Chapter 3

The integers

Recall that an abelian group is a set A with a special element 0, and operation + such that

$$x + 0 = x$$

$$x + y = y + x$$

$$x + (y + z) = (x + y) + z$$

$$\text{every element } x \text{ has an inverse } x + y = 0$$

We also should recall that the inverse is unique, so we denote it by $-x$. We also define subtraction by $y - x = y + (-x)$. In this chapter, we look at the most important 1 example which is the abelian group of integers $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$. This can be characterized by some additional axioms. Let $\mathbb{N} = \{0, 1, 2, \dots\}$ be the subset of natural numbers. Then

1. If $x \in \mathbb{Z}$ then either $x \in \mathbb{N}$ or $-x \in \mathbb{N}$.

2. Both $x \in \mathbb{N}$ and $-x \in \mathbb{N}$ if and only if $x = 0$.

3. If $x \in \mathbb{N}$ and $y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.

4. Mathematical induction: If $S \subseteq \mathbb{N}$ contains 0 and is closed under addition by 1, then $S = \mathbb{N}$.

To appreciate what we can do with these axioms, let us define $x \leq y$ to mean that $y = x + z$ such that $z \in \mathbb{N}$. We can also define all the usual variants. For example $x < y$ means that $x \leq y$ and $x \neq y$.

Lemma 3.1. *$x \leq y$ if and only if $y - x \in \mathbb{N}$.*

Proof. Adding $-x$ to $y = x + z$ and using the associative and commutative laws shows that

$$y - x = (x + z) + (-x) = -x + (x + z) = (-x + x) + z = 0 + z = z$$

□

Theorem 3.2. *The relation $\leq$ is a* linear ordering*, which means that it is*

1. *Reflexive: $x \leq x$*
2. *Antisymmetric: if $x \leq y$ and $y \leq x$ then $x = y$*
3. *Transitive: if $x \leq y$ and $y \leq z$ then $x \leq z$*
4. *Linear: for any x, y, either $x \leq y$ or $y \leq x$.*

Proof. $x \leq x$ because $x = x + 0$.

Suppose that $x \leq y$ and $y \leq x$, then $x - y \in \mathbb{N}$ and $y - x \in \mathbb{N}$. But $y - x = -(x - y)$ (this requires a proof, but it will be relegated to the exercises). By our axioms for $\mathbb{N}$, this forces $x - y = 0$. So $x = y$.

If $x \leq y$ and $y \leq z$ then $y - x \in \mathbb{N}$ and $z - y \in \mathbb{N}$. This implies (by our axioms) that $(y - x) + (z - y) \in \mathbb{N}$. By the associative and commutative laws, we can rearrange this as

$$(y - x) + (z - y) = y - x + z - y = (y - y) + z - x = z - x$$

Thus $z - x \in \mathbb{N}$ which means that $x \leq z$.

Given x and y, either $x - y \in \mathbb{N}$ or $y - x \in \mathbb{N}$ by our axioms. So either $x \leq y$ or $y \leq x$.

□

The induction axiom, which wasn't needed in the previous proof, is a very powerful tool that you have probably used before. It allows us to prove statements like

$$0 + 1 + 2 + \dots n = \frac{n(n+1)}{2}, \quad n \in \mathbb{N}$$

To do this, let S be the set of natural numbers where this holds. Then certainly $0 \in S$. We can see that if $n \in S$ then $n + 1 \in S$ by adding $n + 1$ to both sides and simplifying to obtain

$$0 + 1 + 2 + \dots n + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = \frac{(n+1)(n+2)}{2}$$

Thus $S = \mathbb{N}$. There a number of useful variants of induction.

Theorem 3.3 (Well ordering property)**.** *Any nonempty subset $S \subseteq \mathbb{N}$ has a least element.*

Proof. Let M be the set of natural numbers so that $m \leq s$ for every $s \in S$. Then $0 \in M$. If $s \in S$ then $s + 1 \in M$. Therefore M cannot equal $\mathbb{N}$. So there exists a number $m \in M$ such that $m + 1 \notin M$. We have $m \leq s$ for all $s \in S$ by definition of M. However, $m \notin M$ so $m + 1 > s_0$ for some s_0 in S. This forces $s_0 < m + 1 \leq s_0 + 1$ which is only possible if $m = s_0$. So to summarize $m \in S$ and $m \leq s$ for all s. Therefore m is the least element. □

Theorem 3.4 (Strong induction)**.** *Suppose that $P \subseteq \mathbb{N}$ is a subset such that $0 \in P$ and $n \in P$ whenever $0, 1, \dots n - 1 \in P$ then $P = \mathbb{N}$.*

