Chapter 4

Cyclic groups and dihedral groups

Consider the group C_n of rotational symmetries of a regular n-gon. If we label the vertices consecutively by $1, 2 \dots, n$. Then we can view

$$C_n = \{I, R, R^2, \dots R^{n-1}\} \subset S_n$$

where $I = id$ and

$$R = (123 \dots n)$$

A bit of thought shows that $R^n = I$. We won't need to multiply permutations explicitly, we just use this rule: $R^j R^k = R^{j+k}$ and if $j + k \geq n$, we "wrap around" to R^{j+k-n}. We will encounter other groups with a similar structure.

Definition 4.1. *A finite group G is called cyclic if there exists an element $g \in G$, called a generator, such that every element of G is a power of g.*

Cyclic groups are really the simplest kinds of groups. In particular:

Lemma 4.2. *A cyclic group is abelian.*

Proof. $g^j g^k = g^{j+k} = g^k g^j$. □

Let us give a second example. Let

$$\mathbb{Z}_n = \{0, 1, 2 \dots n-1\}$$

We modify addition using the same wrap around rule as before.

$$x \oplus y = \begin{cases} x + y & \text{if } x + y \in \mathbb{Z}_n \\ x + y - n & \text{otherwise} \end{cases}$$

This is usually called modular addition. It is not completely obvious that this is a group but we will show this later. Here is the table for $n = 2$

$\oplus$	0	1
0	0	1
1	1	0

This is the simplest nonzero abelian group. A somewhat more complicated case is $n = 4$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_n$ with this addition rule is also cyclic with generator 1.

We can see that $\mu_2 = \{1, -1\}$ is a cyclic group under multiplication. More generally, the group of nth roots of unity.

$$\mu_n = \left\{ e^{2\pi ik/n} = \cos\left(\frac{2\pi ik}{n}\right) + i\sin\left(\frac{2\pi ik}{n}\right) \mid k = 0, 1, \dots n-1 \right\}$$

This is a subgroup of the group of nonzero complex numbers $\mathbb{C}^*$ under multiplication. μ_n is generated by $e^{2\pi i/n}$, so it is cyclic.

Although these examples are superficially different, they are the same in some sense. If we associate $k \mapsto R^k$ or $k \mapsto e^{2\pi ik/n}$ and compare addition/multiplication tables, they will match. Here is the precise definition.

Definition 4.3. *If $(G, *, e)$ and $(H, \circ, e')$ are groups. A function $f : G \to H$ is called a homomorphism if $f(e) = e'$ and $f(g_1 * g_2) = f(g_1) \circ f(g_2)$. A one to one onto homomorphism is called an isomorphism. Two groups are isomorphic if there is a homomorphism from one to the other. In symbols, we write $G \cong H$.*

The function $f : \mathbb{Z}_n \to C_n$ defined by $f(k) = R^k$ is an isomorphism. The function $f : \mathbb{Z} \to \mu_n$ defined by $f(k) = e^{2\pi ik/n}$ is a homomorphism which is not an isomorphism because it is not one to one. The *order* of a finite group is the number of elements in it.

Theorem 4.4. *A cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Let G be the cyclic group in question with generator g. Since G is finite, the sequence g^n must repeat itself. That is $g^{n_1} = g^{n_2}$ for $n_1 > n_2$. Taking $n = n_1 - n_2 > 0$ implies that $g^n = e$. Let us assume that n is the smallest such number (this is called the order of g). We claim that $G = \{e, g, \dots, g^{n-1}\}$ and that all the elements as written are distinct. By distinctness we mean that if $m_1 > m_2$ lie in $\{0, 1, \dots n-1\}$ then $g^{m_1} \neq g^{m_2}$. If not then $g^{m_1 - m_2} = e$ would contradict the fact that n is the order of g.

So now the function $f(i) = g^i$ is easily seen to given an isomorphism from $\mathbb{Z}_n$ to G. $\square$

We need to come back and check that $\mathbb{Z}_n$ is actually a group. We make use of a result usually called the "division algorithm". Although it's not an algorithm in the technical sense, it is the basis of the algorithm for long division that one learns in school.

Theorem 4.5. *Let x be an integer and n positive integer, then there exists a unique pair of integers q, r satisfying*

$$x = qn + r,\ 0 \leq r < n$$

Proof. Let

$$R = \{x - q'n \mid, q' \in \mathbb{Z} \text{ and } q'n \leq x\}$$

Observe that $R \subseteq \mathbb{N}$, so we can choose a smallest element $r = x - qn \in R$. Suppose $r \geq n$. Then $x = qn + r = (q+1)n + (r-n)$ means that $r - n$ lies in R. This is a contradiction, therefore $r < n$.

Suppose that $x = q'n + r'$ with $r' < n$. Then $r' \in R$ so $r' \geq r$. Then $qn = q'n + (r' - r)$ implies that $n(q - q') = r' - r$. So $r' - r$ is divisible by n. On the other hand $0 \leq r' - r < n$. But 0 is the only integer in this range divisible by n is 0. Therefore $r = r'$ and $qn = q'n$ which implies $q = q'$.

