MAT2104: INTRODUCTION TO GROUP THEORY
Vers 2.1

Josef Lauri ©
Department of Mathematics
University of Malta

Contents

1 Group Actions

Let X be a set (usually finite with $|X| = n$). The *symmetric group* is the group consisting of all permutations on X, and it is denoted by S_X. If $|X| = n$ then $|S_X| = n!$. Let G be a group. An *action* of G on X is a homomorphism from G to S_X.

If $\phi : G \to S_X$ is an action, then $\phi(g)$ is often denoted by $\widehat{g}$, and $\phi(G)$ by $\widehat{G}$. Note that $\widehat{G} \leq S_X$, each $\widehat{g}$ is a bijection (permutation) on X and, since ϕ is a homomorphism,

$$\widehat{gh} = \widehat{g} \circ \widehat{h}.$$

If ϕ is injective then we say that the action is $faithful$.

Examples

1. Let $G = \{a, a^2, a^3, a^4 = 1\}$ be the cyclic group of order 4. Let $X = \{1, 2, 3, 4\}$ be the set of four vertices of a square (numbered in an anticlockwise sense). Define the following action of G on X: $a^i \mapsto \mathsf{rot}_{\pi i/2}$, where $\mathsf{rot}_{\pi i/2}$ denotes the permutation of the vertices induced by an anticlockwise rotation of the square through an angle of $\pi i/2$. Therefore,

$$a \mapsto (1234) \qquad (= \widehat{a})$$

$$a^2 \mapsto (13)(24) \qquad (= \widehat{a^2})$$

$$a^3 \mapsto (1432) \qquad (= \widehat{a^3})$$

$$1 \mapsto \mathsf{id} \qquad (= \widehat{1}).$$

One should check (it is easy) that this does in fact define an action, that is, ϕ is a homomorphism, meaning that $\phi(a^i)\phi(a^j) = \phi(a^i a^j)$. Notice how this homomorphism is bringing out the similarity between the algebraic significance of "cyclic" in "cyclic group" and the geometric significance of the "cyclic" rotations carried out on the square.

2. The group G is as above, but now $X = \{x, y\}$ where x and y are the two diagonals of the square. The action is now defined by mapping a^i onto the permutation induced on the *diagonals* by a rotation of the square through $\pi i/2$. Therefore in this case, $\widehat{a} = (xy)$, $\widehat{a^2} = \mathsf{id}$, $\widehat{a^3} = (xy)$ and $\widehat{a^4} = \widehat{1} = \mathsf{id}$.

Note that in the first example the action is faithful but in the second it is not. When the action is faithful, G and $\widehat{G}$ (that is, $\phi(G)$) are isomorphic. Therefore G would be isomorphic to a subgroup ($\widehat{G}$) of S_X. In this case we often do not distinguish between G and $\widehat{G}$ and we say that G is a subgroup of S_X, and we denote $\widehat{g}$ by g. Conversely, if G is a subgroup of S_X, that is, G is a group of permutations of the set X, then trivially there is an action of G on X — just take $\phi : G \to S_X$ to be the identity. In fact, our definition of "action" is meant to extend precisely this clear case of an action on X, that is when the group consists of permutations of X.

3. Let $G = \{1, a, a^{-1}, a^2, a^{-2}, \dots\}$ be the infinite cyclic group, and let $X = \mathbb{R}$, the real line. For any real number i, let tr_i be a shift or translation of $\mathbb{R}$ through i; that is, tr_i is a function on $\mathbb{R}$ defined by $\mathsf{tr}_i(x) = x + i$. Clearly, each tr_i is a

bijection on $\mathbb{R}$. Define an action of G on $\mathbb{R}$ by $a^i \mapsto \mathsf{tr}_i$. Check that this is, in fact, an action (that is, $\widehat{a^i} \circ \widehat{a^j} = \widehat{a^i a^j}$) and that it is faithful.

4. Let G and X be as in the previous example. Let rf_i denote reflection of $\mathbb{R}$ through the origin i times, in other words, rf_i is a function on $\mathbb{R}$ defined by $\mathsf{rf}_i(x) = (-1)^i x$. The action is now defined by $a^i \mapsto \mathsf{rf}_i$. This therefore boils down to the following: if i is even then a^i is mapped onto the identity transformation on $\mathbb{R}$, while if i is odd then a^i is mapped onto the function on $\mathbb{R}$ defined by $x \mapsto -x$. Again, check that this defines an action. Clearly it is not faithful.

5. Cayley's Theorem

Let G be any group, and let $X = G$, that is, we are going to create an action of G on itself. For any $g \in G$ define the function $f_g : G \to G$ by $f_g(x) = gx$ (this will be called *left translation*). Then the proof of Cayley's Theorem consists in the following steps:

(i) Show that f_g is a bijection on G, that is, $f_g \in S_G$. This shows that the function ϕ defined by $\phi(g) = f_g$ is a function from G to S_G;
(ii) Show that ϕ is a homomorphism, that is, $\phi(g)\phi(h) = \phi(gh)$, that is, $f_g \circ f_h = f_{gh}$ — therefore (i) and (ii) give that ϕ is an action of G on G;
(iii) Show that ϕ is injective, that is, the action is faithful;
(iv) Conclude that G is isomorphic to $\phi(G)$, that is, to a subgroup of S_G.

Exercise. Complete all the details of the proof of Cayley's Theorem.

2 The Orbit-Stabiliser Theorem

Consider an action of the group G on a set X. Let $x \in X$. The *orbit* of x, denoted by $G(x)$ is the set defined by

$$\{y \in X : y = \widehat{g}(x) \text{ for some } g \in G\}.$$

Note that this is a subset of X.

Exercise: Define a relation on X by: $x \sim y$ iff there is some $g \in G$ such that $y = \widehat{g}(x)$. Show that $\sim$ is an equivalence relation and that the equivalence classes are precisely the orbits of the action of G on X. Therefore the orbits form a partition of X, that is, any two distinct orbits have no element in common, and each element of X lies in exactly one orbit.

The *stabiliser* of x, denoted by G_x, is defined to be the set

$$\{g \in G : \widehat{g}(x) = x\}.$$

Note that this is a subset of G. Our first lemma in fact says more.

Lemma 1. $G_x \leq G$.

Proof. Let $g, h \in G_x$. Then $\widehat{g}(x) = \widehat{h}(x) = x$. Since $\widehat{gh} = \widehat{g}\widehat{h}$, $\widehat{gh}(x) = \widehat{g}(\widehat{h}(x)) = x$. Therefore $gh \in G_x$ (closure).

