Chapter 2. Group Theory Background

This chapter presents the background necessary for understanding the algorithms for small groups. This is very elementary group theory but our emphasis is slightly different from most group theory texts. The examples we discuss will be permutation groups, because the reader will need to be familiar with permutation groups for later chapters, and because we see no advantage in introducing other descriptions of groups at this stage. The concepts to be discussed are group, generators, permutation, subgroup, and coset.

Groups

A *group* is a non-empty set G (of elements) with a multiplication operator × with the properties that

(1) G is closed under $\times$ (that is, for all $g,\ h \in G, g \times h \in G$),
(2) $\times$ is associative (that is, for all $g,\ h,\ k \in G$, $(g \times h) \times k = g \times (h \times k)$),
(3) G has an identity *id* (that is, for all $g \in G, g \times id = id \times g = g$),and
(4) every element g of G has an inverse g^{-1} such that $g \times g^{-1} = g^{-1} \times g = id$.

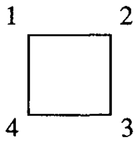
The *order* of the group G is the number of elements in the set G. It is denoted by $|G|$. We will only be concerned with *finite* groups. In this case, for each element g there is always a smallest positive integer m such that

$$g^m = \underbrace{g \times g \times \cdots \times g}_{m \text{ times}} = id$$

The integer m is called the *order* of the element g. It is denoted by $|g|$. Note that $g^{-1} = g^{|g|-1}$.

Our first example is the symmetries of a square in Figure 1a. The rotations and reflections of a square form a group with eight elements. The multiplication operation composes the transformations from left to right. We list the elements in Figure 1b.

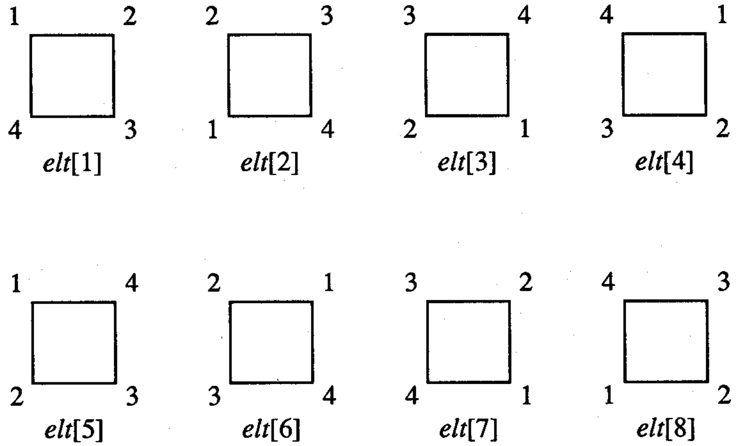
Figure 1a: A square



Note that *elt*[1] is *id*, and that the order of *elt*[2] is four. The first four elements are the rotations about the centre, while the fifth to eighth elements are the reflections of the first four about the leading diagonal.

Let S be a subset of a finite group G. The set S *generates* G if every element of G can be written as a product

Figure 1b : Symmetries of the Square



elt[1] *elt*[2] *elt*[3] *elt*[4]

elt[5] *elt*[6] *elt*[7] *elt*[8]

$$g = s_{i_1} \times s_{i_2} \times \cdots \times s_{i_m}$$

of elements in S, for some m dependent on g. We call S a *set of generators* for G and denote this by $G = < S >$.

Let G be the symmetries of the square. Then G is generated by $\{elt\,[2], elt\,[5]\}$ since

elt [1] = *id*, is the empty product,
elt [2] = *elt* [2],
elt [3] = *elt* [2] × *elt* [2],
elt [4] = *elt* [2] × *elt* [2] × *elt* [2],
elt [5] = *elt* [5],
elt [6] = *elt* [2] × *elt* [5],
elt [7] = *elt* [2] × *elt* [2] × *elt* [5], and
elt [8] = *elt* [2] × *elt* [2] × *elt* [2] × *elt* [5].

We could also write $G = < elt\,[2], elt\,[5] >$.

Permutations

A permutation is a bijection from a set to itself. For example, we can specify a bijection of the set {1,2,3,4} by listing the image of each member of the set, viz

1 2 3 4
2 3 1 4

A shorter notation is to omit the top line, viz

/2 3 1 4/

This is called the *image form* of the permutation.

