ELEMENTARY SET THEORY

DONU ARAPURA

1. Sets

A set is a collection of things called elements. We will generally use capital letters for sets. We write $q \in X$ if q is an element. The negation $\neg(q \in X)$ is written as $q \notin X$. We can specify a set by listing the elements within braces,

$$Animal = \{cat, dog, aardvark, cow, snake, mouse, alligator\}$$

$$= \{dog, dog, aardvark, cat, horse, cow, snake, mouse, alligator\}$$

Note that order and repetitions are irrelevant. Thus $cat \in Animal$ but $potato \notin Animal$. We can form infinite sets such as the set of all natural numbers

$$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$$

A set X is a *subset* of a set Y (or $X \subseteq Y$) if all elements X are also elements of Y. That is if for all x, $x \in X$ implies $x \in Y$, or in symbols

$$\forall x \, (x \in X \to x \in Y)$$

For example,

$$Reptile = \{snake, alligator\} \subseteq Animal$$

We can also give a subset by taking all the elements that satisfy a particular property. For example, the set E of even natural numbers is the subset of $n \in \mathbb{N}$ such that n is divisible by 2. In symbols

$$E = \{n \in \mathbb{N} \mid n \text{ is divisible by } 2\}$$

The symbol $|$ can be read as "such that".

Two sets are the considered equal if and only if they contain the same elements, regardless of how they are defined. This is called the axiom of *extensionallity*. Thus for example the set of prime numbers less than 4 equals the set of solutions to $x^2 - 5x + 6 = 0$. In symbols

$$X = Y \leftrightarrow \forall x (x \in X \leftrightarrow x \in Y)$$

Lemma 2. *$X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.*

We going to give semi-formal proof. Based on rules discussed earlier, we can drop $\forall$'s at the beginning and put them back in at the end.

Proof. Suppose $X = Y$. Then $\forall x (x \in X \leftrightarrow x \in Y)$, or simply $x \in X \leftrightarrow x \in Y$. This implies that $(x \in X \to x \in Y)$ and $(x \in Y \to x \in X)$. Since x is arbitrary, we have $X \subseteq Y$ and $Y \subseteq X$.

For the converse we run the argument backwards. (We omit explicit mention of $\forall$ intro. and elim. steps this time around.) If $X \subseteq Y$ and $Y \subseteq X$. Then $(x \in X \to x \in Y)$ and $(x \in Y \to x \in X)$. Therefore $x \in X \leftrightarrow x \in Y$, so that $X = Y$. □

Lemma 3. *X is not a subset of Y ($X \not\subseteq Y$) if and only if there exists $x \in X$ such that $x \notin Y$.*

Proof. Let P and Q denote $x \in X$ and $x \in Y$ respectively. Then $X \not\subseteq Y$ means

$$\neg \forall x (P \to Q)$$

or equivalently

$$\exists x (\neg (P \to Q))$$

Using truth tables or formal proofs, we can see that $P \to Q$ is equivalent to $P \wedge \neg Q$. □

There is a set called the empty set $\emptyset = \{\}$ which contains no elements. We can translate this as $\neg \exists x (x \in \emptyset)$ or equivalently (by DeMorgan) $\forall x (x \notin \emptyset)$. The axiom of extensionallity implies that there is exactly one empty set.

4. Operations on sets

We define operations among sets. Given X and Y, their union $X \cup Y$ is the set of elements which lie in X or in Y. Their intersection $X \cap Y$ is the set of elements which lie in both X and Y. Their difference $X - Y$ consist of elements in X but not Y. Or in logical notation:

(1) $\forall x (x \in X \cup Y \leftrightarrow (x \in X) \vee (x \in Y))$
(2) $\forall x (x \in X \cap Y \leftrightarrow (x \in X) \wedge (x \in Y))$
(3) $\forall x (x \in X - Y \leftrightarrow (x \in X) \wedge (x \notin Y))$