Also, since $\widehat{g}(x) = x$ then $\widehat{g}^{-1}(x) = x$. But $\widehat{g}^{-1} = \widehat{g^{-1}}$ since $g :\mapsto \widehat{g}$ is a homomorphism (an action), therefore $\widehat{g^{-1}}(x) = x$, that is, $g^{-1} \in G_x$.

Therefore $G_x \leq G$, as required. □

Lemma 2. *Let $y \in G(x)$ and $g, h \in G$ such that $\widehat{g}(x) = \widehat{h}(x) = y$. Then the left cosets gG_x and hG_x are equal.*

Proof. Let $z \in gG_x$, that is, $z = gk$ for some $k \in G_x$; therefore $z = hh^{-1}gk = h(h^{-1}gk)$. But $\widehat{h^{-1}gk} = \widehat{h}^{-1}\widehat{g}\widehat{k}$ and $\widehat{h}^{-1}\widehat{g}\widehat{k}(x) = x$, therefore $h^{-1}gk \in G_x$. Hence, $z \in hG_x$, that is, $gG_x \subseteq hG_x$.

Similarly, $hG_x \subseteq gG_x$. □

Theorem 1. The Orbit-Stabiliser Theorem *Let G be a finite group acting on a finite set X, and let $x \in X$. Then*

$$|G_x|.|G(x)| = |G|.$$

Proof. We shall prove that $|G(x)| = |G|/|G_x| = [G : G_x]$, the index of G_x in G, that is, the number of cosets of G_x in G.

Define the function f from $G(x)$ into the set of left cosets of G_x as follows: Let $y \in G(x)$ and let $y = \widehat{g}(x)$ for some $g \in G$ (such a $\widehat{g}$ must exist since $y \in G(x)$). Then let $f(y) = gG_x$. All we have to do is to show that f is a bijection.

Note first the very important point that f is *well-defined by virtue of Lemma 2* — that is, any choice of g would give the same coset gG_x, provided $y = \widehat{g}(x)$.

Surjectivity follows practically from the definitions. Consider any gG_x. Let $y = \widehat{g}(x) \in G(x)$. Then clearly $f(y) = gG_x$.

Now for injectivity. Let $f(y) = f(z)$. Therefore $gG_x = hG_x$, where $\widehat{g}(x) = y$ and $\widehat{h}(x) = z$. Then $g \in gG_x = hG_x$, therefore $g = hk, k \in G_x$. Hence $\widehat{g} = \widehat{hk}$, therefore $y = \widehat{g}(x) = \widehat{hk}(x) = \widehat{h}(\widehat{k}(x)) = \widehat{h}(x) = z$. □

Example. Find the order of the group G of symmetries of a regular tetrahedron.

Solution. Consider the action of the group on the vertices of the tetrahedron. Clearly all the four vertices are in the same orbit because, given any two vertices, there is some symmetry of the tetrahedron which moves one into the other. Therefore, if x is any vertex, $|G(x)|$=4. Now consider G_x, the stabiliser of x. Fixing a vertex allows three symmetries of the tetrahedron (do not forget to count the identity). Therefore $|G_x| = 3$. Hence, $|G| = |G(x)|.|G_x| = 12$.

The next sections will contain deeper applications of the Orbit-Stabiliser Theorem.

Problems.

1. Let $G = GL(2, \mathbb{R})$, that is the group of all invertible 2×2 real matrices, and let G act on the points of $\mathbb{R}^2$ by matrix multiplication. Consider the action of G on the straight lines in $\mathbb{R}^2$ through the origin. If L is the line $y = 2x$, that is, $L = \{(x, 2x) : x \in \mathbb{R}^2\}$, find $G(L)$ and G_L.

Now let H be the subgroup of G consisting of all matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

and all matrices of the form

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix},$$

where a, b equal 1 or -1. (Therefore H contains 8 matrices.) Find $H(L)$ and H_L.

***2.** Let $X = \{1, 2, \ldots, 7\}$ and let G be the following group of permutations of elements of X:

$$G = \{\text{id}, (1234)(56), (13)(24), (1432)(56)\}.$$

First of all check that G is in fact a group (closure)—it is in fact isomorphic to the cyclic group of order 4. Then find G_1, G_5, G_7, $G(1)$, $G(5)$ and $G(7)$.

***3.** Let G be a group of order 55 acting on a set X of order 18. Show that this action must have at least two fixed points. (A fixed point of the action is an element of X which is left fixed by any $\widehat{g}$, in other words, it is an element whose orbit consists only of itself.)

***4.** Suppose G is an abelian subgroup of S_X, and suppose that the action of G on X has only one orbit (that is, all of X). Show that $|G| = |X|$.

3 Cauchy's Theorem

In this section we shall see how a simple but powerful use of group actions can give us a quick proof of a very important and nontrivial result.

Cauchy's Theorem. *Let G be a finite group and let p be a prime number such that $p||G|$. Then G contains an element of order p, that is, G contains an element $a \neq 1$ such that $a^p = 1$.*

Proof. Let X be the set of all sequences $a_1, a_2, \ldots, a_p$ of elements of G (not necessarily distinct) such that

$$a_1 a_2 \ldots a_p = 1.$$

We would like to show that there is such a sequence all of whose terms are equal (and not equal to 1)—because in this case if all the terms are equal, say, to $a \neq 1$, then we conclude that $a^p = 1$, as required. We shall show the existence of such a sequence by defining an appropriate group action on X.

But first let us determine $|X|$. Each of the first $p-1$ terms of any sequence in X can be chosen in $|G|$ different ways, that is, any element of G can be chosen. But then, having determined the first $p-1$ terms, the pth term can only be

$$(a_1 a_2 \ldots a_{p-1})^{-1}.$$

Therefore $|X| = |G|^{p-1}$. Hence (and this is the important conclusion for what follows)

$$p \text{ divides } |X|.$$

We will define an action of $\mathbb{Z}_p$ (the group of integers under addition modulo p, that is, the cyclic group of order p) as follows. Given $m \in \mathbb{Z}_p$, let $\widehat{m}$ be defined by the transformation

$$\widehat{m} : (a_1, a_2, \ldots, a_p) \mapsto (a_{m+1}, \ldots, a_p, a_1, \ldots, a_m)$$

that is, the element m in the cyclic group $\mathbb{Z}_p$ is mapped onto the cyclic shift (to the left) of the sequence through m steps.

It is an easy exercise to check that this is an action, that is, $\widehat{m+n} = \widehat{m} \circ \widehat{n}$ (remember that addition is modulo p). Now, by the orbit stabiliser theorem, the size of any orbit must divide the size of the acting group $\mathbb{Z}_p$, that is, the size of any orbit must be either 1 or p. Let there be s orbits of size 1 and t orbits of size p. Note that there surely exists one orbit of size 1, namely that consisting of the sequence all of whose terms are equal to the identity of G. Let us, for the moment, call this the trivial orbit.

