Monday: Symmetry Groups

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

Definition. *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.

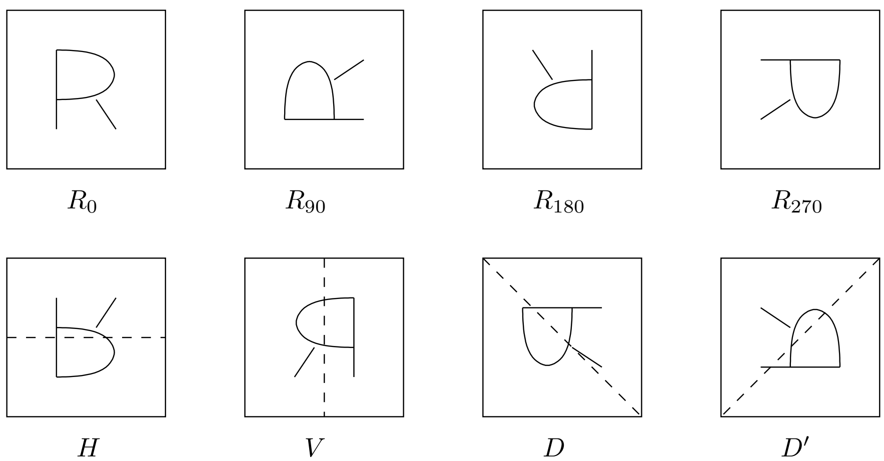

Figure 1: Symmetries of the square

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 B followed by A. 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. *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 2. *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 $A * (B * C) = (A * B) * C$. But the symmetries are functions, and the operation we have is function composition, and we know that composition of functions is an associative operation.

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* $2n$.

Tuesday: The full symmetric group S_n

Related to the symmetry groups we discussed last time are the *full symmetric groups*. The group S_n is defined to be the set of all bijections (one-to-one and onto functions) from $\{1, 2, \ldots, n\}$ to itself. Again, the group operation is "composed with", in other words $f * g = f \circ g$.

Exercise 3. *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

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

and

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

To answer the previous exercise, we can see that there are n ways to fill in the first entry in row 2, $n-1$ ways to fill in the next, $n-2$ for the next and so on, giving a total of $n!$ ways to write such a matrix. Thus $|S_n| = n!$.

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 group D_4 of symmetries of the square, we have that $R_{90} * H = D'$, whereas $H * R_{90} = D$.

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

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 still 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 4. *The elements of S_3 are $e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$, $\varphi = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ and $\psi = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$,*

$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\gamma = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. *Complete the Cayley table for* S_3.

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

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

Proposition 5. *Let* n *be an integer with* $n \geq 3$. *Then* S_n *is non-abelian.*

Cycles in S_n

Definition. *A* cycle *in* S_n *is an element of* S_n *such that there exist distinct* $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ *with* $f(i_j) = i_{j+1}$ *for* $1 \leq j < k$, $f(i_k) = i_1$ *and* $f(j) = j$ *for* $j \notin \{i_1, i_2, \ldots, i_k\}$. *We denote this cycle by* $(i_1\ i_2\ \ldots\ i_k)$.

For example, in S_8 we have

$$(1\ 3\ 4\ 6) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 1 & 7 & 8 \end{bmatrix}.$$

Exercise 6. *Write the elements* φ, ψ, α, β *and* γ *of* S_3 *in cycle form.*

Thursday: Isomorphisms and homomorphisms

We have already used the word "isomorphism" in Section 5.4 of the textbook, when we said that two partially ordered sets $(A, \preceq_A)$ and $(B, \preceq_B)$ are *order-isomorphic* if there is a bijection $f : A \to B$ such that for every $x, y \in A$,

$$f(x) \preceq_B f(y) \text{ if and only if } x \preceq_A y.$$

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. *Let* $(G, *)$ *and* $(H, \diamond)$ *be groups. A* homorphism *from* G *to* H *is a function* $f : G \to H$ *such that for all* $x, y \in G$,

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

An isomorphism *from* G *to* H *is a homomorphism from* G *to* H *which is also a bijection. If there is such an isomorphism, we say that* G *and* H *are* isomorphic, *written* $G \approx H$.

Example 7. *Let* $n \in \mathbb{N}$. *The function* $f : \mathbb{Z} \to \mathbb{Z}_n$ *given by* $f(x) = \overline{x}$ *is a homomorphism, since for every* $x, y \in \mathbb{Z}$ *we have* $\overline{x + y} = \overline{x} + \overline{y}$. *However, it is not an isomorphism because it is not 1–1: we have* $0 \neq n$ *but* $\overline{0} = \overline{n}$.

Example 8. *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 the remainder modulo 10 of $x \cdot y$. Let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, and define an operation $*$ on $\mathbb{Z}_4$ by declaring that $x * y = x +_4 y$. 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 $f : \mathbb{Z}_4 \to U(10)$ given by $f(0) = 1$, $f(1) = 3$, $f(2) = 9$, $f(3) = 7$ is an isomorphism.

Proposition 9. *Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be a homorphism. Then $f(e_G) = e_H$.*

Proposition 10. *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*

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

Exercise 11. *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 $\mathbb{Z}_4$.*

Friday: Subgroups

From now on we will use a convenient convention: we will omit the group operation symbol, just as when we are multiplying numbers we omit the $\cdot$. So for example we will write gh instead of $g * h$. We also write g^2 for gg, g^3 for ggg, g^{-3} for $(g^{-1})^3$ and so on.

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

Example 12. *$\mathbb{Z}$ is a subgroup of the group $(\mathbb{R}, +)$.*

Example 13. *The set $H = \{R_0, R_{90}, R_{180}, R_{270}\}$ is a subgroup of D_4.*

Proposition 14. *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 $x, y \in H$, $xy \in H$; and*
3. *for any $x \in H$, $x^{-1} \in H$.*

Proposition 15. *A subset H of a group G is a subgroup of G if and only if $H \neq \emptyset$ and, for every $x, y \in H$, $xy^{-1} \in H$.*

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 form 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. *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 aH, by*

$$aH = \{\, ah : h \in H \,\}.$$

Lemma 16. *Let H be a subgroup of G and let $a, b \in G$. If $aH \cap bH \neq \emptyset$ then $aH = bH$.*

Lemma 17. *Let H be a subgroup of G. Put*

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

Then Ω is a partition of G.

Lemma 18. *Let H be a subgroup of G and let $a \in G$. Then the function $f_a : H \to aH$ defined by $f_a(h) = ah$ is a bijection.*

Theorem 19. *Let G be a finite group and let H be a subgroup of G. Then $|G|$ is a multiple of $|H|$.*