance:

$\{1, 3, 4\} \subseteq \{1, 2, 3, 4, 5\}$

$\{6, 8, 10, 12, 14, 16\} \subseteq \{2, 4, 6, 8, 10, \ldots\}$

If we want to emphasize that S is a *proper* subset of T, that is $S \subseteq T$ but $S \neq T$, then we write $S \subset T$.

Arguably, the most important set in mathematics is the *empty set*, denoted by the symbol $\varnothing$. The empty set is distinguished by the property that it possesses no members. It behaves like an empty shell, and serves roughly the same function in the theory of sets as does the special integer 0 in the theory of numbers. The following properties of the empty set are easily verified:

1. If x is any mathematical entity then $x \notin \varnothing$.
2. If S is any set, then $\varnothing \subseteq S$.
3. $\varnothing = \{x \,|\, x \neq x\}$.

The "size" of a set is specified by its *cardinality*. By definition, the cardinality of the set $\{1, 2, 3, \ldots, n-1, n\}$ is n. By universal agreement, two sets S and T are said to have the same cardinality if and only if the members of S can be paired in one-to-one correspondence with the members of T. For instance:

$\text{card}(\{a, b, c\}) = \text{card}(\{x, y, z\}) = \text{card}(\{1, 2, 3\}) = 3$

As expected, the cardinality of the empty set is defined to be 0. A set whose cardinality is a non-negative integer is called *finite*, otherwise it is called *infinite*. For instance, the sets

$M = \{2, 4, 6, 8, 10, 12, \ldots\}$

$N = \{1, 2, 3, 4, 5, 6, \ldots\}$

are infinite sets. However, since the members of M can be paired in one-to-one correspondence with the members of N, they are seen to possess the same cardinality.

To represent the cardinalities of infinite sets, mathematicians have manufactured what are called *transfinite numbers*. The smallest tansfinite number is $\aleph_0$, representing the cardinality of the special set $\{1, 2, 3, 4, \ldots\}$. The transfinite numbers form an infinite ascending hierarchy:

$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 < \ldots$

1.3 Operations on Sets

In this section we review some of the basic operations that can be applied to sets to generate new sets. Our treatment is brief and informal. For a more rigorous exposition, the reader may refer to the excellent book by Smith, Egen and St. Andre: *A Transition to Advanced Mathematics*.

Five basic operations are commonly applied to sets to generate new sets:

(a) The *complementary set* operation, denoted by the symbol $\tilde{}$ (eg. $\tilde{A}$)
(b) The *power set* operation, denoted by the symbol $\mathcal{P}$ (eg. $\mathcal{P}(A)$)
(c) The *union* operation, denoted by the symbol $\cup$ (eg. $A \cup B$)
(d) The *intersection* operation, denoted by the symbol $\cap$ (eg. $A \cap B$)
(e) The *Cartesian product* operation, denoted by the symbol $\times$ (eg. $A \times B$)

Of the five operations listed above, the first two are of the *unary* type and the remaining three are of the *binary* type. In general, an operation is called unary if it can operate on only a single object at a time to generate a new object. Similarly, a operation is called binary if it can operate on a pair of objects at a time to generate a new object. For example, in the ordinary system of numerical arithmetic the operation $-$ (opposite) is unary, while the operations $+$ (addition) and $\times$ (multiplication) are binary.

Without loss of generality, we may assume that all sets considered in this section are subsets of a certain fixed set U, called the *universal set*. With the universal set in mind, the *complement* of any set A is defined as the set of members of U which are not members of A:

$$\boxed{\widetilde{A} = \{x \mid x \in U \text{ and } x \notin A\}}$$

Ex: if $U = \{1, 2, 3, 4, 5, 6, 7\}$ and $A = \{1, 2, 4, 7\}$ then $\widetilde{A} = \{3, 5, 6\}$.

The *power set* of a set C is defined as the set of all subsets of C.

$$\boxed{\mathcal{P}(C) = \{X \mid X \subseteq C\}}$$

Ex: if $C = \{1, 2, 4\}$ then $\mathcal{P}(C) = \{\varnothing, \{1\}, \{2\}, \{4\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{1, 2, 4\}\}$.

The *union* of two sets A and B is defined as the set whose members belong to either A or B.

$$\boxed{A \cup B = \{x \mid x \in A \text{ or } x \in B\}}$$

Ex: if $A = \{1, 2, 4, 7\}$ and $B = \{1, 2, 3, 4, 5\}$ then $A \cup B = \{1, 2, 3, 4, 5, 7\}$. Keep in mind that in the language of mathematics the word "or" is always used in the non-exclusive sense. In other words, "or" always means "and/or".