Since the orbits form a partition of X, we have,

$$s + p.t = |X|.$$

But we have seen that p divides $|X|$ therefore s must also be a multiple of p. By the last observation in the previous paragraph, s must be at least 1. Therefore s must be at least p. Hence, apart from the trivial orbit, there are at least $p-1$ other orbits of size 1. Now consider such a nontrivial orbit. Its single element is a sequence $(a_1, a_2, \ldots, a_p)$ which remains unchanged under any cyclic shift. Therefore all the terms of the sequence must be equal, say equal to a. Therefore $a^p = 1, a \neq 1$, as required. □

Remark. Note that we have in fact proved that there are at least $p-1$ elements a satisfying $a^p = 1, a \neq 1$.

The above proof has introduced us to the very important idea of fixed points of an action. More precisely, let the group G act on the set X. Then $x \in X$ is said to be a *fixed point* in this action if, for every $g \in G$, $\widehat{g}(x) = x$. In other words, x is a fixed point iff it is the only element in its orbit, that is, its orbit has size 1. We shall have more to say about fixed points in what follows. (See also Problem 3 of Section 2.)

Exercise. Without using Cauchy's Theorem, prove the following special case: If G is a group of even order, then it contains an element $a \neq 1$ such that $a^2 = 1$. [Hint: Removing the identity from G leaves an odd number of elements. Now pair off inverses, that is, pair off the elements of $G - \{1\}$ as $\{x, x^{-1}\}$. Since an odd number of elements are being paired, some element must be its own inverse.]

4 Conjugacy

The single most important instance of a group acting on itself is the action of conjugacy. Let G be a group and let the set X on which G will be acting be

also G. For any $g \in G$ let $\widehat{g}$ be the mapping on G defined by

$$\widehat{g}(x) = gxg^{-1}.$$

We first have to show that this does define an action. First of all, any $\widehat{g}$ is injective since, if $\widehat{g}(x) = \widehat{g}(y)$ then $gxg^{-1} = gyg^{-1}$ and therefore $x = y$ by cancellation. Also, $\widehat{g}$ is surjective since, given $y \in G$, the element $x = g^{-1}yg$ is in G and clearly $\widehat{g}(x) = y$. Therefore $\widehat{g}$ is a permutation of G. Lastly, we must show that $\phi : g \mapsto \widehat{g}$ is a homomorphism. But $\widehat{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = \widehat{g}(\widehat{h}(x))$, that is, $\widehat{gh} = \widehat{g}\widehat{h}$, and hence ϕ is a homomorphism.

The action we have just defined is called *conjugacy*. Conjugacy is so important that some special terminology has been developed in this case. For example, $\widehat{g}(x)$ is often denoted by x^g. If two elements $x, y \in G$ are in the same orbit under conjugacy, then we say that x and y are *conjugate* elements—therefore $x, y \in G$ are conjugate iff there is some element $g \in G$ such that $y = gxg^{-1}$. Conjugacy is therefore an equivalence relation and the orbits of the action—or, the equivalence classes of the relation—are called *conjugacy classes*.

Notice that conjugacy is, in general, *not* a faithful action (that is, ϕ is not injective, that is, different elements $g, h \in G$ could correspond the same permutation of G, that is $\widehat{g}$ and $\widehat{h}$ could be the same permutation even though $g \neq h$). For example, if G is an abelian group, then $\widehat{g}(x) = gxg^{-1} = gg^{-1}x = x$, and therefore every $\widehat{g}$ is the identity permutation. This is the extreme situation, and it tells us that conjugacy is not interesting for abelian groups. In fact the sequel will show us that conjugacy is, in some sense, a measure of how nonabelian the group is.

Which are the fixed points of this action? An element $x \in G$ is a fixed point iff, for all $g \in G$, $\widehat{g}(x) = x$. Hence, $gxg^{-1} = x$, that is, $gx = xg$. Therefore x is a fixed point iff it commutes with all the elements of G. The set of all fixed points is called the *centre* of G, and it is denoted by $Z(G)$. That is,

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}.$$

Keep in mind that the centre consists of all those elements of G which commute with every other element.

What about the stabiliser of $x \in G$? An element $g \in G$ is in the stabiliser G_x iff $\widehat{g}(x) = x$, that is, $gxg^{-1} = x$, that is, $gx = xg$. The stabiliser of x is therefore the set of all those elements in G which commute with x. This set is given a special name, the *centraliser* of x, and it is denoted by $C(x)$. We therefore have

$$C(x) = \{g \in G : gx = xg\}.$$

Exercises.

In the following exercises, $\widehat{g}$ always denotes the permutation $\widehat{g} : x \mapsto gxg^{-1}$.

1. Let x and y be conjugates. Then the order of x is equal to the order of y.

2. If $g \in Z(G)$ then $\widehat{g}$ is the identity permutation.

3. For any $x \in G$, $C(x) \leq G$; $C(x) = G$ iff $x \in Z(G)$.
The centre $Z(G)$ is a normal subgroup of G—in fact, if H is a subgroup of G contained in $Z(G)$ then H is a normal subgroup of G.
For any $x \in G$, $C(x)$ contains $Z(G)$.

4. Let $N \trianglelefteq G$. Then N is equal to the union of conjugacy classes of G.

5. The mapping $\widehat{g}$ is more than just a permutation (bijection) of G—it is also a homomorphism, that is, $\widehat{g}$ is an *automorphism* (bijective homomorphism) of G. Later on we shall study automorphisms and we shall then look more closely at the role of $\widehat{g}$ as an automorphism of G.

All we have said above about conjugacy holds for infinite groups — we did not need, nor did we assume, that G is finite. But now suppose $|G|$ is finite. Remember that the conjugacy classes partition G. Also, by the Orbit-Stabiliser Theorem, the size of each conjugacy class divides $|G|$. This situation is similar to the case of the cosets of a subgroup of G. But, unlike the situation with cosets, the sizes of the conjugacy classes are, in general, not all equal. How many classes have size 1? We have seen above that the answer is $|Z(G)|$. Suppose that there are c other conjugacy classes (that is, of size greater than 1), and let their sizes be $n_1, n_2, \ldots, n_c$. As we have said, each n_i divides $|G|$. Note that we are not assuming anything regarding whether or not some (or all) of the n_i are equal. Also, if G is abelian, that is, $G = Z(G)$, then there are no conjugacy classes apart from those of size 1, and therefore all these n_i would be zero. Remember, however, that $|Z(G)| \geq 1$ because the centre certainly contains the identity element.