If

$$A = \{aardvark, alligator\}$$

is the subset of *Animal* starting with a, then

$$A \cup Reptile = \{aarvark, alligator, snake\}$$

$$A \cup Reptile = \{alligator\}$$

$$A - Reptile = \{aardvark\}$$

In complete analogy with results from propositional logic, we have

Theorem 5. *Given sets X, Y, Z, the following equalities hold:*

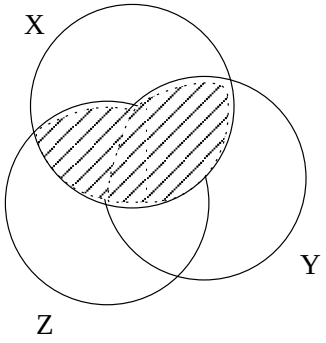
(1) *(Idempotence for $\cap$) $X = X \cap X$.*
(2) *(Idempotence for $\cup$) $X = X \cap X$.*
(3) *(Commutative law for $\cap$) $X \cap Y = Y \cap X$.*
(4) *(Commutative law for $\cup$) $X \cup Y = Y \cup X$.*
(5) *(Associative law for $\cap$) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$.*
(6) *(Associative law for $\cup$) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.*
(7) *(Distributive law I) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.*
(8) *(Distributive law II) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cap Z)$.*
(9) *(DeMorgan law I) $X - (Y \cap Z) = (X - Y) \cap (X - Z)$.*
(10) *(DeMorgan law II) $X - (Y \cup Z) = (X - Y) \cup (X - Z)$.*

Proof. We give a proof of one of the distributive laws, and leave the rest for homework. We will assume that $\in$ take priority over everything else.

$$\begin{aligned} x \in (X \cap (Y \cup Z)) &\leftrightarrow x \in X \wedge x \in (Y \cup Z) \\ x \in X \wedge x \in (Y \cup Z) &\leftrightarrow x \in X \wedge (x \in Y \vee x \in Z) \\ x \in X \wedge (x \in Y \vee x \in Z) &\leftrightarrow (x \in X \wedge x \in Y) \vee (x \in X \wedge x \in Z) \\ (x \in X \wedge x \in Y) \vee (x \in X \wedge x \in Z) &\leftrightarrow x \in (X \cap Y) \vee x \in (X \cap Z) \\ x \in (X \cap Y) \vee x \in (X \cap Z) &\leftrightarrow x \in (X \cap Y) \cup (X \cap Z) \end{aligned}$$

□

There is another way to see these identities using Venn diagrams. One draws three mutually overlapping circles describing the sets X, Y, Z, and shades the regions described on both sides of the equation. Here is the diagram for $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.



5.1. **Homework:**

1. Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $B = \{n^2 | n \in \mathbb{N}\}$ and $E = \{2n | n \in \mathbb{N}\}$. List the elements of $A \cap ((E - B) \cup (B - E))$.

   In problems 2 and 3 use Venn diagrams to show that for any sets A, B, C.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
3. $A \cap ((B - C) \cup (C - B)) = ((A \cap B) - C) \cup ((A \cap C) - B)$
4. Give a written proof of 3 (without Venn diagrams).
5. Give an example of three sets of numbers A, B, C such that $A \cup (B - C) \neq (A \cup B) - C$.
6. Give a written proof that if $A \subseteq B \cup C$ then $A - B \subseteq C$.

6. Functions

Given a pair of objects x and y, we can form a new object (x, y) called an ordered pair. The basic rule is that $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$. Note that (x, y) is not the same as $\{x, y\}$. If A and B are sets then their cartesian product is

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

You would have already encountered this notion in a calculus or linear algebra course, where you consider the plane as the cartesian product $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ of the set of real numbers $\mathbb{R}$ with itself.

A subset of $A \times B$ is called a *relation*. A relation $f \subseteq A \times B$ is called a *function* or *map* from A to B if for every $x \in A$, there is a unique $y \in B$ with $(x, y) \in f$. Given x, we denote this element y by $f(x)$. To translate this into logic, we note that uniqueness of y amounts to asserting that $z = y$ whenever $(x, z) \in f$. Then for f to be a function, we must have

$$\forall x(x \in A \to \exists y[y \in B \wedge (x, y) \in f \wedge \forall z(z \in B \wedge (x, z) \in f \to z = y)])$$

This looks fairly complicated, but we can introduce useful abreviations to make it shorter. Let

(1) $(\forall x \in A)\phi$ stand for $(\forall x)(x \in A \to \phi)$.
(2) $(\exists x \in A)\phi$ stand for $(\exists x)(x \in A \wedge \phi)$.
(3) $(\exists! x)(\dots x \dots)$ stand for $(\exists x)[(\dots x \dots) \wedge \forall z((\dots z \dots) \wedge \to z = x))$

