1 Groups

In Section 5.5 of the textbook, we learned about binary operations, and some of the properties that an operation on a set might have, such as associativity and commutativity. In these notes we will learn about sets which have a binary operation with three particular properties (associativity, an identity, and inverses). We call a set with such an operation a *group*. It turns out that groups occur in many situations in mathematics.

Definition 1.1
Let $*$ be a binary operation on a set A. An element e of A is an identity *element if $a * e = e * a = a$ for all $a \in A$.*

Example 1.2
The element 0 is an identity element for the operation $+$ on $\mathbb{R}$: for any $x \in \mathbb{R}$ we have $x + 0 = 0 + x = x$.

Exercise 1.3
Which of the binary operations in Example 5.5.2 of the textbook have an identity element?

Proposition 1.4
If $*$ has an identity element, it is unique.

Definition 1.5
Let $*$ be a binary operation on a set A with identity element e. Let $a \in A$. Then b is an inverse *of a if $a * b = b * a = e$.*

Example 1.6
The inverse of a real number x under the operation $+$ is the number $-x$: we have $x + (-x) = (-x) + x = 0$.

Definition 1.7
A group *is a pair $(G, *)$ where $*$ is a binary operation on G such that*

- *for any $a, b, c \in G$, $a * (b * c) = (a * b) * c$;*
- *there is some $e \in G$ such that, for every $a \in G$, $a * e = e * a = a$; and*
- *for any $a \in G$ there is some $b \in G$ with $a * b = b * a = e$.*

We often abuse notation and refer to "the group G" instead of "the group $(G, *)$".

Example 1.8
The integers form a group under addition, in other words $(\mathbb{Z}, +)$ is a group. The non-zero real numbers for a group under multiplication, in other words $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.

Proposition 1.9
The inverse of a is unique. In other words, if $a * b = b * a = e$ and $a * c = c * a = e$ then $b = c$.

Because of this uniqueness, we can denote the inverse of an element a by a^{-1}.

Proposition 1.10
If $(G, *)$ is a group and $a, b, c \in G$ with $a * b = a * c$ then $b = c$.

This is sometimes called the *cancellation law*.

1.1 Cayley tables

If $*$ is a binary operation on a finite set, we can write down a "multiplication table" for $*$. For example, we can define an operation $*$ on the set $G = \{e, a, b, c\}$ by the following table:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We call this the *Cayley table* of the operation.

Exercise 1.11
Show that if $*$ is defined by the above table then $(G, *)$ is a group.

Proposition 1.12
Each element of G occurs exactly once in each row and each column of the Cayley table of a group operation.

Proposition 1.13
Let $(G, *)$ be a group with identity element e.

1. *If $x \in G$ satisfies $x * x = x$, then $x = e$.*
2. *If $x, y \in G$ satisfy $x * y = y$, then $x = e$. [Put another way, if $x * y = y$ for* some *$y \in G$ then $x * y = y$ for* every *$y \in G$.]*

Exercise 1.14
Given that $\oplus$ is a group operation on the set $G = \{p, q, r, s\}$, complete the following Cayley table:

$\oplus$	p	q	r	s
p	r			
q		q		
r				
s				

1.2 Symmetry Groups

In this section we will discuss a very important class of groups, the *symmetry groups* of solid objects.

Definition 1.15
A symmetry *of a solid object is a way of moving it so that it ends up in the space it originally occupied. We are only interested in the final position of the object, not how it got there, so for example a clockwise rotation of* $90°$ *is the same as an anticlockwise rotation of* $270°$*.*

For example, consider the set of symmetries of a square. We can rotate it anticlockwise through $90°$, $180°$ or $270°$. We can also flip it over either horizontally or vertically, or along the main diagonal or the other diagonal. And, of course, we can simply put the square back where we found it. We denote these symmetries by R_{90}, R_{180}, R_{270}, H, V, D, D' and R_0 respectively. We can represent these in Figure 1: we imagine that the square is transparent and has the letter R on it.