Now, since the conjugacy classes partition G, adding all their sizes gives $|G|$, that is,

$$|G| = |Z(G)| + n_1 + n_2 + \cdots + n_c.$$

This very important equation is called the *class equation*. This equation can be written in another way. By the Orbit-Stabiliser Theorem, the size of the orbit of $x \in G$ is equal to $|G|/|C(x)|$. Therefore, summing the sizes of all the orbits gives the class equation in the form

$$|G| = \sum_x \frac{|G|}{|C(x)|} = |Z(G)| + \sum_y \frac{|G|}{|C(y)|}$$

where the first summation runs over one element from each conjugacy class whereas the second summation runs over one element from each conjugacy class whose size is ≥ 2.

Applications to p-groups.

Let p be prime. A finite group $|G|$ is said to be a *p-group* if $|G| = p^r, r \geq 1$.

Exercise. Show that G is a p-group iff the order of any element of G is a power of p.

Theorem 1. *Let G be a p-group. Then $|Z(G)| \geq p$, and therefore the centre of G contains at least one other element apart from the identity.*

Proof. By the class equation,

$$p^r = |Z(G)| + n_1 + \cdots + n_c$$

where (unless each n_i equals zero) every $n_i > 1$ and each divides $|G|$. Therefore p divides each of the n_i and so it divides $|Z(G)|$. But since $|Z(G)| \neq 0$, it follows that $|Z(G)| \geq p$. □

Theorem 2. *Let $|G| = p^2$, p prime. Then G is abelian.*

Proof. We have to prove that $Z(G) = G$. By Theorem 1, $|Z(G)| > 1$, therefore by Lagrange's Theorem, $|Z(G)|$ must equal p or p^2. If $|Z(G)| = p^2$ then we are done.

So suppose that $|Z(G)| = p$ and let $x \in G$, $x \notin Z(G)$. Consider the centraliser $C(x)$ of x. Now recall that $Z(G) \leq C(x) \leq G$ (see Exercise 3 above). Since x is in $C(x)$ but x is not in $Z(G)$, $Z(G) \neq C(x)$. Therefore $p < |C(x)| \leq p^2$, and by Lagrange's Theorem $C(x)$ must equal G. That is, every element of G commutes with x, that is $x \in Z(G)$, which is a contradiction. □

Problems.

***1.** Let G be a group of order p^2, p prime. Prove that either G is cyclic or else it is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. [*Hint:* Suppose G contains no element of order p^2. Let $x \in Z(G), x \neq 1$ and let $y \notin < x >, y \neq 1$. Show that $G \simeq < x > \times < y >$.]

***2.** Let p be an odd prime and let G be a group of order $2p$. Prove that G is either cyclic or dihedral. [*Hint:* Let $x \in G$ have order p, and let $y \in G$ have order 2. Then $< x >$ and its right coset $< x > y$ fills out the whole group; note that $< x >$ is a normal subgroup of G (Why?). Show that the order of xy equals 2 or $2p$ (that is, cannot be p). Therefore either G is cyclic or $yx^{-1} = x^{-1}y$.] Deduce that a nonabelian group of order $2p$ must be isomorphic to D_p.

***3.** Prove that if $G/Z(G)$ is cyclic then G is abelian. Deduce Theorem 2.

***4.** Find the conjugacy classes of the dihedral groups D_5 and D_6. Repeat for D_n in general.

5 A Useful lemma

In the previous section we have seen the importance which fixed points of an action can have in certain situations. The technique used in Theorem 1 for showing that there are fixed points will be very useful when we come to proving Sylow's Theorems, so we here single it out for attention. (Remember that if a, b, c are integers then $a = b \bmod c$ means that $a = b + kc$ for some integer k.

Lemma 1. *Let G be a p-group acting on a set X. Let X_1 be the set of fixed points of this action. Then*

$$|X_1| = |X| \ mod\ p.$$

Proof. Let there be a_i orbits of size $i > 1$ (the number of orbits of size 1 is $|X_1|$). Of course, the only possible values of i are factors of $|G|$ (for any other $i > 1$, a_i would be zero), that is, powers of p. Since the orbits form a partition of X,

$$|X| = |X_1| + \sum i.a_i.$$

Therefore $|X_1| = |X| \bmod p$, as required. □

Exercises.

1. Suppose a 5-group acts on a set of size 14. What are the possibilities for the number of fixed points of the action.

2. Suppose that the order of a group G acting on a set X is pq, both p and q prime, and suppose that there are no positive integers a, b, c such that $|X| = ap + bq + cpq$. Show that the action must have at least one fixed point.

Look back at Problem 3 from the first set of problems.

6 Strong form of Cayley's Theorem

Let G be a group and H a subgroup of G. Let X be the set of all left cosets of H in G. Then there is a natural action of G on X defined by

$$\widehat{g} : xH \mapsto gxH.$$

This does indeed define an action. First of all, $\widehat{g}$ is injective since, if $\widehat{g}(xH) = \widehat{g}(yH)$ then $gxH = gyH$, therefore $(gx)^{-1}gy \in H$, therefore $x^{-1}y \in H$, hence $xH = yH$. Also, $\widehat{g}$ is surjective since, if $xH \in X$, then $g^{-1}xH$ is also in X and $\widehat{g}(g^{-1}xH) = xH$. Finally, $g \mapsto \widehat{g}$ is a homomorphism since $\widehat{gh}(xH) = ghxH = \widehat{g}(hxH) = \widehat{g} \circ \widehat{h}(xH)$.

The action we have just defined is a generalisation of that used in the proof of Cayley's Theorem. In fact, if we let $H = \{1\}$, then the cosets would be singleton sets, and the above action reduces to left translation of the elements of G. The advantage with this new action is that now, instead of a homomorphism to S_G, which contains $|G|!$ elements, we have a homomorphism into S_X which has $|X|! = (|G|/|H|)!$ elements.

However, this action now need not be faithful. Therefore we can naturally ask what the kernel of this homomorphism is. (Remember, the homomorphism is the function $\phi : g \mapsto \widehat{g}$. Therefore the kernel is the set of elements g of G such that $\widehat{g}$ is the identity permutation, that is $\widehat{g}(xH) = xH$.) Let K be the kernel. Therefore

$$K = \{g \in G : gxH = xH \text{ for all } x \in G\}.$$

Remember that K is a normal subgroup of G. We now claim that $K \subseteq H$. For suppose $g \in K$. Therefore $\widehat{g}(H) = H$, that is, $gH = H$, and so $g \in H$. Also, K is the largest normal subgroup of G which is contained in H in the sense that if $N \trianglelefteq G, N \subseteq H$, then $N \subseteq K$. For let N be a normal subgroup of G contained in H. Let $n \in N$. Then, for any $x \in G$, $x^{-1}nx \in N \subseteq H$, therefore

$x^{-1}nxH = H$, therefore $nxH = xH$, that is, $\widehat{n}(xH) = xH$. Therefore $\widehat{n}$ is the identity permutation on the cosets of H, that is $n \in K$, hence $N \subseteq H$.

