Chapter 5

Finite sets, counting and group theory

Let $\mathbb{N} = \{0, 1, 2 \ldots\}$ be the set of natural numbers. Given n, let $[n] = \{x \in \mathbb{N} \mid x < n\}$. So that $[0] = \emptyset$ is the empty set, and $[n] = \{0, 1, \ldots, n-1\}$ if $n > 0$. A set X is called *finite* if there is a one to one onto function (also called a one to one correspondence) $f : [n] \to X$ for some $n \in \mathbb{N}$. The choice of n is unique (which we will accept as a fact), and is called the cardinality of X, which we denote by $|X|$.

Lemma 5.1. *If X is finite and $g : X \to Y$ is a one to one correspondence, then Y is finite and $|Y| = |X|$.*

Proof. By definition, we have a one to one correspondence $f : [n] \to X$, where $n = |X|$. Therefore $g \circ f : [n] \to Y$ is a one to one correspondence. □

Proposition 5.2. *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 $X = Y_1 \cup Y_2 \cup \ldots Y_n$ such that Y_i and Y_j are disjoint whenever $i \neq j$.

Corollary 5.3. *If $X = Y_1 \cup Y_2 \cup \ldots Y_n$ is a partition, then $|X| = |Y_1| + |Y_2| + \ldots |Y_n|$.*

Proof. We have that

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

□

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 5.4. *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. □

The cartesian product of two sets is the set of ordered pairs

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

Theorem 5.5. *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,

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

□

Let us apply these ideas to group theory.

Given a subgroup $H \subset G$ and $g \in G$, let $gH = \{gh \mid h \in H\}$. This is called a (left) coset. For example, when $G = S_3$ and $H = \{I, (123), (321)\}$, the cosets are

$$IH = (123)H = (321)H = H$$

and

$$(12)H = (13)H = (23)H = \{(12), (13), (23)\}$$

Thus the collection of distinct cosets gives a partition of S_3 into rotations and flips, and there are the same number of each. We will prove that is a similar statement in general.

Lemma 5.6. *If two cosets g_1H and g_2H have a nonempty intersection then $g_1H = g_2H$.*

Proof. If $g \in g_1 H \cap g_2 H$, we can write $g = g_1 h_1 = g_2 h_2$ with $h_1, h_2 \in H$. Then $g_2 = g_1 h_1 h_2^{-1}$. If $h \in H$, then $h_1 h_2^{-1} h \in H$ because H is a subgroup. Therefore $g_2 h = g_1 h_1 h_2^{-1} h \in g_1 H$. This proves that $g_2 H \subseteq g_1 H$. The same argument, with g_1 and g_2 interchanged, shows that $g_1 H \subseteq g_2 H$. Therefore these sets are equal. □

Lemma 5.7. *G/H is a partition of G*

Proof. Every element $g \in G$ lies in the coset gH. Therefore G is the union of cosets. By the previous lemma, the cosets are pairwise disjoint. □

Lemma 5.8. *If H is finite, $|gH| = |H|$ for every g.*

Proof. Let $f : H \to gH$ be defined by $f(h) = gh$. Then f is onto. Suppose that $f(h_1) = f(h_2)$. Then $h_1 = g^{-1} g h_1 = g^{-1} g h_2 = h_2$. Therefore f is also one to one. Consequently $|gH| = |H|$. □

Theorem 5.9 (Lagrange)**.** *If $H \subseteq G$ is a subgroup of a finite group, then*

$$|G| = |H| \cdot |G/H|$$

In particular, the order of H divides the order of G.

Proof. By the previous results, G/H is a partition of G into $|G/H|$ sets each of cardinality $|H|$. □

Given $g \in G$, the *order* of g is the smallest positive n such that $g^n = e$. This was shown in a previous exercise to be the order of the subgroup generated by g. Therefore:

Corollary 5.10. *The order of any element $g \in G$ divides the order of G.*

Corollary 5.11. *If the order G is a prime number, then G is cyclic.*

Proof. Let $p = |G|$. By the previous corollary $g \in G$ divides p. If $g \neq e$, then the order must be p. Therefore G is generated by g. □

One can ask whether the converse of the first corollary holds, that is if $|G|$ is divisible by n, does G necessarily have element of order n? The answer is no, it would fail for $n = |G|$ unless G is cyclic. Even if we require $n < |G|$ then it may still fail (exercise 9). However, if n is prime, then it is true.