The *intersection* of two sets A and B is defined as the set whose members belong to both A and B:

$$\boxed{A \cap B = \{x \mid x \in A \text{ and } x \in B\}}$$

Ex: if $A = \{1, 2, 4, 7\}$ and $B = \{1, 2, 3, 4, 5\}$ then $A \cap B = \{1, 2, 4\}$.

Two sets R and S are considered *disjoint* when they share no members in common.

$$\boxed{R \text{ and } S \text{ are disjoint if and only if } R \cap S = \varnothing}$$

Ex: The sets $R = \{1, 2, 3\}$ and $S = \{5, 7\}$ are disjoint.

The *Cartesian product* of two sets C and D is defined as the set of all *ordered pairs* whose first component is a member of C and whose second component is a member of D.

$$\boxed{C \times D = \{(c, d) \mid c \in C \text{ and } d \in D\}}$$

Ex: if $C = \{1, 2, 4\}$ and $D = \{2, 5\}$ then $C \times D = \{(1, 2), (2, 2), (4, 2), (1, 5), (2, 5), (4, 5)\}$.

Keep in mind that two ordered pairs are equal if and only if the corresponding components are equal. For instance, $(1, 2) \neq (2, 1)$. Hence the Cartesian product is not a *commutative* operation. In other words, the statement $C \times D = D \times C$ is not valid in all cases.

The notion of ordered pair can be generalized to the notion of *ordered n-tuple*. By definition, an ordered n-tuple is an expression of the form $(x_1, x_2, \ldots, x_n)$ where the components x_i may be mathematical entities of any type (usually numbers). Two ordered n-tuples are considered equal if and only if the corresponding components are equal.

$$\boxed{(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \text{ if and only if } x_i = y_i\,,\ i = 1, 2, \ldots, n}$$

If $n \geq 2$, the Cartesian product of n copies of a set X, denoted by the expression X^n, is defined as the set of all n-tuples whose components are members of X. For the special case $n = 1$, we define $X^1 = X$.

$$\boxed{X^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X,\ \ i = 1, 2, \ldots, n\}}$$

Ex: If $X = \{1, 2\}$, $X^3 = \{(1,1,1), (1,1,2), (1,2,1), (2,1,1), (2,2,1), (2,1,2), (1,2,2), (2,2,2)\}$

The following list of propositions serves as a minimal synopsis of the basic properties of sets and the elementary relations that hold between them. This list is not meant to be exhaustive. Every one of these propositions can be proved with a minimum of effort using only the raw definitions and elementary logic. Every student of mathematics should be completely familiar with these propositions and should be able to produce their proofs without the slightest hesitation.

Let A, B and C be sets. Then

(a) $A \cup \varnothing = A$

(b) $A \cap \varnothing = \varnothing$

(c) $A \subseteq A \cup B$

(d) $A \cap B \subseteq A$

(e) $A \cup B = B \cup A$

(f) $A \cap B = B \cap A$

(g) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(h) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(i) $A \widetilde{\cup} B = \widetilde{A} \cap \widetilde{B}$

(j) $A \widetilde{\cap} B = \widetilde{A} \cup \widetilde{B}$

(k) $A \times \varnothing = \varnothing$

(l) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(m) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

If A and B are finite sets, then:

(n) $\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B)$

(o) $\operatorname{card}(A \times B) = \operatorname{card}(A) \cdot \operatorname{card}(B)$

(p) $\operatorname{card}(\mathcal{P}(A)) = 2^{\operatorname{card}(A)}$

(q) $\operatorname{card}(A^n) = (\operatorname{card}(A))^n$

1.4 Special Numerical Sets

The most basic family of numbers is the set of natural numbers, denoted by the symbol $\mathbb{N}$.

$$\boxed{\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}}$$

Although the set $\mathbb{N}$ is *closed* under the common operations of addition and multiplication, which is to say that the sum and product of any two natural numbers is again a natural number, it is not closed under the operation of subtraction. For instance, $2 - 5$ is not a natural number. Consequently, unless we venture outside of the set of natural numbers, it is not possible to solve a simple equation such as $5 + x = 2$. The smallest numerical set containing the natural numbers and admitting solutions to any equation of the form $n + x = m$, where $m, n \in \mathbb{N}$, is the set of integers, denoted by the symbol $\mathbb{Z}$.