We have therefore proved the following theorem.

Strong Form of Cayley's Theorem. *Let G be a group, $H \leq G$ and X the set of left cosets of H in G. Then there is an action of G on X (left translation on cosets) such that the kernel of the action is the largest normal subgroup of G which is contained in H.* □

Any group G has trivially two normal subgroups, G itself and $\{1\}$. If these are the only normal subgroups of G then G is called *simple*. Note that if G is simple and H is a proper subgroup of G, then the action in the above theorem must be faithful (trivial kernel), and therefore G would be isomorphic to a subgroup of S_X, quite an improvement on Cayley's Theorem.

Example.
Let G be a group of order 36, and let H be a subgroup of G of order 9. Then H must contain a nontrivial normal subgroup of G.
Solution. The number of left cosets of H is $\frac{36}{9} = 4$, that is, $|X| = 4$. But $|G| = 36 > 4! = |S_X|$. Therefore the above action, since it is a function from G to S_X, cannot be injective, and so it has a nontrivial kernel which is contained in H.

The technique in the above example can be generalised as follows.

Corollary 1. *Let G be a finite group, $H \leq G, H \neq G$, and let $m = [G : H]$. Suppose $|G|$ does not divide $m!$. Then H must contain a nontrivial normal subgroup of G. In particular, G cannot be simple.*

Proof. If the action ϕ in the above theorem were faithful, then $|\phi(G)| = |G|$. But $\phi(G) \leq S_X$, and $|S_X| = m!$, giving that $|G|$ divides $m!$. Therefore the action cannot be injective, and so it has a nontrivial kernel which is a normal subgroup of G contained in H. □

Problem. * Let G be a group of order 28. Show that it contains a normal subgroup of order 7. Deduce that if G also contains a normal subgroup of order 4 then G must be abelian.

7 Burnside's Counting Lemma

In this section we shall take some time off from applying the theory of group actions to group theory itself, and we shall instead concentrate on an application of groups actions to certain enumeration problems which have a more combinatorial flavour. The work in this section will be extended in the Combinatorics Elective Course where we shall be treating Pólya's Theorem.

Suppose that we are given a wire made out in the form of a square and that a bead is attached to each corner of the square. Suppose also that each of the beads can be given any one of two colours, black or white. In home many different ways can the beads be coloured?

The answer depends, of course, on what we mean by "different". If, for example, the square is fixed to a wall, then, since there are four beads and each can be given any of two colours, then the total number of colourings possible would

be equal to $2^4 = 16$. However, if we are free to move the square around (without distorting its shape), then many of these colourings would be *equivalent*, that is, one can be transformed into the other by a movement of the square. In this case, how many non-equivalent colourings of the square are there, if all movements which are symmetries of the square are allowed? It is easy to verify that out of all the sixteen original colourings, only six are non-equivalent. (Check this!)

Clearly, this problem is intimately connected with the group of symmetries of the square, which is the dihedral group D_4. In fact, if we are not allowed to "flip over" the square, that is, if only a cyclic subgroup of D_4 were allowed as the group of symmetries, then the number of non-equivalent colourings would be different. (How many would there be in this case?)

How can we obtain a general way of solving this type of problem (enumerating configurations which are in some sense non-equivalent under the action of some group) in a way which will enable us to solve larger or more general problems than this simple one which can be solved by hand? For example, if we had c colours instead of two, what would have been the number of non-equivalent colourings of the square? And what would have been the solution if, instead of a square, we had, say, n beads equally spaced along a circular wire?

To be able to solve these and similar problems we have to translate it into the language of group actions. The group of symmetries acting on the vertices of the square induces in a natural way an action on the sixteen possible colourings of the square. Those colourings which happen to lie in the same orbit under this action are, in fact, equivalent in the sense described above. They are, so to speak, indistinguishable from each other. So, in order to exhibit a set of non-equivalent colourings we need to take *one* representative from each orbit. In other words, the number of non-equivalent colourings of the square is equal to the number of orbits into which the sixteen colourings are partitioned by the group action in question. (Verify this, that is, partition the sixteen colourings of the square into the orbits resulting from the induced action of D_4.)

In other words, the enumeration problem we are discussing here boils down to this question. *Suppose a group G is acting on a finite set X. Into how many orbits is X partitioned by this action?* Note that while the Orbit-Stabiliser Theorem gives us information about the *size* of an orbit, the question here asks how many orbits there are.

Before giving the theorem which answers our question we need one definition and two very simple lemmas. Suppose G acts on a finite set X, let $g \in G$ and let $\widehat{g}$ be the corresponding permutation of X. The $F(g)$ denotes the set of fixed points of $\widehat{g}$, that is, $F(g) = \{x \in X : \widehat{g}(x) = x\}$.

Lemma 1. *Let G act on a finite set X and suppose $x, y \in X$ are in the same orbit. Then $|G_x| = |G_y|$.*

Proof. This is obvious by the Orbit-Stabiliser Theorem, since $|G_x| = |G|/|G(x)| = |G|/G(y) = |G_y|$. □

Lemma 2. *Let G act on a finite set X, and let $x, y \in X$. Then*

$$\sum_{y \in G(y)} |G_y| = |G|.$$

Proof. Let $G(x) = \{y_1, y_2, \ldots, y_r\}$. The the summation equals

$$\begin{aligned} & |G_{y_1}| + \ldots + |G_{y_r}| \\ = \; & |G_x| + \ldots + |G_x| \\ = \; & |G(x)| \cdot |G_x| \\ = \; & |G| \end{aligned}$$

by the Orbit-Stabiliser Theorem. □

Burnside's Counting Lemma.[1] *Let the finite group G act on the finite set X. The the number of orbits in which X is partitioned by this action is given by*

$$\frac{1}{|G|} \sum_{g \in G} |F(g)|.$$

Proof. We shall use a very powerful and frequent combinatorial trick. We shall define a set of ordered pairs, and we shall count the number of elements of the set in two ways. Thus, let $E = \{(g, x) : g \in G, x \in X, g(x) = x\}$. For a given $g \in G$, the number of elements (g, x) in E is equal to $|F(g)|$. Therefore the size of E is given by

$$|E| = \sum_{g \in G} |F(g)|.$$

Now, for a given $x \in X$, the total number of elements (g, x) in E is equal to $|G_x|$. Therefore

$$|E| = \sum_{x \in X} |G_x|.$$

But let t be the number of orbits into which X is partitioned, and let they be $G(x_1), \ldots, G(x_t)$. Counting the contribution given to the above summation by the elements x of $G(x_1)$ gives, by Lemma 2, $|G|$. This is the same for all the other orbits, therefore the above summation is equal to $t \cdot |G|$. Equating the the values of $|E|$ gives that

$$t \cdot |G| = \sum_{g \in G} |F(g)|,$$

which is the required result. □

Exercises.