Theorem 5.12 (Cauchy)**.** *If the order of a finite group G is divisible by a prime number p, then G has an element of order p*

Proof when $p = 2$. Suppose that G is even. We can partition G into $A = \{g \in G \mid g^2 = e\}$ and $B = \{g \in G \mid g^2 \neq e\}$. Therefore $|G| = |A| + |B|$. Every element $g \in B$ satisfies $g \neq g^{-1}$. Therefore $|B|$ is even, because we can write B as a disjoint union of pairs $\{g, g^{-1}\}$. Therefore $|A| = |G| - |B|$ is even. Furthermore $|A| \geq 1$ because $e \in A$. It follows that A contains an element different from e, and this must have order 2. □

Next, we want to develop a method for computing the order of a subgroup of S_n.

Definition 5.13. *Given $i \in \{1, \ldots, n\}$, the orbit* $\mathrm{Orb}(i) = \{g(i) \mid g \in G\}$. *A subgroup $G \subseteq S_n$ is called transitive if for some i,* $\mathrm{Orb}(i) = \{1, \ldots, n\}$.

Definition 5.14. *Given subgroup $G \subseteq S_n$ and $i \in \{1, \ldots n\}$, the stabilizer of i, is* $\mathrm{Stab}(i) = \{f \in G \mid f(i) = i\}$

Theorem 5.15 (Orbit-Stabilizer theorem)**.** *Given a subgroup $G \subseteq S_n$, and $i \in \{1, \ldots, n\}$ then*

$$|G| = |\operatorname{Orb}(i)| \cdot |\operatorname{Stab}(i)|$$

In particular,

$$|G| = n|\operatorname{Stab}(i)|$$

if G is transitive.

Proof. We define a function $f : G \to \mathrm{Orb}(i)$ by $f(g) = g(i)$. The preimage $T = f^{-1}(j) = \{g \in G \mid g(i) = j\}$. By definition if $j \in \mathrm{Orb}(i)$, there exists $g_0 \in T$. We want to show that $T = g_0 \operatorname{Stab}(i)$. In one direction, if $h \in Stab(i)$ then $g_0 h(i) = j$. Therefore $g_0 h \in T$. Suppose $g \in T$. Then $g = g_0 h$ where $h = g_0^{-1} g$. We see that $h(i) = g_0^{-1} g(i) = g_0^{-1}(j) = i$. Therefore, we have established that $T = g_0 \operatorname{Stab}(i)$. This shows that

$$|G| = \sum_{j \in \mathrm{Orb}(i)} |f^{-1}(j)| = \sum_{j \in \mathrm{Orb}(i)} |\operatorname{Stab}(i)| = |\operatorname{Orb}(i)| \cdot |\operatorname{Stab}(i)|$$

□

Corollary 5.16. $|S_n| = n!$

Proof. We prove this by mathematical induction starting from $n = 1$. When $n = 1$, S_n consists of the identity so $|S_1| = 1 = 1!$. In general, assuming that the corollary holds for n, we have prove it for $n+1$. The group S_{n+1} acts transitively on $\{1, \ldots, n+1\}$. We want to show that there is a one to one correspondence between $\mathrm{Stab}(n+1)$ and S_n. An element of $f \in \mathrm{Stab}(n+1)$ looks like

$$\begin{pmatrix} 1 & 2 & \ldots n & n+1 \\ f(1) & f(2) & \ldots f(n) & n+1 \end{pmatrix}$$

Dropping the last column yields a permutation in S_n, and any permutation in S_n extends uniquely to an element of $\mathrm{Stab}(n+1)$ by adding that column. Therefore we have established the correspondence. It follows that $|\operatorname{Stab}(n+1)| = |S_n| = n!$. Therefore

$$|S_{n+1}| = (n+1)|\operatorname{Stab}(n+1)| = (n+1)(n!) = (n+1)!$$

□

5.17 Exercises

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

2. 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.

3. 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?

   Explain how you got your answers.

4. Let $G \subseteq S_n$ be a subgroup.

   (a) Prove that the stablizer H of an element i is a subgroup of G.

   (b) A subgroup $H \subset G$ is a normal subgroup if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. Is the stabilizer a normal subgroup?

5. By the previous results, the order of an element $g \in S_n$ must divide $n!$. We can do much better. Find a better bound using the cycle decomposition.

6. What is the probability that an element of S_5 has order 2?

7. Choose two elements g_1, g_2 from a finite group G. What is the probability that $g_1 g_2 = e$?

8. Determine all the transitive subgroups of S_3.

9. Let $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \mathbb{Z}_{m_n} = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{Z}_{m_i}\}$ be the set of vectors.

   (a) Show that this becomes a group using $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ with mod m_i arithmetic in each slot.

   (b) Show that the order of this group is $m_1 m_2 \ldots m_n$.

   (c) Let m be the least common multiple of $m_1, \ldots, m_n$. Show that all elements have order dividing m.

10. Prove that Cauchy's theorem holds for the group defined in the previous exercise.