$$\boxed{\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}}$$

Although the set $\mathbb{Z}$ is closed under the operations of addition, subtraction and multiplication, it is not closed under the operation of division. For instance, $2 \div 5$ is not an integer. Consequently, unless we venture outside of the set of integers, an equation as simple as $5x = 2$ cannot be solved. The smallest numerical set containing $\mathbb{Z}$ and admitting solutions to any equation of the form $nx = m$, where $m, n \in \mathbb{Z}$, $n \neq 0$, is the set of rational numbers, denoted by the symbol $\mathbb{Q}$.

$$\boxed{\mathbb{Q} = \left\{ x \;\middle|\; x = \frac{m}{n}, \quad \text{where} \quad m, n \in \mathbb{Z}, \quad \text{and} \quad n \neq 0 \right\}}$$

The set $\mathbb{Q}$ is closed under the four basic operations of addition, subtraction, multiplication and division. Any system of numbers which is closed under these four basic operations and on which these operations conform to certain reasonable conditions (including commutativity, associativity and distributivity) is called a *field*. Thus, $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$.

To the mathematicians of antiquity (especially Pythagoras, circa 500 B.C.) it came as a great shock to discover that the set $\mathbb{Q}$ is too sparse to admit solutions to some elementary algebraic equations. For instance, the equation $x^2 = 5$ cannot be solved unless we venture outside of $\mathbb{Q}$. In other words, $\sqrt{5}$ is not a rational number. But even if we enlarge $\mathbb{Q}$ by appending to it the solutions of all possible algebraic equations, the resulting system of numbers still is not rich enough to permit values to be assigned to the outcomes of certain elementary numerical processes. For instance, consider the following sequence of rational numbers:

$$\left(1 + \tfrac{1}{1}\right)^1, \ \left(1 + \tfrac{1}{2}\right)^2, \ \left(1 + \tfrac{1}{3}\right)^3, \ \left(1 + \tfrac{1}{4}\right)^4, \ \ldots, \ \left(1 + \tfrac{1}{n}\right)^n, \ \ldots$$

As $n \to \infty$, this sequence of rational numbers converges to a specific value $e \approx 2.718281828\ldots$. The striking fact that no algebraic equation can exist to which this special number e is a solution was proved in 1873 by the French mathematician Charles Hermite. Numbers of this kind, of which there are infinitely many, are called *transcendental*. The set of real numbers, denoted by the symbol $\mathbb{R}$, consists precisely of all numbers that can be generated as the limits of sequences of rational numbers.

$$\boxed{\mathbb{R} = \{x \mid x \text{ equals the limit of a sequence in } \mathbb{Q}\}}$$

Equipped with the usual operations of addition, subtraction, multiplication and division, the set $\mathbb{R}$ turns out to be a field. Moreover, every convergent sequence of real numbers converges to a real number. Mathematicians use a special phrase to refer to a state of affairs such as this. A set of numbers having the property that every convergent sequence converges to a number in the set is said to be *topologically closed*. The word "topological" is roughly synonymous with the word "spatial". To see why the word "topological" is pertinent here, recall that the set of real numbers can be modeled by a continuous "number line" (a purely spatial entity). Since the real number line has no holes, it follows that no bounded sequence of points on the number line can converge to a point outside of the number line.

However, from an algebraic point of view, the set $\mathbb{R}$ still exhibits a serious deficiency. It is not *algebraically closed*. For example, the simple algebraic equation $x^2 = -5$ cannot be solved unless we venture outside of $\mathbb{R}$. This deficiency is rectified by appending to $\mathbb{R}$ all expressions of the form $z = x + iy$ where $x, y \in \mathbb{R}$ and where $i = \sqrt{-1}$. The resulting set is the set of complex numbers, denoted by the symbol $\mathbb{C}$.

$$\boxed{\mathbb{C} = \{z \mid z = x + iy \text{ where } x, y \in \mathbb{R}\}}$$

Equipped with the usual operations of addition, subtraction, multiplication and division, the set $\mathbb{C}$ turns out to be a field. But, unlike the field $\mathbb{Q}$, the field $\mathbb{C}$ is topologically closed (every convergent sequence of complex numbers converges to a complex number). And, unlike the field $\mathbb{R}$, the field $\mathbb{C}$ is algebraically closed (every polynomial equation with complex coefficients possesses a solution in the field of complex numbers). The latter assertion is known as the Fundamental Theorem of Algebra.