1. Necklaces are manufactured by arranging thirteen white beads and three black beads on a loop of string. How many necklaces can be produced this way?

***2.** Find the number of distinct bracelets of five beads made up of green, blue and red beads, assuming that (i) the bracelet cannot be flipped over; (ii) it can be flipped over.

[1] It is now well-known that this result is due to Cauchy and Frobenius, but it is still often quoted as Burnside's Theorem.

***3.** Find the number of distinct necklaces which can be made from six beads using any of the three colours red, green or blue if (i) flipping over of the neclace is allowed; (ii) flipping over is not allowed.

***4.** It is straightforward to calculate directly the number of distinct strings of length 3 made up of blue and red beads. Verify Burnside's Lemma in this case.

***5.** *Fermat's Little Theorem.* A necklace is to be made from p beads, with p prime, and where each bead can be given any one of m different colours. How many distinct necklaces are there if flipping over is not allowed? Deduce that

$$m^p \equiv m \mod p$$

and hence that, if p does not divide m, then

$$m^{p-1} \equiv 1 \mod p.$$

6. Show that when $n_1 + n_2$ is an odd prime the number of necklaces which can be made with n_1 black and n_2 white beads is

$$\frac{1}{2(n_1+n_2)}\binom{n_1+n_2}{n_1} + \frac{1}{2}\binom{\frac{1}{2}(n_1+n_2-1)}{\lfloor \frac{1}{2}n_1 \rfloor}.$$

***7.** Identity cards are to be made as follows. An $n \times n$ grid of equally spaced lines is drawn on both sides of a plastic square. Then, two circular holes are punched into the square, one hole in each of two of the n^2 cells of the grid. How many distinct cards can be made this way? What would the answer be if, instead of punching holes, two cells are "blacked out" on one side only of the square?

***8.** By considering the symmetries of the cube, show that there are 30 possible different dice.

8 Sylow's Theorems

We now return to proving the main theorems of this course. These theorems, partial converses of Lagrange's Theorem, are the central theorems in group theory and they are landmarks of mathematical beauty. The proofs presented here, using the machinery of group actions, are due to Wielandt.

We first require a number-theoretic/combinatorial lemma. Recall the basic fact that if a prime p divides a product $abc\ldots$ then it must divide at least one of $a, b, c, \ldots$ and, in fact, any factor p of the product must arise from factors of the respective terms; that is, if p^k divides $abc\ldots$, and if p divides a e_a times, it divides b e_b times, etc, then $e_a + e_b + \ldots$ must be at least k.

Lemma 1. *Let p, m be positive integers, p prime, such that p does not divide m. Then p does not divide $\binom{p^k m}{p^k}$.*

Proof. Note first that

$$\binom{p^k m}{p^k} = \frac{m(p^k m-1)\dots(p^k m-i)\dots(p^k m-p^k+1)}{1\cdot 2\cdot\dots\cdot i\cdot\dots\cdot(p^k-1)}.$$

By the previous comments, any factor p of the numerator arises from a factor of $mp^k - i$ and similarly any factor p of the denominator arises from a factor of i. We shall now show that these factors cancel out.

Consider the rational number $(p^k m - i)/i, 1 \leq i < p^k$. Suppose first that p^j divides i. Then $j < k$ and therefore p^j divides $p^k m - i$. Now suppose that p^j divides $p^k m - i$, that is, $p^k m - i = qp^j$ for some integer q. Note first that $j < k$, otherwise $i = p^k m - qp^j = p^k(m - qp^{j-k})$ which is impossible since $i < p^k$. Therefore $i = p^j(p^{k-j}m - q)$, that is, p^j divides j.

Therefore, pairing off all terms $p^k m - i$ from the numerator with corresponding terms i from the denominator for $1 \leq i < p^k$, all powers of p cancel out. The remaining term m is not a multiple of p, therefore p does not divide the binomial coefficient. □

Sylow Theorem 1. *Let G be a group of order $p^k m$, with p prime and such that p does not divide m. Then G contains a subgroup of order p^k.*

Proof. Let X be the set of all p^k-subsets of G (that is, subsets of size p^k). Therefore $|X| = \binom{p^k m}{p^k}$, and so p does not divide $|X|$. Define an action of G on X by left translation, that is, for any $g \in G, B \in X$, $\widehat{g}(B) = gB = \{gb : b \in B\}$. (One can easily check that this is, in fact an action, that is, $\widehat{g}$ is a bijection on X and $\widehat{gh} = \widehat{g}\widehat{h}$.)

Since p does not divide $|X|$ there is some orbit whose size is not a multiple of p. Let the set B be in this orbit, that is, p does not divide $|G(B)|$. Consider the stabiliser G_B of B (that is, the set of all those elements $g \in G$ such that, for any $b \in B$, $gb \in B$); remember that $G_B \leq G$.

Now, $|G_B| = |G|/|G(B)| = p^k m/|G(B)|$. But p does not divide $|G(B)|$ therefore $|G_B| = p^k m'$ with m' a factor of m. Therefore $|G_B| \geq p^k$.

Now let b be some element of B and consider the coset $G_B b$. Since G_B is the stabiliser of B, $G_B b \subseteq B$. Therefore $|G_B b| = |G_B| \leq |B| = p^k$. Hence $|G_B| = p^k$, and this is therefore a subgroup of G of order p^k. □

Exercises.

1. Show that the $\widehat{g}$ in the above proof do define an action on X.

2. Using Theorem 1 of Appendix 4 prove the following immediate corollary of Sylow's first theorem: If p^k divides $|G|$, p prime, then, for any $0 \leq i \leq k$, G contains a subgroup of order p^i.

We now proceed with the presentation of Sylow's theorems. The first theorem suggests the following definition. If G is a finite group and k is the highest power of the prime p which divides $|G|$ then any subgroup of G of order p^k is called a *Sylow p-subgroup* of G. The number of Sylow p-subgroups of G will be denoted by n_p.

We recall the following elementary facts about normal subgroups. You should be able to prove them without any difficulty and we collect them here in one place because they will be used very often.