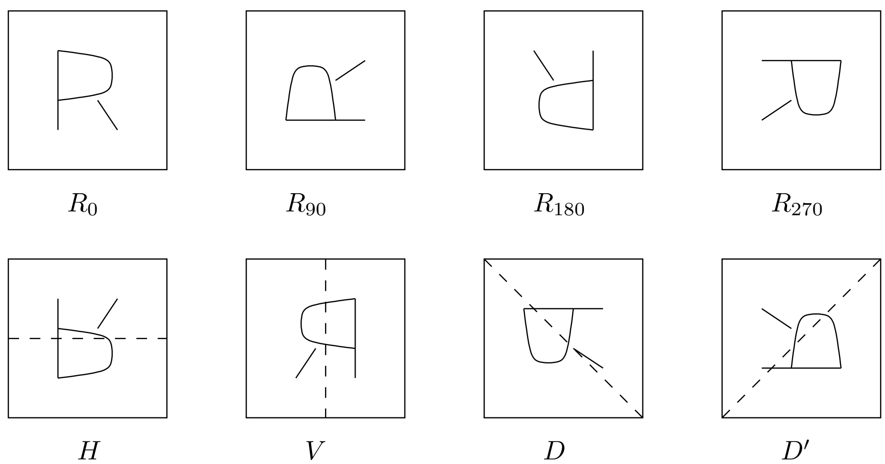

Figure 1: Symmetries of the square

To form a group, we need an operation. For symmetries A and B, we define $A * B$ to be the symmetry which has the same effect as A followed by B. For example, $R_{90} * R_{180} = R_{270}$. Less obviously, $R_{90} * H = D$. And we obviously have $R_0 * A = A = A * R_0$ for any A.

Exercise 1.16
Complete the Cayley table of $*$*.*

$*$	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}				D			
R_{180}	R_{180}							
R_{270}	R_{270}							
H	H							
V	V							
D	D							
D'	D'							

Proposition 1.17
The set of symmetries of the square forms a group under the operation $*$.

The hardest part of proving this would be to check associativity: there are $8^3 = 512$ ways of choosing A, B and C to check that $A * (B * C) = (A * B) * C$. The best bet is to realise that the symmetry A defines a function f_A from the points of the square to the points of the square, and then we have $f_{A*B} = f_B \circ f_A$. But then we have

$$f_{A*(B*C)} = (f_C \circ f_B) \circ f_A = f_C \circ (f_B \circ f_A) = f_{(A*B)*C}.$$

Since $f_{A*(B*C)} = f_{(A*B)*C}$, we have $A * (B * C) = (A * B) * C$, as required.

The symmetry group of the square is usually denoted D_4. More generally, the symmetries of a regular n-gon form a group with $2n$ elements, usually denoted D_n and called the *dihedral group of order* $2n$.

Another related class of groups is the class of *full summetric groups*. The group S_n is defined to be the set of all bijections (one-to-one correspondences) from $\{1, 2, \ldots, n\}$ to itself. Again, the group operation is "followed by", in other words $f * g = g \circ f$.[1]

Exercise 1.18
How many elements does S_n *have?*

We can represent the elements of S_n in matrix form, as follows. For our example, we will fix $n = 4$. We represent the element f by the 2×4 matrix which has $\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix}$ as its first row and $\begin{bmatrix} f(1) & f(2) & f(3) & f(4) \end{bmatrix}$ as its second row. For example the bijection which has $f(1) = 3$, $f(2) = 4$, $f(3) = 2$, $f(4) = 1$ is represented by the matrix $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$. We can then work out the composition of two elements. For example, we have

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}.$$

1.3 Commutativity and abelian groups

For any real numbers x and y we have $x + y = y + x$. Thus the group operation in $(\mathbb{R}, +)$ is a commutative operation. However, there is no need for every group operation to be commutative. For example, looking back at the symmetries of the square, we have that $R_{90} * H = D$, whereas $H * R_{90} = D'$.

Definition 1.19
A group $(G, *)$ *is* abelian *if* $*$ *is a commutative operation, and* non-abelian *otherwise.*

[1]Unfortunately there are two conflicting conventions for the notation of composition of functions. In analysis, calculus and topology it is usual to write functions as we do in this course, writing $f(x)$ for "the value of f evaluated at x". In algebra, it is more common to write xf instead. Using the first notation, it is more natural to define composition of functions by $(g \circ f)(x) = g(f(x))$, whereas with the second notation it is more natural to write $x(f * g) = (xf)g$. Some algebra books even use $\circ$ for "left-to-right" composition in this way, while others just write fg for the composition "f followed by g".

So $(\mathbb{R}, +)$ is an abelian group whereas D_4 is a non-abelian group.

Notice that even if G is a non-abelian group, there will be *some* elements x and y satisfying $x * y = y * x$. For example, this will be true if $x = y$, or if $x = e$ or $y = e$ (where e is the identity element).

Exercise 1.20
The elements of S_3 are $e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$, $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$, $\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$, $\gamma = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\varphi = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ *and* $\psi = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$. *Complete the Cayley table for S_3.*

$*$	e	α	β	γ	φ	ψ
e						
α						
β						
γ						
φ						
ψ						

Find elements x and y such that $x * y \neq y * x$.