The first two symbols restrict quantifiers to range over a set A. The third symbol $(\exists! x)$ means "there exists a unique x". With these symbols, the condition for f to be a function simply reads

$$(\forall x \in A)(\exists! y)[(x, y) \in f]$$

Some examples of relations are:

(1) $l = \{(dog, 3), (cat, 3), (aardvark, 7), (cow, 3), (snake, 5), (mouse, 5), (alligator, 9)\}$
(2) " $<$ " $= \{(x, y) \in \mathbb{N} \times \mathbb{N} \,|\, x < y\}$
(3) $i = \{(a, b) \in A \times A | \, a = b\}$ for any set A.
(4) $sq = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = x^2\}$.
(5) $sq^{-1} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x = y^2\}$.
(6) $d = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = 2x\}$.

Only items 1, 3, 4 and 6 are functions. $l(x)$ is the number of letters in the word x, $i(x) = x$, $sq(x) = x^2$ and $d(x) = 2x$. The example i is particularly important and is called the *identity* function.

Given a subset $A \subset X$, we define the *image* of A under f to be the subset

$$f(A) = \{y \in Y \mid (\exists x \in A)\}$$

For example, $sq(\mathbb{R})$ is the set of non-negative numbers.

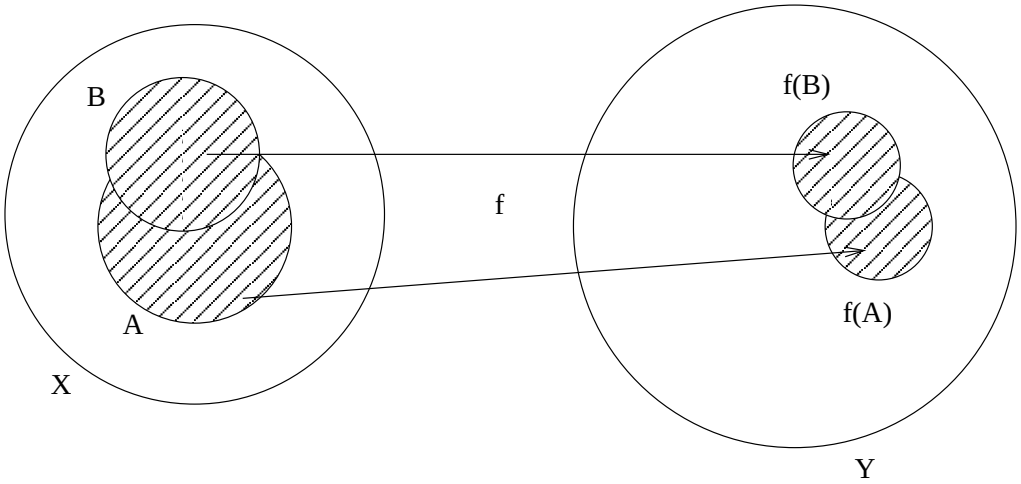
Lemma 7. *If A and B are subsets of X, then*

(1) $f(A \cup B) = f(A) \cup f(B)$.
(2) $f(A \cap B) = f(A) \cap f(B)$.

Proof. We prove the first statement.

$$\begin{aligned}
y \in f(A \cup B) &\leftrightarrow y = f(x) \wedge x \in A \cup B \\
y = f(x) \wedge x \in A \cup B &\leftrightarrow y = f(x) \wedge (x \in A \vee x \in B) \\
y = f(x) \wedge (x \in A \vee x \in B) &\leftrightarrow (y = f(x) \wedge x \in A) \vee (y = f(x) \wedge x \in B) \\
(y = f(x) \wedge x \in A) \vee (y = f(x) \wedge x \in B) &\leftrightarrow (y \in f(A)) \vee (y \in f(B)) \\
(y \in f(A)) \vee (y \in f(B)) &\leftrightarrow y \in f(A) \cup f(B)
\end{aligned}$$

□



We say that a function $f : X \to Y$ is *onto* if $f(X) = Y$. This is equivalent to

$$(\forall y \in Y)(\exists x \in X)(y = f(x))$$

The function $sq : \mathbb{R} \to \mathbb{R}$ above is not onto, since there is no $x \in \mathbb{R}$ with $x^2 = -1$. However, the functions $i : A \to A$ and $d : \mathbb{R} \to \mathbb{R}$ are both onto. We say that $f : X \to Y$ is *one to one* if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. In symbols,

$$(\forall x_1 \in X)(\forall x_2 \in X)(f(x_1) = f(x_2) \to x_1 = x_2)$$

By taking the contrapositive, we get an equivalent condition that $x_1 \neq x_2$ implies that $f(x_1) \neq f(x_2)$. The function d above is one to one, since $2x_1 = 2x_2$ implies $x_1 = x_2$. But l is not, since $l(cat) = l(dog)$.