Proof. We prove this by contradiction. Suppose that $P \neq \mathbb{N}$. Then the complement $S = \{n \in \mathbb{N} \mid n \notin P\}$ is nonempty. Let s be the least element. Then $s \neq 0$ because $0 \in P$. Since s is the least element, all the numbers $0, 1, \ldots s - 1 \in P$. But this implies that $s \in P$ which is a contradiction. □

There is another kind of induction is very useful, and that is inductive or recursive definitions, where a function is defined in terms of its previous values. This often is used implicitly. For example the factorial

$$n! = 1 \cdot 2 \cdots n = (1 \cdot 2 \cdots (n-1))n$$

is really short for the inductive definition

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{otherwise} \end{cases}$$

Here is the general statement.

Theorem 3.5. *Given a set A, an element $a \in A$, and a function $g : \mathbb{N} \times A \to A$, there exists a unique function $f : \mathbb{N} \to A$ satisfying*

$$f(n) = \begin{cases} a & \textit{if } n = 0 \\ g(n, f(n-1)) & \textit{otherwise} \end{cases}$$

Before giving the proof, we need to clarify exactly what a function is. Given sets X, Y, the cartesian product $X \times Y$ is the set of ordered pairs $\{(x, y) \mid x \in X, y \in Y\}$. A subset of $X \times Y$ is called a *relation.* We can identify a function $f : X \to Y$ with its graph, which is the relation $\{(x, y) \mid y = f(x), x \in X\}$. Relations which arise from functions are very special.

Definition 3.6. *A subset $f \subset X \times Y$ is a function if for every $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$. We then write $y = f(x)$.*

The key step to prove the theorem is the following.

Lemma 3.7. *Let $A, a,$ and g be as above, then there exists a sequence of functions $f_n : \{0, 1, 2 \ldots n\} \to A$ so that each f_n satisfies the conditions of the proposition, and such that f_n and f_{n-1} agree on their domains.*

Proof. We prove this by induction. Let $f_0(0) = a$. If f_n exists, then we define

$$f_{n+1}(x) = \begin{cases} f_n(x) & \text{if } x \leq n \\ g(n, f(n)) & \text{otherwise} \end{cases}$$

□

Proof of theorem. Thinking of f_n as a subset $\{0, 1, \ldots n\} \times A$ we define $f = \bigcup_n f_n = f_0 \cup f_1 \cup \ldots$. This determines a function which agrees with f_n on its domain. Therefore the theorem follows from the previous lemma. □

Natural numbers are important because they can be used to count. Given a natural number $n \in \mathbb{N}$, let

$$[n] = \{x \in \mathbb{N} \mid x < n\} = \{0, 1, 2, \dots n-1\}$$

Let X be a set, then we say that X has n elements, or that X has cardinality n, or $|X| = n$ if there exists a one to one correspondence $f : [n] \to X$. (A one to one correspondence is the same thing as function which is one to one and onto.) If no such n exists, then we say that X is an infinite set. The first problem is to show that $|X|$ cannot have multiple values. This is guaranteed by the following:

Theorem 3.8. *If there exists a one to one correspondence $f : [n] \to [m]$, then $n = m$.*

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 $m = n$. □

Proposition 3.9. *If a finite set X can be written as a union of two disjoint subsets $Y \cup Z$, then $|X| = |Y| + |Z|$. (Recall that $Y \cup Z = \{x \mid x \in Y \text{ or } x \in Z\}$, and disjoint means their intersection is empty.)*

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

A *partition* of X is a decomposition of X as a union of subsets $X = Y_1 \cup Y_2 \cup \dots Y_n$ such that Y_i and Y_j are disjoint whenever $i \neq j$.

Corollary 3.10. *If $X = Y_1 \cup Y_2 \cup \dots Y_n$ is a partition, then $|X| = |Y_1| + |Y_2| + \dots |Y_n|$.*

Proof. We have that

$$|X| = |Y_1| + |Y_2 \cup \dots Y_n| = |Y_1| + |Y_2| + |Y_3 \cup \dots Y_n| = \dots = |Y_1| + |Y_2| + \dots |Y_n|$$

□

Given a function $f : X \to Y$ and an element $y \in Y$, the preimage

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

Proposition 3.11. *If $f : X \to Y$ is a function, then*

$$|X| = \sum_{y \in Y} |f^{-1}(y)|$$

Proof. The collection $\{f^{-1}(y)\}$ forms a partition of X. □

Next consider the cartesian product of two finite sets.