Finally, we summarize the progression of extensions starting with $\mathbb{N}$ and ending with $\mathbb{C}$:

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}}$$

In some important ways this progression mirrors the evolution of the number concept from ancient to modern times.

1.5 Rings and Fields

By a *ring* we mean an algebraic system consisting of a set $\mathcal{R}$ and two binary operations $+$ and $\times$ (addition and multiplication), which jointly are governed by a specific set of rules called the *ring axioms*. The ring axioms are modeled on the usual rules of arithmetic satisfied by the integers. However, the elements of the set $\mathcal{R}$ need not be numbers. They could be matrices, functions, or some other species of objects.

THE RING AXIOMS

[1] $\mathcal{R}$ is closed under addition (if $x, y \in \mathcal{R}$ then $x + y \in \mathcal{R}$).

[2] $\mathcal{R}$ is closed under multiplication (if $x, y \in \mathcal{R}$ then $xy \in \mathcal{R}$).

[3] There exists a special element $0 \in \mathcal{R}$ such that $x + 0 = x$ for all $x \in \mathcal{R}$.

[4] Addition is commutative in $\mathcal{R}$ ($x + y = y + x$ for all $x, y \in \mathcal{R}$).

[5] Addition is associative in $\mathcal{R}$ ($(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathcal{R}$).

[6] For every $x \in \mathcal{R}$ there exists $-x \in \mathcal{R}$ such that $x + -x = 0$ (existence of opposites).

[7] Multiplication is associative in $\mathcal{R}$ ($(xy)z = x(yz)$ for all $x, y, z \in \mathcal{R}$).

[8] If $x, y, z \in \mathcal{R}$, then $x(y + z) = xy + xz$ (left distributivity of mult. over addition).

[9] If $x, y, z \in \mathcal{R}$, then $(y + z)x = yx + zx$ (right distributivity of mult. over addition).

A ring can be either finite or infinite depending on whether the underlying set $\mathcal{R}$ is finite or infinite. In the event that the *dominant* operation $\times$ (multiplication) is commutative ($xy = yx$ for all $x, y \in \mathcal{R}$) then the ring itself is called *commutative*. In the event that a *multiplicative identity element* $1 \in \mathcal{R}$ exists satisfying the condition $x \cdot 1 = 1 \cdot x = x$ for all $x \in \mathcal{R}$, then $\mathcal{R}$ is called a *ring with identity* or *ring with unity*.

Rings pervade all branches of mathematics. The following are some common examples of rings:

(a) Each of the special numerical sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (equipped with the usual operations of multiplication and addition) is an infinite commutative ring with identity.

(b) The numerical set $\mathbb{E} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ consisting of the even integers (equipped with the usual operations of multiplication and addition) is an infinite commutative ring without identity.

(c) The set $M_2(\mathbb{Z})$ consisting of all 2×2 matrices with integer entries (equipped with the usual operations of matrix multiplication and matrix addition) is an infinite noncommutative ring with identity.

(d) The set $M_2(\mathbb{E})$ consisting of all 2×2 matrices with even integer entries (equipped with the usual operations of matrix multiplication and matrix addition) is an infinite noncommutative ring without identity.

(e) The finite set $\mathbb{Z}_3 = \{0, 1, 2\}$ equipped with the operations of multiplication and addition (mod 3) is a finite commutative ring with identity.

(f) The set $M_2(\mathbb{Z}_3)$ consisting of all 2×2 matrices with entries in $\mathbb{Z}_3$ and equipped with the operations of matrix multiplication and matrix addition (mod 3) is a finite noncommutative ring with identity.

Let $\mathcal{R}$ be a ring with identity (not necessarily commutative). An element $x \in \mathcal{R}$ is said to be *invertible* if a corresponding element $x^{-1} \in \mathcal{R}$ exists such that $x^{-1} \cdot x = x \cdot x^{-1} = 1$. The element x^{-1}, if it exists, is called the *multiplicative inverse* or the *reciprocal* of x in $\mathcal{R}$. Examples:

(a) In $\mathbb{Z}$ the only invertible elements are 1 and -1.

(b) In $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all nonzero elements are invertible.

(c) In $M_2(\mathbb{Z})$ the element $\begin{bmatrix} 2 & 5 \\ 3 & 7 \end{bmatrix}$ is invertible, while the element $\begin{bmatrix} 2 & 3 \\ 7 & 5 \end{bmatrix}$ is <u>not</u> invertible.