1. Let $H \leq G$ and $g \in G$. Then $gHg^{-1} = \{ghg^{-1} : \forall h \in H\} \leq G$ and, if H is finite, then $|H| = |gHg^{-1}|$.

2. If $H \leq G$, $|H| = m$ and H is the only subgroup of G of order m then $H \trianglelefteq G$. If H has index 2 in G then $H \trianglelefteq G$.

3. If $H, K \leq G$ and $H = gKg^{-1}$ for some $g \in G$ then H and K are said to be *conjugates*. Conjugacy is an equivalence relation on the subgroups of G.

4. A subgroup H of G is normal in G iff it is its only conjugate.

Sylow Theorem 2. *Let G be as in Sylow Theorem 1. Any two Sylow p-subgroups of G are conjugate.*

Proof. Let H, K be two Sylow p-subgroups of G. Let X be the set of left cosets of H in G, and let K act on X by left translation, that is, for $k \in K$, $\widehat{k} : xH \mapsto kxH$. Since $|X| = p^k m/p^k = m$ is relatively prime to p and since K is a p-group, by our Useful Lemma there is some x_0H in X which is fixed by the action, that is, $kx_0H = x_0H$ for all $k \in K$. Therefore ${x_0}^{-1}kx_0 \in H$ for all $k \in K$ [we are using the fact that if $aH = bH$ then $b^{-1}a \in H$]. Therefore ${x_0}^{-1}Kx_0 \subseteq H$. But $|{x_0}^{-1}Kx_0| = |K| = |H|$, therefore ${x_0}^{-1}Kx_0 = H$, that is, H and K are conjugates. □

Exercise. A SYLOW p-SUBGROUP OF G IS NORMAL IN G IFF IT IS THE ONLY SYLOW p-SUBGROUP OF G.

Sylow Theorem 3. *Let G be as in Sylow Theorem 1. The number n_p of Sylow p-subgroups of G is congruent to 1 mod p and is a factor of m.*

Proof. Let $t = n_p$ and let $X = \{H_1, \ldots, H_t\}$ be the set of all distinct Sylow p-subgroups of G. Let H_1 act on X by conjugation, that is, for $h \in H$, $\widehat{h} : H_i \mapsto hHh^{-1}$. [Exercise: How do we know that hHh^{-1} is still in X?] We claim that H_1 is the only fixed point under this action.

First of all, note that H_1 is fixed under the action is clear. Suppose then that, for some i, $hH_ih^{-1} = H_i$ for all $h \in H$, that is H_i is a fixed point of the action. Therefore for $h \in H_1$ and $h_i \in H_i$ there is some $h_i' \in H_i$ such that $hh_i = h_i'h$. Therefore the sets H_1H_i $(= \{hh_i : h \in H, h_i \in H_i\})$ and H_iH_1 $(= \{h_ih : h \in H, h_i \in H_i\})$ are equal. Let this set be S. Now, it is easy to check that $S \leq G$ (checking closure is easy). Also, both H_1 and H_i are subgroups of S and, in fact, H_i is a normal subgroup of S. But H_1 and H_i are Sylow p-subgroups of S and so conjugate in S, and therefore, since $H_i \trianglelefteq S$, $H_i = H_1$.

It now follows from the Useful Lemma that $|X| = 1 \bmod p$, that is, $n_p = t = 1 \bmod p$, as required.

Now let G act on X by conjugation. Since all the Sylow subgroups are conjugate in G, X forms one whole orbit under this action. Therefore $|X|$ divides $|G|$ by the Orbit-Stabiliser Theorem, that is t divides $p^k m$. But p does not divide t, therefore t divides m, as required. □

Sylow's Theorems can have powerful applications in the study of the structure of finite groups. We give here a few examples.

Examples.

1. A group G of order 42 cannot be simple.

Solution. The number n_7 of Sylow 7-subgroups of G equals 1 mod 7, that is, $n_7 = 1 + 7k$. Since $42 = 7 \cdot 6$, n_7 must divide 6. Therefore $n_7 = 1$, that is the group has a unique Sylow 7-subgroup, which is therefore normal in G. Hence G is not simple.

2. Classify all groups of order pq, both p and q prime such that $p < q$ and $q \neq 1 \mod p$.

Solution. Since n_q divides p, n_q can be either 1 or p, in any case, $n_q \leq p$. But $n_q = 1 + kq$, and $q > p$, therefore $k = 0$, that is, $n_q = 1$. Hence G contains a unique Sylow q-subgroup H which is therefore a normal subgroup of G. (H is a cyclic group of order q.)

Also, n_p divides q (therefore n_p equals 1 or q) and $n_p = 1 + hp$. If $n_p = q$ then $q = 1 \mod p$ which is impossible. Therefore again $n_p = 1$, that is G has a normal Sylow p-subgroup K. (K is a cyclic group of order p.)

Since $H \cap K = \{1\}$ (Why?), $G = HK$ (Why?). Therefore $G \simeq H \times K$ (Exercise 4 in Appendix 2). Therefore G is isomorphic to the cyclic group of order pq (Exercise 2 in Appendix 2).

Problems.

***1.** Let G be the following group of permutations of the set $\{1, 2, 3, 4\}$:

$$\{ \quad \text{id}, (123), (132), (124), (142), (134), (143), (234), \\ (242), (12)(34), (13)(24), (14)(23)\}.$$

(Verify that G is a group. It is, in fact, the alternating group A_4 (see Appendix 6).) Show that G does not contain any subgroup of order 6, and therefore that the converse of Lagrange's Theorem is false.

***2.** Show that a group of order 56 cannot be simple.

***3.** Let G be a group of order p^2q, where p and q are primes such that $q < p$ and q does not divide $p^2 - 1$. Prove that G is isomorphic either to $\mathbb{Z}_{p^2} \times \mathbb{Z}q$ or to $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$.

***4.** Classify all groups of order $20,449$.

5. Let P be a p-subgroup of the finite group G. Then P is contained in some Sylow p-subgroup of G.

6. *The Frattini Argument.* Let K be a finite normal subgroup of G and let P be a Sylow p-subgroup subgroup of K. Then $G = N_G(P).K$. [Recall that $G = X.Y$, for two subgroups X, Y of G, means that any element $g \in G$ can be written as $g = xy$ for some $x \in X$ and $y \in Y$.]

9 Classification of groups of small order (≤ 15)

We now have developed enough group theoretic machinery to classify all groups of order at most 15. By classifying all groups of some particular order n we mean obtaining a list of groups such that any group of order n must be isomorphic to one of the groups in the list. Carrying out this classification for $n \leq 15$ is

not in itself such a big deal after all. But the exercise is worth doing because it brings into play most of the results we have encountered up to now, including the important types of group which were introduced in the problems in Section 4, and it gives a slight inkling of how difficult the general problem of classifying all finite groups is (in fact, there is no complete solution to the general problem) and an idea of the types of technique required.