A function $f : X \to Y$ is called a *one to one correspondence* if it is both one to one and onto. The *inverse* of f is the relation

$$f^{-1} = \{(y, x) \in Y \times X \mid y = f(x)\}$$

For example, the inverse of sq was given above, and

$$l^{-1} = \{(3, dog), (3, cat), (7, aardvark), (3, cow), (5, snake), (5, mouse), (9, alligator)\}$$

Notice that neither of these are functions.

Lemma 8. *A function $f : X \to Y$ is a one to one correspondence if and only if f^{-1} is a function. In this case, $f^{-1}(y)$ is the unique solution to $y = f(x)$.*

9. Equivalence Relations

Given a relation R, we usually write xRy instead of $(x, y) \in R$. A relation R is called an *equivalence relation* if it satisfies the following conditions

(1) It's reflexive, xRx.
(2) It's symmetric, if xRy then yRx.
(3) It's transitive, if xRy and yRz then xRz.

Examples:

(1) Equality.

(2) Given the set

$$C = \{red-shirt, blue-shirt, red-sock, yellow-sock, yellow-shirt\}$$

Define xRy exactly when they have the same color.

(3) Let T be the set of triangles. We view a triangle as a positive triple of positive real numbers (L, K, M) measuring the length of the sides. We will say that two triangles are *congruent* (in symbols $\Delta_1 \equiv \Delta_2$) if these lengths are the same after relabelling the sides.

In order to check 2, we make another definition. A partition of a set S is a subset P of the powerset $P(S)$ such that every $s \in S$ lies in exactly on subset $E \in P$. For example, grouping things of the same color

$$Red = \{red-shirt, red-sock\}$$

$$Blue = \{blue-shirt\}$$

$$Yellow = \{yellow-sock, yellow-shirt\}$$

yields a partition

$$\{Red, Blue, Yellow\}$$

of C.

Lemma 10. *If P is a partition of S, then define $x \sim y$ iff x, y are both in the same set in P. Then $\sim$ is an equivalence relation.*

Thus to each triangle, we can form the set of all posible relabelled triangles.

$$\{(L, K, M), (K, M, L), (M, L, K), (L, M, K), (K, L, M), (M, K, L)\}$$

This gives a partition of the set of triangles, and the corresponding equivalence relation is precisely congruence.

Given functions $f : X \to Y$ and $g : Y \to Z$, we define a new function $g \circ f : X \to Z$ by $g \circ f(x) = g(f(x))$.

Lemma 11. *$g \circ f$ is one to one if f and g are both are.*

You will show in the home work that the same thing goes for "onto". Therefore $g \circ f$ is a one to one correspondence if f and g are both are. We define a relation between sets as follows $X \sim Y$ (read X has the same cardinality as Y) if there is a one to one correspondence $f : X \to Y$.

Theorem 12. *The relation $\sim$ is an equivalence relation.*

Outline of proof (full details in class). In order to show that $X \sim X$, we use the identity function $i : X \to X$ given by $i(x) = x$. This is a one to one correspondence.

If $X \sim Y$, then there exists a one to one correspondence $f : X \to Y$. The inverse $f^{-1} : Y \to X$ gives a one to one correspondence in the opposite direction. Therefore $Y \sim X$.

Suppose that $X \sim Y$ and $Y \sim Z$, then there are one to one correspondences $f : X \to Y$ and $g : Y \to Z$. $g \circ f : X \to Z$ gives another one to one correspondence. Therefore $X \sim Z$.

12.1. **Homework:** All of the problems refers to functions $f : X \to Y$, $g : Y \to Z$, and subsets A, B of X.