A commutative ring with identity in which every nonzero element is invertible is called a *field*. Within a field, it is possible always to solve the linear equation $ax = b$, provided $a \neq 0$. The unique solution is $x = a^{-1}b$, which also may be expressed in fractional notation as $x = \dfrac{b}{a}$.

The following are some common examples of fields:

(a) Each of the special numerical sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (equipped with the usual operations of multiplication and addition) is a field.

(b) The numerical set $\mathbb{Q}(\sqrt{2}) = \{x \mid x = a + b\sqrt{2} \text{ where } a, b \in \mathbb{Q}\}$, equipped with the usual operations of multiplication and addition, is a field. The field $\mathbb{Q}(\sqrt{2})$ is an *extension* of the field $\mathbb{Q}$ (since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$), and it is a *subfield* of $\mathbb{R}$ (since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$).

(c) The set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, equipped with the operations of multiplication and addition (mod 5), is a finite field. In fact, if p is any prime number, then $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is a field. Finite fields are of special importance in Number Theory and in Coding Theory.

1.6 The Principle of Mathematical Induction

Should ever you need, or feel inclined, to provide proof that a specific claim about the natural numbers is valid for all $n \in \mathbb{N}$, a good strategy to keep in mind is the Principle of Mathematical Induction. In general, a *proof by induction* proceeds as follows:

I. Show that Claim(1) is true.

II. Show that whenever Claim(k) is true then Claim($k+1$) also is true.

III. Conclusion: Claim(n) is true for all $n \in \mathbb{N}$.

Step II, called the *inductive step*, is the only part of the proof that might call for some creative reasoning. Naturally, if Claim(n) is not valid for some $n \in \mathbb{N}$, then this step will not be feasible. The following are some examples of proof by induction.

(a) Claim: $n < 2^n$ for all $n \in \mathbb{N}$.

Proof: To begin, we must establish Claim(1). That is, we must verify that $1 < 2^1$. Plainly, this is true, since $1 < 2$. Next, we must show that if Claim(k) holds, then Claim($k+1$) also holds. That is, we must show that if $k < 2^k$, then $k + 1 < 2^{k+1}$. Starting with $k < 2^k$, and multiplying both sides by 2, we get $2k < 2^{k+1}$. Since $k \in \mathbb{N}$, it follows that $k + 1 \leq k + k = 2k$, which, when compared with the previous inequality, yields $k + 1 < 2^{k+1}$. Thus we conclude that $n < 2^n$ for all $n \in \mathbb{N}$.

(b) Claim: The formula $1 + 2 + 3 + \cdots + n = \dfrac{n^2 + n}{2}$ holds for all $n \in \mathbb{N}$.

Proof: To begin, we must verify Claim(1). That is, we must verify that $1 = (1^2 + 1)/2$. Plainly, this is true, since $1 = 1$. Next, we must show that if Claim(k) is true, then Claim($k+1$) is also true. That is, we must show that if $1 + 2 + 3 + \cdots + k = (k^2 + k)/2$, then $1 + 2 + 3 + \cdots + k + k + 1 = ((k+1)^2 + k + 1)/2$. It is a straightforward exercise to show that the second formula (Claim($k+1$)) follows from the first formula (Claim(k)) simply by adding $k + 1$ to both sides. Thus we conclude that the formula is valid for all $n \in \mathbb{N}$.

(c) Claim: If A is a finite non-empty set and $\text{card}(A) = n$, then $\text{card}(\mathcal{P}(A)) = 2^n$.

Proof: To begin, suppose $\text{card}(A) = 1$, say $A = \{a\}$. Then $\mathcal{P}(A) = \{\varnothing, \{a\}\}$. So $\text{card}(\mathcal{P}(A)) = 2^1$. This establishes the claim for $n = 1$. Next, suppose it has already been established that $\text{card}(\mathcal{P}(A)) = 2^k$ whenever $\text{card}(A) = k$. Let B be a set of cardinality $k+1$, say $B = A \cup \{b\}$ where $\text{card}(A) = k$. Let C be a typical subset of B. Then either $b \in C$ or $b \notin C$. If $b \notin C$, then C must be a subset of A. Thus there are exactly 2^k subsets of B which do not contain the element b. On the other hand, if $b \in C$, then C must have the form $C = D \cup \{b\}$, where $D \subseteq A$. Thus there are exactly 2^k subsets of B which contain the element b. Therefore the total number of subsets of B equals $2^k + 2^k = 2^{k+1}$. By the Principle of Mathematical Induction, we conclude that the claim is true for all $n \in \mathbb{N}$.