The elements of the group of symmetries of the square as permutations of {1,2,3,4} are now listed in image form.

/1 2 3 4/	/4 1 2 3/	/3 4 1 2/	/2 3 4 1/
elt[1]	*elt*[2]	*elt*[3]	*elt*[4]
/1 4 3 2/	/2 1 4 3/	/3 2 1 4/	/4 3 2 1/
elt[5]	*elt*[6]	*elt*[7]	*elt*[8]

A *cycle* of a permutation is a sequence of set members

$$i_1, i_2, \cdots i_c$$

where

i_2 is the image of i_1,
i_3 is the image of i_2,
.
.
.
i_c is the image of i_{c-1}, and
i_1 is the image of i_c.

For example, 1, 2, 3 is a cycle of the permutation

$$/ 2\ 3\ 1\ 4 /.$$

A permutation may be specified by listing its cycles, viz

$$(1, 2, 3)(4)$$

Usually the cycles of length one are omitted, viz

$$(1, 2, 3)$$

This is called the *cycle form* of the permutation.

Multiplication of permutations is from left to right. First take the image under the left permutation, and then take the image of this under the right permutation. For example, if $g = /$ $2\ 3\ 1\ 4\ /$ and $h = /\ 2\ 1\ 4\ 3\ /$ then $g \times h = /\ 1\ 4\ 2\ 3\ /$, as shown in Figure 2.

Figure 2 : Multiplying Permutations

$$\begin{tikzcd} \begin{matrix}1\\2\\3\\4\end{matrix} \arrow[r, "g"] & \begin{matrix}2\\3\\1\\4\end{matrix} \arrow[r, "h"] & \begin{matrix}1\\4\\2\\3\end{matrix} \end{tikzcd}$$

Our second example is the set of all permutations of {1,2,3,4}. This set is a group called the symmetric group of degree 4, (because the set {1,2,3,4} has size 4). There are 24 such permutations, so the order of the group is 24.

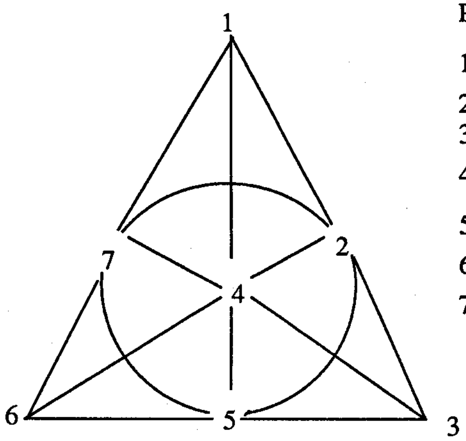
Our third example is the set of symmetries of the projective plane of order two. Consider a three-dimensional vector space over GF(2), the field of two elements {0,1}. The transformations which preserve the structure of a vector space are the linear transformations which map linearly independent vectors to linearly independent vectors. These are usually represented by *matrices*, in this case 3×3 matrices with entries from GF(2). There are 168 such invertible matrices, which form a group generated by

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

There is also a well-known geometry (Figure 3) associated with this vector space. The *projective plane* of order two is a set of seven points, together with seven lines, such that each line intersects in precisely one point, and each pair of points lie on a unique line. We can take the points to be the nonzero vectors, and the lines to be the two-dimensional subspaces. The 168 linear transformations preserve the geometry, in the sense that they map lines to lines. Regarded as permutations of the seven points, the group generators are

$$a=(1,2)\,(3,5) \quad b=(2,4,3)\,(5,7,6)$$

Figure 3 : Projective Plane of Order Two



POINTS	LINES
1. (1,0,0)	{1,2,3}
2. (0,1,0)	{1,4,5}
3. (1,1,0)	{1,6,7}
4. (0,0,1)	{2,4,6}
5. (1,0,1)	{2,5,7}
6. (0,1,1)	{3,4,7}
7. (1,1,1)	{3,5,6}

Every element in the group can be expressed as a product

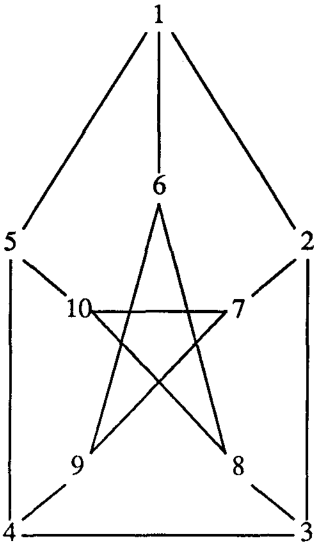
$$a^{i_1} \times b^{j_1} \times a^{i_2} \times b^{j_2} \times \cdots \times a^{i_m} \times b^{j_m}$$

for suitable non-negative values of the integers m, i_1, i_2,... i_m, j_1, j_2, $\cdots$ j_m.