Theorem 3.12. *If X and Y are finite sets, then $|X \times Y| = |X||Y|$.*

Proof. Let $p : X \times Y \to Y$ be the projection map defined by $p(x, y) = y$. Then

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

and $(x, y) \to x$ gives a one to one correspondence to X. Therefore, by the previous corollary,

$$|X \times Y| = \sum_{y \in Y} |p^{-1}(y)| = |Y||X|$$

□

Finally, we are ready to tie up a loose end from before.

Theorem 3.13. $|S_n| = n!$

Proof. The intuitive argument is that to specify a permutation,

$$\begin{pmatrix} 1 & 2 & \dots & n \\ n \text{ choices} & n-1 \text{ choices} & \dots & 1 \text{ choice} \end{pmatrix}$$

we make $n(n-1)\dots 1 = n!$ choices. We will turn this into a rigorous proof using induction on n starting from $n = 1$. The case $n = 1$ is clear because the identity $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is the only permutation.

Now assume that the theorem holds for $n - 1$, i.e. that $S_{n-1} = (n-1)!$. Consider the map $\phi : S_n \to \{1, \dots, n\}$ sending f to $f(n)$. We claim that there is a one to one to correspondence between $\phi^{-1}(i)$ and S_{n-1} for any $i \in \{1, \dots, n\}$. Assuming the claim, we are done because proposition 3.11 implies that

$$|S_n| = \sum_{i=1}^{n} |\phi^{-1}(i)| = \sum_{i=1}^{n} (n-1)! = n(n-1)! = n!$$

It now remains to prove the claim. To start off, consider $\phi^{-1}(n)$. This is the set of permutations $f \in S_n$ of the form

$$\begin{pmatrix} 1 & \dots & n-1 & n \\ f(1) & \dots & f(n-1) & n \end{pmatrix}$$

Removing the last column $\begin{pmatrix} n \\ n \end{pmatrix}$ gives a permutation of $1, \dots, n-1$. Conversely, adding this column to a permutation in S_{n-1} yields an element of $\phi^{-1}(n)$. So we have a one to one correspondence between $\phi^{-1}(n)$ and S_{n-1} as claimed. The general case is similar but a bit messier to write out. Given i, let

$$g(k) = \begin{cases} k & \text{if } k < i \\ k-1 & \text{if } k \geq i \end{cases}$$

We define a function from $\phi^{-1}(i) \to S_{n-1}$ defined by

$$\begin{pmatrix} 1 & \dots & n-1 & n \\ f(1) & \dots & f(n-1) & i \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & n-1 \\ g(f(1)) & \dots & g(f(n-1)) \end{pmatrix}$$

can be seen to be a one to one correspondence.

□

3.14 Exercises

1. Given integers a, b, c, d such that $a \leq b$ and $c \leq d$ prove that $a + c \leq b + d$.

2. Given an abelian group A, an element $a \in A$ and $n \in \mathbb{N}$, we define $n \cdot a = a + a + \dots$ (n times) by induction. To make this a bit clearer, write this as $m_a(n)$ temporarily. Then

$$m_a(n) = \begin{cases} 0 & \text{if } n = 0 \\ a + m_a(n-1) & \text{otherwise} \end{cases}$$

   Prove one of the distributive laws $n(a + b) = na + nb$, or equivalently that $m_{a+b}(n) = m_a(n) + m_b(n)$, by induction on n.

3. Given finite sets Y, Z. Prove that $|Y \cup Z| = |Y| + |Z| - |Y \cap Z|$. Recall that the intersection $Y \cap Z = \{x \mid x \in Y \text{ and } x \in Z\}$.

4. If $B \subseteq A$, prove that $|A - B| = |A| - |B|$, where $A - B = \{a \mid a \in A \text{ and } a \notin B\}$. Use this to prove that the set of distinct pairs $\{(x_1, x_2) \in X \times X \mid x_1 \neq x_2\}$ has $|X|^2 - |X|$ elements.

5. We can use the above counting formulas to solve simple exercises in probability theory. Suppose that a 6 sided dice is rolled twice. There are $6 \times 6 = 36$ possible outcomes. Given a subset S of these outcomes, called an *event*, the probability of S occurring is $|S|/36$.

   a) What is the probability that a five or six is obtained on the first role?
   b) What is the probability that a five or six is obtained in either (or both) roll(s)?
   c) What is probability that the same number is rolled twice?
   d) What is probability that different numbers be obtained for each roll?

   It's important that you explain how you got your answers.