1.7 Exercises

1. Decide if the statement is true or false.
   (a) $\{1\} \in \{1, 2, 3\}$
   (b) $\mathcal{P}(\varnothing) = \varnothing$
   (c) $1 \in \{\{1\}, \{2\}, \{3\}\}$
   (d) $\{1, 2\} \in \mathcal{P}(\{1, 2, 3\})$
   (e) $\text{card}(\mathcal{P}(\varnothing)) = 1$
   (f) $\{\{1\}, \{2\}, \{3\}\} \cap \{1, 2, 3\} = \varnothing$
   (g) $1 \in \{\{1, 2, 3\}\}$
   (h) $\{0\} = \varnothing$
   (i) $\{x \in \mathbb{Z} \mid x + 1 < 1\} = \varnothing$
   (j) $\{x \in \mathbb{R} \mid 3x = x\} = \varnothing$

2. Decide if the claim is true or false. If true, provide a rigorous proof. If false, give a specific counterexample. The symbols A, B and C denote sets.
   (a) Claim: If $A \cap B = \varnothing$ then $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)$
   (b) Claim: If $A \subseteq B \cup C$ then $A \subseteq B$ or $A \subseteq C$
   (c) Claim: If $A \subseteq B$ then $\widetilde{A} \subseteq \widetilde{B}$
   (d) Claim: $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$
   (e) Claim: $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

3. Let A and B be sets such that $\text{card}(A) = 5$, $\text{card}(B) = 8$ and $\text{card}(A \cap B) = 3$. Determine the cardinality of each of the following sets.
   (a) $A \cup B$
   (b) $\mathcal{P}(A)$
   (c) $A \times B$
   (d) A^3
   (e) $\mathcal{P}(A) \cup \mathcal{P}(B)$

4. Determine the cardinality of each of the following sets.
   (a) $\left\{x \in \mathbb{N} \,\middle|\, x^2 \leq 20\right\}$
   (b) $\left\{x \in \mathbb{Z} \,\middle|\, x^2 \leq 20\right\}$
   (c) $\left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, x^2 + y^2 = 25\right\}$
   (d) $\left\{x \in \mathbb{Z} \,\middle|\, 3x^3 - 8x^2 + 5x = 0\right\}$
   (e) $\left\{x \in \mathbb{R} \,\middle|\, x^6 - 5x^4 + 6x^2 - 1 = 0\right\}$
5. Test each of the following sets for closure under the usual numerical operations of addition $(+)$ and multiplication $(\times)$. Justify your conclusions.
   (a) $\{0, 3, 6, 9, 12, \ldots\}$
   (b) $\{1, 3, 5, 7, 9, \ldots\}$
   (c) $\{\ldots, -4, -3, -2, -1, 0\}$
   (d) $\{0, 1, -1, i, -i\}$
6. Find a set X such that $\text{card}(X) = 3$ and such that every member of X is a subset of X.
7. Find the multiplicative inverse (reciprocal) of each non-zero element in the finite field $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.
8. Find the multiplicative inverse (reciprocal) of:
   (a) the element $1 + 3\sqrt{2}$ in the field $\mathbb{Q}(\sqrt{2})$
   (b) the element $3 - 4i$ in the field $\mathbb{Q}(i) = \{x \mid x = a + bi \text{ where } a, b \in \mathbb{Q}\}$
   (c) the element $\begin{bmatrix} 4 & 5 \\ 3 & 4 \end{bmatrix}$ in the ring $M_2(\mathbb{Z})$
9. Show that the finite ring $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (equipped with the operations of addition and multiplication (mod 6)) is <u>not</u> a field.
10. Use the Principle of Mathematical Induction to prove each of the following claims:
    (a) If $a \in \mathbb{R}$ and $a > 0$, then, for every $n \in \mathbb{N}$, $1 + na \leq (1 + a)^n$.
    (b) For every $n \in \mathbb{N}$, $6^n - 1$ is divisible by 5.
    (c) For every $n \in \mathbb{N}$, $1 + 3 + 5 + 7 + \cdots + 2n - 1 = n^2$.
11. Let A and B be finite sets such that $\text{card}(A) = n$, $\text{card}(B) = m$, and $n \geq m$.
    (a) Show that the number of functions from A to B equals m^n.
    (b) Use the above result (a) to show that $\text{card}(\mathcal{P}(A)) = 2^n$.