Proposition 1.21
Let n be an integer with $n \geq 3$. Then S_n is non-abelian.

1.4 Isomorphisms and homomorphisms

We have already used the word "isomorphism" in Section 5.3 of the textbook, when we said that two partially ordered sets $(A, \leqslant)$ and $(B, \sqsubseteq)$ are *order-isomorphic* if there is a bijection $f : A \to B$ such that for every $x, y \in A$,

$$f(x) \sqsubseteq f(y) \text{ if and only if } x \leqslant y.$$

We can think of this as meaning that B is really just a "re-labelled" version of A, with exactly the same structure.

We can do the same thing for groups. In this case, the structure we have is not an order relation but a binary operation, but the idea—that the isomorphism should preserve the structure—is exactly the same.

Definition 1.22
Let $(G, *)$ and $(H, \diamond)$ be groups. An isomorphism *from G to H is a bijection $f : G \to H$ such that for all $x, y \in G$,*

$$f(x * y) = f(x) \diamond f(y).$$

if there is such a function, we say that G and H are isomorphic, *written $G \approx H$.*

Example 1.23
Let $U(10) = \{1, 3, 7, 9\}$. We define an operation $\diamond$ by declaring that, for $x, y \in U(10)$, $x \diamond y$ is $xy \bmod 10$ (in other words, the remainder you get when dividing xy by 10. Let $C_4 = \{0, 1, 2, 3\}$,

and define an operation $*$ on C_4 by declaring that $x * y = x + y \mod 4$. So we have the Cayley tables

$\diamond$	*1*	*3*	*7*	*9*
1	*1*	*3*	*7*	*9*
3	*3*	*9*	*1*	*7*
7	*7*	*1*	*9*	*3*
9	*9*	*7*	*3*	*1*

$*$	*0*	*1*	*2*	*3*
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

Then the function $f : U(10) \to C_4$ given by $f(0) = 1$, $f(1) = 3$, $f(2) = 9$, $f(3) = 7$ is an isomorphism.

Proposition 1.24
Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be an isomorphism. Then $f(e_G) = e_H$.

Proposition 1.25
Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be an isomorphism. Then, for every $x \in G$, we have

$$f(x) \diamond f(x) = e_H \text{ if and only if } x * y = e_G.$$

Exercise 1.26
Let G be the group given by the group table

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Show that G is not *isomorphic to C_4.*

1.5 Subgroups

Definition 1.27
A subgroup *of a group $(G, *)$ is a subset H of G such that $*$ is a group operation on H.*

Example 1.28
$\mathbb{Z}$ is a subgroup of the group $(\mathbb{R}, +)$.

Example 1.29
The set $H = \{R_0, R_{90}, R_{180}, R_{270}\}$ is a subgroup of D_4.

Proposition 1.30
A subset H of a group G is a subgroup of G if and only if

1. *$e \in H$ (where e is the identity element of G);*
2. *for any $x, y \in H$, $x * y \in H$; and*

3. for any $x \in H$, $x^{-1} \in H$.

Proposition 1.31
A subset H of a group G is a subgroup of G if and only if $H \neq \varnothing$ and, for every $x, y \in H$, $x * y^{-1} \in H$.

Our goal for this section will be to prove *Lagrange's Theorem*. This is the statement that if G is a finite group and H is a subgroup of G then the number of elements of G is a multiple of the number of elements of H.

To prove this, we will show that we can use the subgroup H to for a partition of G. The number of elements in each set in the partition will be the same as the number of elements in H. Thus the number of elements in G is equal to the number of elements in H times the number of sets in the partition. And that's all there is to it! Of course, we have to check the details.

Definition 1.32
Let H be a subgroup of a group G, and let $a \in G$. We define the left coset of H in G containing a, *written $a * H$, by*

$$a * H = \{\, a * h : h \in H \,\}.$$

Lemma 1.33
Let H be a subgroup of G and let $a, b \in G$. If $a * H \cap b * H \neq \varnothing$ then $a * H = b * H$.

Lemma 1.34
Let H be a subgroup of G. Put

$$\Omega = \{\, a * H \mid a \in G \,\}.$$

Then Ω is a partition of G.

Lemma 1.35
Let H be a subgroup of G and let $a \in G$. Then the function $f_a : H \to a * H$ defined by $f_a(h) = a * h$ is a bijection.

Theorem 1.36
Let G be a finite group and let H be a subgroup of G. Then $|G|$ is a multiple of $|H|$.