8 Building a Library of Groups

In answering problems about groups it is often useful to know what different types of groups exist and to know their properties. In this section we look at the possible groups of small order that exist and at some of their features.

8.1 Cyclic Groups

We have already seen that the set of elements

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\} \text{ where } a^n = 1$$

forms a group for every value of n. We call this the *cyclic group of order n* and note that:

- cyclic groups are always abelian;
- a cyclic group of prime order will have no subgroups; if $n=mk$ then the element a^m will generate a subgroup consisting of k elements.

8.2 Direct Product of Cyclic Groups

If we have two cyclic groups C_n and C_m with elements $\{1, a, \ldots, a^{n-1}\}$ and $\{1, b, \ldots, b^{m-1}\}$ respectively we can always form the group

$$C_n \times C_m = \{a^i b^j : 0 \le i \le n-1, 0 \le j \le m-1\} \quad \text{where } a^n = b^m = 1, ab = ba.$$

We call this the *direct product* of C_n and C_m and note that:

- the group above has order mn.
- the group is abelian as ab = ba is one of our defining relations
- the group is cyclic if gcd(m,n) = 1 (it can be generated by the element ab); otherwise it is non-cyclic as there is no element of order mn in the group.

In a similar way we can define the direct product of more than two groups. For example

$$C_2 \times C_2 \times C_4 = \{a^i b^j c^k : 0 \le i \le 1, 0 \le j \le 1, 0 \le k \le 3\} \text{ where } a^2=b^2=c^4=1, ab=ba, ac=ca, bc=cb$$

is a group of order 16. In constructing groups of this type we must always ensure that each generating symbol commutes with every other generating symbol.

It can be shown, though we will not do so in this course, that every finite abelian group can be described as a direct product of cyclic groups. (For a proof see, for example J.B. Fraleigh 3rd Edition Chapter 20).

8.3 Dihedral Groups

Given the cyclic groups C_n and C_2 (n>2) we construct the group

$$D_n = \{a^i b^j : 0 \le i \le n-1, 0 \le j \le 1\} \text{ where } a^n = b^2 = 1, ba = a^{n-1}b$$

which we call the *dihedral group of order 2n.* We note that D_n is

- non-abelian as $ab \ne ba$;
- D_n is another way of looking at the symmetry group of a regular n-sided polygon with a corresponding to a clockwise rotation of $2\pi/n$ and b corresponding to a reflection of the polygon in one of its axes of symmetry.

8.4 Quaternion/Dicyclic Groups

If we take the definition of dihedral groups given above and modify it slightly we obtain another class of 2-generator groups. Instead of obtaining a group of this type whenever the order is even (as we do for dihedral groups), this time we note that we have a dicyclic group whenever the order is 4k (k>1). The group is defined as

$$Q_{2k} = \{a^i b^j : 0 \le i \le 2k-1, 0 \le j \le 1\} \text{ where } a^{2k} = 1, b^2 = a^k, ba = a^{2k-1}b\}$$

Dicyclic groups are:

- non-abelian as $ab \ne ba$;

8.5 Symmetric Groups

We have already seen that sets of permutations can be used to construct a group. If we use all permutations of length n we obtain what we call the *symmetric group on n elements* which we write as S_n. Since there are n! permutations of length n this allows us to construct symmetric groups of order

$$2! = 2, 3! = 6, 4! = 24, 5! = 120 \text{ etc.}$$

We will not normally consider the group of permutations on 2 elements as this is really just another way of looking at the cyclic group of order 2. S_3 has the following elements:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

We note that in general:

- S_n is non-abelian (n>2) as in general multiplication of permutations is non-commutative.

8.6 Alternating Groups

These are special subgroups of the symmetric group and we define them by noting the following:

- every permutation may be expressed as the product of *transpositions* (a transposition is a permutation that swaps two elements over and leaves the rest unaltered). For example

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

  and so we can express it as the product of two transpositions.

- a permutation is said to be either *odd* or *even* depending on whether it can be represented as the product of odd or even numbers of transpositions.

(Note: This description is unique - while there may be many different ways of expressing a permutation as the product of transpositions they will either all be odd or will all be even. By convention we note that the identity permutation where everything is unchanged is even as it can be written as the product of zero transpositions and zero is an even number).

- if we have two even permutations σ_1 and σ_2 then their product will also be an even permutation since if σ_1 can be expressed as the product of 2s transpositions while σ_2 can be expressed as the product of 2t transpositions it follows that $\sigma_1\sigma_2$ can be expressed as the product of 2(s+t) transpositions.

Since we have a finite group and a subset of elements closed under the group operation we note that the set of even permutations forms a subgroup of S_n. We call this the *Alternating Group on n elements* which we write as A_n. A_n contains exactly half the elements of S_n and this class of groups has been very important in the history of mathematics.