1. Prove that $f(A \cap B) = f(A) \cap f(B)$.
2. Prove that $A \subseteq B$ implies $f(A) \subseteq f(B)$.
3. Define $x_1 =_f x_2$ to mean that $f(x_1) = f(x_2)$. Prove that this is an equivalence relation.
4. Prove that $g \circ f$ is onto if f and g are both are.
5. Does $f(A - B) = f(A) - f(B)$? Try and prove it, and if you can't then look for an example where this fails!

13. Natural numbers

The set of natural numbers $\mathbb{N} = \{0, 1, 2 \ldots\}$. We want to give a characterization of this set at its most primitive level. We observe that there is a function $++ : \mathbb{N} \to \mathbb{N}$ called the successor function, which produces the next number: $++(0) = 1, ++(1) = 2, \ldots$. There are three properties which characterize $\mathbb{N}$, called Peano's axioms[1]

P1. $++$ is one to one i.e. $\forall x \forall y(++(x) = ++(y) \to x = y)$.
P2. $0 \notin ++(\mathbb{N})$ i.e. $\forall x(++(x) \neq 0)$.
P3. Given a set X, $x_0 \in X$ and a function $\phi : X \to X$, there exists a unique function $f : \mathbb{N} \to X$ satisfying

$$\begin{cases} f(0) = x_0 \\ f(++(n)) = \phi(f(n)) \end{cases}$$

The last property deserves some comment. It is really a form of *mathematical induction*. However, we are formulating it in terms of the ability to make *inductive* or *recursive* definitions. It says that to define a function for all n, it is enough to define it for 0, and to define the value for $++(n)$ in terms of the value for n. For example, we can define addition inductively by setting $m + n = A_m(n)$ where

$$\begin{cases} A_m(0) = m \\ A_m(++(n)) = ++(A_m(n)) \end{cases}$$

In fact, it is possible to build all the standard operations of arithmetic in this way. There is another form of induction which is probably more familiar. Suppose $P(n)$ is a property of natural numbers that we are trying to prove for all n. Then we can proceed as follows.

Proposition 14 (Mathematical Induction)**.** *If $P(0)$ holds, and $P(n) \to P(++(n))$. Then $\forall n P(n)$.*

Proof. Define functions $p, p' : \mathbb{N} \to \{T, F\}$, with $p(n)$ giving the truth value of $P(n)$, and $p'(n) = T$. Then $p(0) = T$, and $p(++(n)) = p(n)$ by assumption. But $p'(0) = T, p'(++(n)) = p'(n)$ also satisfies these equations. By uniqueness $p = p'$. So $P(n)$ is always true. □

We can replace the property P by the set $X = \{n \mid P(n)\}$. Thus

Corollary 15. *Given $X \subseteq \mathbb{N}$ such that $0 \in X$ and $++(X) \subseteq X$ then $X = \mathbb{N}$.*

As a simple example, let us see that

[1]There a number of variations.

Lemma 16. *Every natural number other than* 0 *is the successor of something.*

Proof. Let $X = \{0\} \cup {+}{+}(\mathbb{N})$. Then ${+}{+}(X) \subseteq X$ and $0 \in X$. Therefore $X = \mathbb{N}$. □

We give a proof of the commutative law for addition $m + n = n + m$ from first principles. Since this involves induction on two variables, the proof is quite tricky.

Theorem 17. *The following hold for all* $m, n \in \mathbb{N}$.

(1) $A_0(n) = n$.
(2) ${+}{+}(A_n(m)) = A_{{+}{+}(n)}(m)$.
(3) $A_m(n) = A_n(m)$.

Proof. We prove (1) by induction. We have $A_0(0) = 0$. Suppose (1) holds for n. Then $A_0({+}{+}(n)) = {+}{+}(A_0(n)) = {+}{+}(n)$ as required to finish the induction.