□

We denote the number r given above by $x \, mod \, n$; *mod* is read "modulo" or simply "mod". When $x \geq 0$, this is just the remainder after long divison by n.

Lemma 4.6. *If x_1, x_2, n are integers with $n > 0$, then*

$$(x_1 + x_2) \, mod \, n = (x_1 \, mod \, n) \oplus (x_2 \, mod \, n)$$

Proof. Set $r_i = x_i \, mod \, n$. Then $x_i = q_i n + r_i$ for appropriate q_i. We have $x_1 + x_2 = (q_1 + q_2)n + (r_1 + r_2)$. We see that

$$(x_1 + x_2) \, mod \, n = \begin{cases} r_1 + r_2 = r_1 \oplus r_2 & \text{if } r_1 + r_2 < n \\ r_1 + r_2 - n = r_1 \oplus r_2 & \text{otherwise} \end{cases}$$

□

This would imply that $f(x) = x \, mod \, n$ gives a homomorphism from $\mathbb{Z} \to \mathbb{Z}_n$ if we already knew that $\mathbb{Z}_n$ were a group. Fortunately, this can be converted into a proof that it is one.

Lemma 4.7. *Suppose that $(G, *, e)$ is a group and $f : G \to H$ is an onto map to another set H with an operation $*$ such that $f(x * y) = f(x) * f(y)$. Then H is a group with identity $f(e)$.*

In the future, we usually just write + for modular addition.

The dihedral group D_n is the full symmetry group of regular n-gon which includes both rotations and flips. There are $2n$ elements in total consisting of n rotations and n flips. Label the vertices consecutively by $1, 2, 3 \ldots$. Let $R = (123 \ldots n)$ be the basic rotation. This generates a cyclic subgroup $C_n \subset D_n$. The reflection around the line through the midpoint of $\overline{1n}$ and opposite side or vertex is

$$F = (1\,n)(2\,n-1)(3\,n-2)\ldots$$

One can calculate that

$$\begin{aligned} FR &= \begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix} \\ &= (1\,n-1)(2\,n-2)\ldots \end{aligned}$$

is another flip, and furthermore that

$$\begin{aligned} FRF &= \begin{pmatrix} 1 & 2 & \ldots & n \\ n-1 & n-2 & \ldots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \ldots & n \\ n & 1 & \ldots & n-1 \end{pmatrix} \\ &= R^{-1} \end{aligned}$$

Here's the point. We will eventually see that the elements of D_n are given by $I, R, R^2 \ldots, F, FR, FR^2$. So we say that these elements generate the group. (In general, to say that a set elements generates a group, means that we have to take products in every possible way such as FR^2F^3.) We have three basic relations among the generators

$$F^2 = I,\ R^n = I,\ FRF = R^{-1}$$

Everything else about D_n follows from this. In particular, we won't have to multiply any more permutations. For instance, let us check that $(FR)^2 = I$ using only these relations

$$(FR)^2 = (FRF)R = R^{-1}R = I$$

4.8 Exercises

1. Determine all the generators of $\mathbb{Z}_6$ and $\mathbb{Z}_8$. Is there an obvious pattern?

2. Let $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ with an operation defined by $x \odot y = (x \cdot y)\ mod\, 7$. Assume that it is associative, and check that $\mathbb{Z}_7^*$ is a cyclic group.

3. Given a finite group G and $g \in G$, prove that $\{e, g, g^2, \ldots\}$ is a cyclic subgroup. This called the subgroup generated by G. The order of this group is called the *order of* g. Prove that the order is the smallest positive integer n such that $g^n = e$.

4. Given a function $f : H \to G$ such that $f(x * y) = f(x) * f(y)$, prove that f takes the identity to the identity and is therefore a homomorphism.

5. Complete the proof of lemma 4.7.

6. Let us say that an infinite group is cyclic if it isomorphic to $\mathbb{Z}$. Prove that the set of even integers is cyclic.

7. Let $G \subseteq \mathbb{Z}$ be nonzero subgroup. Let $d \in G$ be the smallest positive element. Prove that if $x \in G$, then $x = qn$ for some integer q. Conclude that G is cyclic.

8. Let $F, R \in D_n$ be as above.

   (a) For any $i > 0$, show that $FR^iF = R^{-i}$, where R^{-i} is the inverse of R^i.

   (b) Show that for any $i, j > 0$, $(FR^i)(FR^j)$ is a rotation.

   (c) Show every element of D_n is either R^i or FR^i with $i = 0, 1, \ldots, n$.

9. Assuming the previous exercise, show that $f : D_n \to \mathbb{Z}_2$ given by $f(R^i) = 0$ and $f(FR^i) = 1$ is a homomorphism.

10. Let $G \subset O(2)$ be the set of matrices

$$\left\{ \begin{bmatrix} \cos\theta & \pm\sin\theta \\ \sin\theta & \mp\cos\theta \end{bmatrix} \mid \theta = \frac{2\pi k}{n}, k = 0, 1, \ldots n-1 \right\}$$

Let

$$R = R\left(\frac{2\pi}{n}\right), F = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Check that G is generated by these two elements, and that they satisfy the same relations as the generators of the D_n. Use these facts to prove that D_n is isomorphic to G.