[Historical note:

The concept of a group was first used by the French mathematician Evariste Galois in the early 19th century. He was interested in the problem of finding roots of the polynomial equation

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0.$$

We all know that if n=2 we can solve the equation by using the formula for roots of a quadratic equation. Building on this approach mathematicians of the 16th and 17th century had quickly discovered methods that could find roots of polynomials of degree 3 and degree 4 but were unable to deal with $n \geq 5$. Galois managed to show that no method or formula was possible; his approach was to rewrite the problem in terms of a question about subgroups of permutations and to demonstrate that the group A_5

was very different in terms of the structure of its subgroups from A_4, A_3, A_2 and that this difference meant that no solution was possible.

Unfortunately this brilliant piece of mathematics was not immediately appreciated; Galois was very poor at expressing his ideas and was, in any case, as interested in politics as he was in mathematics. After his death in a duel at an early age his mathematical papers were not properly examined and only many years after his death were the importance of his results and the elegant use of group theory that enabled them to be proved fully appreciated.]

The categories described above re the main ways of constructing finite groups and every group of order less than 16 falls into one of these categories. Once the order reaches 16 things become more complicated - there are 14 different groups of order 16.

In the table on the following pages we attempt to summarise the structure of the groups of small order.

Order	Name of Group	Elements	Defining Relations	Abelian?	Other Forms/Comments
1	Trivial	{1}	None	✓	
2	C_2	{1, a}	$a^2 = 1$	✓	Also S_2
3	C_3	{1, a, a^2 }	$a^3 =1$	✓	Also A_3
4	C_4	{1, a, a^2, a^3}	$a^4 = 1$	✓	
	K_4	{1, a, b, ab}	$a^2 = b^2 = 1$	✓	$C_2 \times C_2$
5	C_5	{1, a, a^2, a^3, a^4}	$a^5 = 1$	✓	
6	C_6	{1, a, a^2, a^3, a^4, a^5}	$a^6 = 1$	✓	$C_3 \times C_2$ - in this form elements are {1, a, a^2, b, ab, a^2b} with $a^3 = b^2 = 1$, ab = ba
	D_3	{1, a, a^2, b, ab, a^2b}	$a^3 = b^2 = 1$, ba = a^2b	×	Same group as S_3; also has form {1, a, b, ab, ba, aba} with $a^2=b^2=1$, aba = bab. Symmetry group of the equilateral triangle. Smallest non-abelian group.
7	C_7	{1, a, a^2, a^3, a^4, a^5, a^6}	$a^7 = 1$	✓	
8	C_8	{1, a, a^2, a^3, a^4, a^5, a^6, a^7}	$a^8 = 1$	✓	
	$C_4 \times C_2$	{1, a, a^2,a^3, b, ab, a^2b, a^3b}	$a^4 = b^2 = 1$, ab = ba	✓	
	$C_2 \times C_2 \times C_2$	{1, a, b, c, ab, ac, bc, abc}	$a^2=b^2=c^2=1$, ab=ba, ac=ca, bc=cb	✓	
	D_4	{1, a, a^2,a^3, b, ab, a^2b, a^3b}	$a^4 = b^2 = 1$, ba = a^3b	×	Symmetry group of the square.
	Q = Q_4	{1, a, a^2,a^3, b, ab, a^2b, a^3b}	$a^4 = 1$, $b^2 = a^2$, ba = a^3b	×	Called the Quaternion group. Other forms include: {1,i,j,k,-1,-i,-j,-k} where $i^2=j^2=k^2=-1$, ij= k=-ji, jk= i=-kj, ki=j=-ik
9	C_9	{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8}	$a^9 = 1$	✓	
	$C_3 \times C_3$	{1, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2}	$a^3=b^3=1$, ab = ba	✓	
10	C_{10}	{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9}	$a^{10} = 1$	✓	$C_5 \times C_2$
	D_5	{1, a, a^2,a^3, a^4, b, ab, a^2b, a^3b, a^4b}	$a^5 = b^2 =1$, ba = a^4b	×	Symmetry group of the regular pentagon
11	C_{11}	{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}}	$a^{11} = 1$	✓	

12	C_{12}	$\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}$	$a^{12} = 1$	✓	$C_4 \times C_3$
	D_6	$\{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$	$a^6 = b^2 = 1, ba = a^5b$	×	Symmetry group of the regular hexagon
	Q_6	$\{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$	$a^6 = 1, b^2 = a^3, ba = a^5b$	×	
	A_4	$\{1, a, b, b^2, ab, ba, ab^2, aba, bab, abab, b^2ab, bab^2\}$	$a^2=1, b^3=1, (ab)^3=1.$	×	Here a and b represent permutations; a is any pair of disjoint transpositions while b rotates three elements and leaves the fourth fixed.
	$C_6 \times C_2$	$\{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$	$a^6 = b^2 = 1, ab = ba$	✓	