We prove (2) by induction on m. For $m = 0$:

$$A_{{+}{+}(n)}(0) = {+}{+}(n) = {+}{+}(A_n(0))$$

Suppose (2) holds for m. Then

$$A_{{+}{+}(n)}({+}{+}(m)) = {+}{+}(A_{{+}{+}(n)}(m)) = {+}{+}({+}{+}(A_n(m))) = {+}{+}(A_n({+}{+}(m)))$$

We prove the final statement by induction on n. When $n = 0$, we use (1) to obtain

$$A_m(0) = m = A_0(m)$$

Suppose (3) holds for n. Then from (2), we get

$$A_m({+}{+}(n)) = {+}{+}(A_m(n)) = {+}{+}(A_n(m)) = A_{{+}{+}(n)}(m)$$

□

17.1. **Homework.**

1. Let $m \leq n$ stand for $\exists \ell (n = m + \ell)$. Prove that $n \neq 0$ if and only if $1 \leq n$.
2. Prove the associative law $(\ell + m) + n = \ell + (m + n)$, or equivalently $A_{\ell+m}(n) = A_\ell(A_m(n))$. (Hint: do this by induction on n.)
3. Prove that $\leq$ is transitive: $(m \leq n) \wedge (n \leq r) \to (m \leq r)$.

18. Finite sets

We defined $\leq$ in the homework, and let $n < m$ stand for $n \leq m \wedge n \neq m$. We have following basic properties (which we will assume)

(1) $\leq$ is reflexive: $n \leq n$.
(2) $\leq$ is transitive.
(3) $\leq$ is antisymmetric $n \leq m$ and $m \leq n$ implies $n = m$.
(4) $\leq$ is a total order: $\forall m \forall n (m \leq n \vee n \leq m)$.

Given a natural number $n \in \mathbb{N}$, let

$$[n] = \{m \in \mathbb{N} \,|\, m < n\} = \{0, 1, \ldots m - 1\}$$

A set X is called *finite* if there is a one to one correspondence $f : [n] \to X$ for some $n \in \mathbb{N}$, otherwise it is infinite.

Theorem 19. *If there is a one to one correspondence from* $[m]$ *to* $[n]$*, then* $m = n$.

Proof. We will prove this by induction on the minimum M of n and m. Suppose that M is zero. Then $n = 0$ or $m = 0$. If $n = 0$, then $[n] = \emptyset$, so that $f : \emptyset \to [m]$ is onto. It follows that $m = 0$. If $m = 0$, then $f^{-1} : \emptyset \to [n]$ is onto, so that $n = 0$.

Assume that $M > 0$ and that the theorem holds for $M - 1$. Then define $g : [n-1] \to [m-1]$ by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < f(n-1) \\ f(i) - 1 & \text{if } f(i) > f(n-1) \end{cases}$$

This is a one to one correspondence, therefore $m - 1 = n - 1$, which implies $m = n$. □

Corollary 20. *If X is finite, then there is a unique natural n for which there is a one to one correspondence from $[n] \to X$.*

The number n above is called the *cardinality* of X, it is denoted by $card(X)$.

Theorem 21. *If X and Y are two disjoint finite sets then $X \cup Y$ is finite and $card(X \cup Y) = card(X) + card(Y)$.*

Proof. Let $f : [n] \to X$ and $g : [m] \to Y$ be one to one correspondences. Define $h : [n + m] \to X \cup Y$ by

$$h(i) = \begin{cases} f(i) & \text{if } i < n \\ g(i - n) & \text{if } i \geq n \end{cases}$$

This is a one to one correspondence. □

Corollary 22. *If X and Y are finite, then $card(X \cup Y) = card(X) + card(Y) - card(X \cap Y)$.*

Proof. We can write X as a disjoint union

$$X = (X - Y) \cup (X \cap Y)$$

Therefore $card(X) = card(X - Y) + card(X \cap Y)$. Likewise $card(Y) = card(Y - X) + card(X \cap Y)$. Expressing $X \cup Y$ as disjoint union

$$X \cup Y = (X - Y) \cup (Y - X) \cup (X \cap Y)$$

gives

$$card(X \cup Y) = card(X - Y) + card(Y - X) + card(X \cap Y)$$

$$= card(X) - card(X \cap Y) + card(Y) - card(X \cap Y) + card(X \cap Y)$$

which simplifies to the above expression. □

We can now define multiplication by the formula $m \cdot n = card([m] \times [n])$. Then $card(X \times Y) = card(X)card(Y)$ for any pair of finite sets. The basic laws follow easily from this definition.

Theorem 23.

(1) $m \cdot n = n \cdot m$.
(2) $m \cdot (n \cdot r) = (m \cdot n) \cdot r$.
(3) $m \cdot (n + r) = m \cdot n + m \cdot r$

Proof. For (1), define the one to one correspondence $s : [m] \times [n] \to [n] \times [m]$ by $s(x, y) = (y, x)$.