Our fourth example is the group of automorphisms of Petersen's graph, shown in Figure 4. The automorphisms are the permutations of {1,2,...,10} that permute the edges {1,2} {1,5} {1,6} {2,3} {2,7} {3,4} {3,8} {4,5} {4,9} {5,10} {6,8} {6,9} {7,9} {7,10} {8,10} amongst themselves. The group has order 120 and is generated by / 1 2 3 8 6 5 7 4 10 9 /, / 1 5 4 3 2 6 10 9 8 7 /, and / 3 4 5 1 2 8 9 10 6 7 /.

Our fifth example is the set of all operations of Rubik's cube. These may be viewed as permutations of the starting configuration where we number the squares which are not in the centre of a face. The quarter turns of each face generate the group, so, with suitable numbering of the 48 noncentral squares, the generators are

Figure 4 : Petersen's Graph



(1,3,8,6)(2,5,7,4)(9,48,15,12)(10,47,16,13)(11,46,17,14);
(6,15,35,26)(7,22,34,19)(8,30,33,11)(12,14,29,27)(13,21,28,20);
(1,12,33,41)(4,20,36,44)(6,27,38,46)(9,11,26,24)(10,19,25,18);
(1,24,40,17)(2,18,39,23)(3,9,38,32)(41,43,48,46)(42,45,47,44);
(3,43,35,14)(5,45,37,21)(8,48,40,29)(15,17,32,30)(16,23,31,22); and
(24,27,30,43)(25,28,31,42)(26,29,32,41)(33,35,40,38)(34,37,39,36).

The group has order

$$2^{27}3^{14}5^{3}7^{2}11$$
$$= 43\ 252\ 003\ 274\ 489\ 856\ 000.$$

This group is *not* small. It can, however, be handled by the algorithms for large permutation groups.

Subgroups and Cosets

A *subgroup* of a group G is a subset of G that is itself a group with the same multiplication operator as G. For example, the rotations of the square are a subgroup of order four of the symmetries of the square, and the symmetries of the projective plane of order two that leave the point 1 fixed form a subgroup of order 24 of the group of all symmetries of the plane.

Given a subgroup H of a group G and an element g of G, the *(right) coset* $H \times g$ is the set of elements $\{ h \times g \mid h \in H \}$. We can easily prove that if $\overline{g} \in H \times g$ then $H \times \overline{g} = H \times g$. This means that two cosets of H in G are either disjoint or the same. Thus the cosets of H partition the elements of G. Furthermore, all the cosets of H have size $|H|$. The number of cosets is called the *index* of H in G and is denoted by $|G:H|$. This gives

Lagrange's Theorem

If H is a subgroup of a finite group G then $|G| = |H| \times |G:H|$.

If we choose precisely one element from each coset of H, we get *a set of coset representatives* $\{g_1, g_2, \ldots, g_m\}$. Each coset $H \times g_i$ is disjoint from the others, so the elements of G (without repetition) are

$$\left[H \times g_1\right] \cup \left[H \times g_2\right] \cup \cdots \cup \left[H \times g_m\right]$$

If g is an element of G then there is a unique coset representative g_i and a unique element h of H such that

$$g = h \times g_i$$

Consider the example where G is the symmetries of the square, and H is the rotations of the square. Then the two cosets of H are $\{$ *elt*[1], *elt*[2], *elt*[3], *elt*[4] $\}$ = H = $H \times id$, and $\{$ *elt*[5], *elt*[6], *elt*[7], *elt*[8] $\}$ = $H \times$ *elt*[5]. A set of coset representatives is { elt[1], elt[5] } and the reader can verify that each element is uniquely expressible as a product of an element of H and a coset representative.