For (2), define the one to one correspondence $f : [m] \times ([n] \times [r]) = ([m] \times [n]) \times [r]$ by $f(x, (y, z)) = ((x, y), z)$.

For (3), choose disjoint sets X, Y, Z of cardinality m, n and r respectively. Then we have a disjoint union

$$X \times (Y \cup Z) = X \times Y \cup X \times Z$$

□

24. Countable sets

A set X is called *countably infinite* or just *countable* if there is a one to one correspondence $f : \mathbb{N} \to X$. (The point here is that there are uncountable sets, so infinite does not imply countable.)

Example 25. $\mathbb{N}$ *is countable (using the identity function).*

Example 26. *The sets E and O of even and odd natural numbers are countable.*

The functions $f : \mathbb{N} \to E$ and $g : \mathbb{N} \to O$ given by $f(n) = 2n$ and $g(n) = 2n + 1$ are one to one correspondences.

Lemma 27. *If X and Y are disjoint countable sets, then $X \cup Y$ is also countable.*

Proof. Let $f : \mathbb{N} \to X$ and $g : \mathbb{N} \to Y$ be the one to one correspondences. Define $h : \mathbb{N} \to X \cup Y$ by

$$h(n) = \begin{cases} f(n/2) & \text{if } n \text{ is even} \\ g((n-1)/2) & \text{if } n \text{ is odd} \end{cases}$$

It follows that the set of integers $\mathbb{Z}$ is countable since it can be written as a disjoint union of $\mathbb{N}$ and the set of negative integers.

Theorem 28. *An infinite subset of $\mathbb{N}$ is countable.*

Before giving the proof, we recall the well ordering principle which is closely related to induction:

Theorem 29. *Every nonempty subset of $\mathbb{N}$ has a smallest element.*

Now we prove the previous theorem. Let X be an infinite subset of $\mathbb{N}$. We define a function $f : \mathbb{N} \to X$ as follows. Let $f(0)$ be the smallest element of X, let $f(1)$ to be the smallest element of $X - \{f(0)\}$ and so on. More precisely, we can use an inductive definition. If $f(n)$ is already been defined, then let $f(n + 1)$ be the smallest element of $\{x \in X \mid x > f(n)\}$ (this can't be empty since X is infinite).

We prove that f is onto by contradiction. So we assume that f is not onto. Let x be the smallest element of X which is not in the image of f. The set $T = \{t \in X \mid t < x\}$ is finite and nonempty (since otherwise $x = f(0)$). Let $\tau \in T$ be the largest element. All elements of T lie in the image of f; in particular, $\tau = f(n)$ for some n. It should be clear from our set up that x is the smallest element of X greater than $f(n)$. Thus $x = f(n + 1)$ contrary to assumption.

By construction, we have $f(n) < f(n + 1) < f(n + 2) \ldots$. Thus $f(n) < f(m)$ whenever $n < m$. This shows that f is one to one, and so we are done.

Theorem 30. *If $X_0, X_1 \ldots$ is a countable collection of finite or countable sets, then $X_0 \cup X_1 \cup \ldots$ is countable.*

We are going to give a proof based on facts from arithmetic that we recall. A natural number is prime if it at least 2, and it has no divisors other than 1 and itself. For example, $2, 3, 5, 7, 11 \ldots$ are prime. We need two facts.

1) There are infinitely many primes. Thus the set of primes are countable, so we can label them $p_0, p_1 \ldots$

2) Fundamental theorem of arithmetic: Any natural greater than 1 can be factored into a product of primes in exactly one way (up to rearranging factors, e.g $52 = 2^2 \times 13$).

Proof of the theorem. We assume for simplicity that all the sets are disjoint ($X_i \cap X_j = \emptyset$ whenever $i \neq j$) and countable, and that we have one to one correspondences $f_i : \mathbb{N} \to X_i$. Define $S = \{p_i^{n+1} \,|\, i, n \in \mathbb{N}\}$ be the set of positive powers of primes. S is countable, so it is enough to construct a one to one correspondence from it to $X_0 \cup X_1 \ldots$. We do this simply by sending $p_i^{n+1} \to f_i(n)$. This is certainly onto. It is one to one by the fundamental theorem of arithmetic.

Corollary 31. $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof This can be written as a union $\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\} \cup \ldots$.