Conjugates and Normal Subgroups

A *conjugate* under G of an element h is an element of the form $g \times h \times g^{-1}$, for some element g of G. A conjugate under G of a subset H is a set of the form $g \times H \times g^{-1} = \{ g \times h \times g^{-1} \mid h \in H \}$, for some element g of G. The conjugate of a subgroup is again a subgroup. If S generates H then $g \times S \times g^{-1}$ generates $g \times H \times g^{-1}$.

For example, in the symmetric group of degree 4, let h=(1,2) and g=(1,3)(2,4). Then (3,4)=$g \times h \times g^{-1}$ is a conjugate of h. Let H={ (1,2), (3,4) }. Then $g \times H \times g^{-1} = H$. Let $H = <(1,2), (3,4)>$. Then $g \times H \times g^{-1} = H$ while $(2,4) \times H \times (2,4)^{-1} = <(1,4), (2,3)>$.

An element g in G *normalizes* a subgroup H if the conjugate $g \times H \times g^{-1}$ is H. The set of all such elements is a subgroup, $N_G(H)$, called the *normalizer* of H in G.

For example, g=(1,3,2,4) normalizes $H = <(1,2), (3,4)>$ in the symmetric group of degree 4. Indeed, $N_G(H) = <H, g>$.

A subgroup H whose normalizer in G is the whole group G is said to be a *normal* subgroup of G. Therefore all conjugates of a normal subgroup H are H itself. An alternative, but equivalent, definition of a normal subgroup is that

$$H \times g = g \times H, \text{ for } all\ g \in G.$$

The coset representatives of a normal subgroup can be chosen to have a special form. If $G = <H, s_1, s_2, \ldots, s_m>$ then the coset representatives can be chosen from $<s_1, s_2 \ldots, s_m>$. If $m = 1$, then the coset representatives are

$$id,\ s_1,\ s_1^2,\ \ldots,\ s_1^{n-1},$$

where s_1^n is the first power of s_1 that lies in H.

For example, the subgroup $H = < (1,2)\,(3,4)\,,\ (1,3)\,(2,4) >$ is normal in the symmetric group of degree 4. The group is generated by H together with s_1=(1,2,3) and s_2=(1,2). The coset representatives may be taken to be

$$id,\ s_1,\ s_1^2,\ s_2,\ s_1 \times s_2,\ s_1^2 \times s_2.$$

The group $< H,\ s_1 >$ is also normal in the group. Its coset representatives may be taken to be

$$id,\ s_2$$

since $s_2^2 = id \in\ < H,\ g >$. If instead we had s_2=(1,2,3,4) then the coset representatives may be taken to be

$$id,\ s_2$$

since $s_2^2 = (1,3)\,(2,4) \in\ < H,\ g >$.

The cosets of a normal subgroup H in G form a group called the *factor group* or *quotient group* G/H. The inverse of a coset $H \times g$ is $H \times g^{-1}$, while the product of two cosets $H \times g_1$ and $H \times g_2$ is the coset $H \times (g_1 \times g_2)$. The inverse and product are independent of the choice of coset representative, because the subgroup H is normal.

Commuting Elements

Two elements g and h *commute* if $g \times h = h \times g$. For example, in these circumstances, we also say that g *centralizes* h, since $g \times h = h \times g$ implies that $g \times h \times g^{-1} = h$. The set of all elements that centralize h is a subgroup, $C_G(h)$, called the *centralizer* of h in G.

In the symmetric group of degree 4, the element (1,2) centralizes the element (3,4). The centralizer of (1,2) is just < (1,2), (3,4) >.

Exercises

(1/Easy) If H is a subgroup of G and g, g' are elements of G, then show that $(\ H \times g\ ) \times g'$ is a coset of H with coset representative $g \times g'$.

Bibliographical Remarks

There are many excellent texts on group theory and permutation groups. Two introductory texts are C.D.H. Cooper, **Permutations and Groups**, John Murray, London, 1975 and W. Ledermann, **Introduction to Group Theory**, Oliver-Boyd, Edinburgh, 1973. The standard reference is H. Wielandt, **Finite Permutation Groups**, Academic Press, New York, 1964.

A standard reference on group theory is M. Hall, Jr, **The Theory of Groups**, Macmillan, New York, 1959. An advanced text is I. D. Macdonald, **The Theory of Groups**, Oxford University Press, Oxford, 1968.