By a similar argument, we can prove the set $\mathbb{Q} = \{a/b \,|\, a, b \in \mathbb{Z},\, b \neq 0\}$ of rational numbers is countable. We leave this for homework.

31.1. **Homework:**

1. Let $X_1, \ldots X_n$ be disjoint finite sets. Prove by induction that $card(X_1 \cup X_2 \cup \ldots X_n) = card(X_1) + card(X_2) + \ldots card(X_n)$.
2. Let X and Y be finite sets, and let F be the set of functions from X to Y. What do you think the cardinality of this set is? Prove it!
3. Prove (from first principles) that the union of a finite set with a countable set is countable.
4. Given a finite set A called an alphabet, a string is a finite sequence of elements in A e.g. "aardvark" is a string in the Roman alphabet. Show that the set of strings S is countable (hint: write this as a countable union ...).
5. Prove that $\mathbb{Q}$ is countable.

32. Uncountable sets

One might get the feeling that one infinite set is as big as any other, but in fact:

Theorem 33 (Cantor)**.** *The set of real numbers* $\mathbb{R}$ *is uncountable.*

Before giving the proof, recall that a real number is an expression given by a (possibly infinite) decimal, e.g. $\pi = 3.141592 \ldots$. The notation is slightly ambigous since

$$1.0 = .9999 \ldots$$

We will break ties, by always insisting on the more complicated nonterminating decimal.

Proof It suffices to prove that $\mathbb{R}$ has an uncountable subset. We we work with numbers in the interval $I = \{x \in \mathbb{R} \,|\, 0 \leq x \leq 1\}$. We give a proof by contradiction.

Suppose that I was countable, and let's say that $f : \mathbb{N} \to I$ is a one to one correspondence. Let y_i be the ith digit of the ith number on this list. Now let

$$x_i = \begin{cases} 0 & \text{if } y_i = 9 \\ y_i + 1 & \text{otherwise} \end{cases}$$

This yields a new number $x = .x_1x_2\ldots \in I$ which differs from every number on this list $f(0), f(1), \ldots$ by at least one digit. Then we have found a number not in the image of f, which contradicts the fact f is onto. For example if

$$f(0) = .\underline{1}23\ldots;\ y_1 = 1$$
$$f(1) = .2\underline{5}6\ldots;\ y_2 = 5$$
$$f(2) = .26\underline{9}\ldots;\ y_3 = 9$$
$$\ldots$$

Then

$$x = .260\ldots$$

Cantor originally applied this to prove that most real numbers are not solutions to polynomial equations with integer coefficients (contrary to earlier hopes). We expand on this idea as follows. Say that a number is *describable* if there is a name (such as 5, π) or formula (e.g. $1+\sqrt{2}/3$) for it, or perhaps a computer program for calculating it. The point is that the description should involve a finite number of symbols in a fixed finite alphabet. Since the set of such descriptions is countable (by homework), we obtain.

Corollary 34. *There are real numbers which cannot be described (and in particular computed).*

This is the starting point for Cantor's theory of *transfinite* numbers. The cardinality of a countable set (denoted by the Hebrew letter $\aleph_0$) is at the bottom. Then we have the cardinallity of $\mathbb{R}$ denoted by $2^{\aleph_0}$, because it is possible to find a one to one correspondence $\mathbb{R} \to P(\mathbb{N})$. We can continue this process indefinitely because

Theorem 35 (Cantor)**.** *For any set X, there does not exist a one to one correspondence from X to $P(X)$. In particular, the power set $P(\mathbb{N})$ is uncountable.*

Proof We prove this by contradiction. Suppose that $f : X \to P(X)$ is a one to one correspondence. Define $C = \{x \,|\, x \notin f(x)\}$. Note that C is an element of $P(X)$, it is given as $f(x_0)$ for some $x_0 \in X$. Either $x_0 \in C$ or $x_0 \notin C$. If $x_0 \in C$, then $x_0 \notin f(x_0) = C$ which is a contradiction. So $x_0 \notin C = f(x_0)$, this implies that $x_0 \in C$, which is again a contradiction. The only way to avoid a contradiction is for f not to exist.

35.1. **Homework.**

1. Prove that the set of all irrational real numbers is uncountable.
2. Prove that the set of functions $f : \mathbb{N} \to \mathbb{N}$ is uncountable.