Exercise. One might well ask whether or not the number of groups of order n is finite. In fact, this is easily proved: Prove that the number of groups of order n is at most n^{n^2}.

We can immediately dispose of all groups of prime order: by Lagrange's Theorem these can have no nontrivial subgroups and are therefore cyclic (a first-year result). This takes care of orders 2, 3, 5, 7, 11, 13.

Problem 1 of Section 4 takes care of the groups of order p^2, p prime. Such a group is either isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. This takes care of orders 4 and 9. [The result for order 4 should already have been obtained by very elementary first-year techniques. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is known as the Klein 4-group.]

Problem 2 of Section 4 classifies all groups of order $2p$, p prime. Such a group is either isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p. This disposes of orders 6, 10, 14.

Groups of order 15 are taken care of by Example 2 of the previous section, since $15 = 3.5$ and $5 \neq 1 \bmod 3$. Therefore a group of order 15 must be isomorphic to the cyclic subgroup $\mathbb{Z}_{15}$.

This leaves groups of orders 8 and 12. It turns out that we cannot deal with these two orders with a single blow as above. A more detailed case-by-case analysis is required. This is, in fact, the rule rather than the exception when trying to classify groups of some particular order. We shall consider the two cases separately.

Notation. The order of an element g will be denoted by $|g|$.

Groups of order 8

It turns out that we can carry out the classification without the need for Sylow's Theorems. Let m be the maximal order of any element of G. Then m can only be equal to 8, 4 or 2 (by Lagrange's Theorem and since m cannot be equal to 1, otherwise G would only contain the identity element.)

Case 1: $m = 8$

Clearly G is isomorphic to the cyclic group $\mathbb{Z}_8$.

Case 2: $m = 4$

Let $x \in G$, $|x| = 4$. Let $H =< x >$ and let $y \in G - < x >$, $y \neq 1$. Therefore $|y| = 2$ or 4. The index of H in G equals 2. Therefore $H \trianglelefteq G$ and the cosets H and Hy give a partition of G, that is

$$G = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

and so x and y generate G. Now, $yxy^{-1} \in H$. Since $|yxy^{-1}| = |x|$ (Easy exercise!) yxy^{-1} can only be x or x^3.

Now we consider the two cases $|y| = 2$ and $|y| = 4$.

Case 2.1: $|y| = 2$

Therefore $y^2 = 1$. Consider separately $yxy^{-1} = x$ and $yxy^{-1} = x^3$.

Case 2.1.1: $yxy^{-1} = x$

Therefore $yx = xy$, G is abelian, and it can be described as

$$G =< x, y | x^4 = y^2 = 1, xy = yx > .$$

It is easy to check that $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$, the isomorphism mapping x to $(1, 0)$ and y to $(0, 1)$.

Case 2.1.2: $yxy^{-1} = x^3$

Therefore $yxy^{-1} = x^{-1}$, so that G can be described as

$$G =< x, y | x^4 = y^2 = 1, yxy^{-1} = x-1 >$$

and this is just the dihedral group D_4.

Case 2.2: $|y| = 4$

Note first that $y^2 \notin Hy$, otherwise y would be in H. Therefore $y^2 \in H$. Also, y^2 cannot be x or x^3 or 1, since $|y^2| = 2$. Therefore $y^2 = x^2$. Again we consider the two subcases $yxy^{-1} = x$ and $yxy^{-1} = x^3$.

Case 2.2.1: $yxy^{-1} = x$

Therefore $yx = xy$, hence G is abelian. Since $x^2 = y^2$, $(xy^{-1})^2 = 1$, that is $|xy^{-1}| = 2$. The group G is generated by x and $z = xy^{-1}$, and G can be described as

$$G =< x, z | x^4 = z^2 = 1, xz = zx >$$

and again it is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$, the isomorphism mapping x to $(1, 0)$ and z to $(0, 1)$.

Case 2.2.2: $yxy^{-1} = x^3$

The group G can therefore be described as

$$G =< x, y | x^4 = y^4 = 1, yxy^{-1} = x^{-1} >$$

and a little checking shows that $G \simeq Q$, the group of quaternions (Problem III in Section 4), the isomorphism mapping x to i and y to j.

Case 3: $m = 2$

Therefore every nonidentity element of G has order 2 and hence G is abelian (easy exercise). Choose $x, y, z \in G - \{1\}$ such that $xy \neq z$ (easy to see that such elements can be found). Let $H = \{1, x, y, xy\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, that is, H is isomorphic to the Klein 4-group. Let $K = \{1, z\} \simeq \mathbb{Z}_2$. Then $G = HK$ and $H \cap K = \{1\}$, therefore $G \simeq H \times K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Conclusion: *A group of order eight is isomorphic to one of the following groups*

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q.$$

Groups of order 12

This is the case which requires most work. Let G be a group of order 12 and let n_3 and n_4 denote respectively the number of Sylow 3-subgroups and 4-subgroups of G. Then $n_3 = 1+3k$ and $n_3 \big| 4$. Therefore $n_3 = 1$ or 4. Similarly, $n_4 = 1$ or 3.

Case 1: $n_3 = 1$

Let H be the Sylow 3-subgroup of G. Then $H \lhd G$. Let $H =< x >$. Let K be a Sylow 2-subgroup of G (therefore $|K| = 4$).

Case 1.1: K is cyclic

Let $K =< y >$. Since $H \cap K = \{1\}$, $y \notin H$, and so the cosets H, Hy, Hy^2, Hy^3 are distinct. These give a partition of G, therefore $G = HK$. Since H is normal, $yxy^{-1} \in H$. The only possibilities are $yxy^{-1} = x$ and $yxy^{-1} = x^2$.

If $yxy^{-1} = x$, then G is abelian, and so $G \simeq H \times K \simeq \mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$.

If $yxy^{-1} = x^2$, that is, $yx = x^2y$, then G is the group

$$\{1, x, x^2, y, xy, xy^2, y^2, xy^2, x^2y^2, y^3, xy^3, x^2y^3\}$$

with product defined by

$$(x^a y^b)(x^c y^d) = x^{a+2^b c} y^{b+d}$$

where the power of x is computed modulo 3 and that of y modulo 4. Another way of describing G is as

$$G =< x, y | x^3 = y^4 = 1, yx = x^2 y > .$$

This is an example of the class of groups called the *dicyclic groups*.

Case 1.2: K is not cyclic

Therefor $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein 4-group. Let $K = \{1, u, v, w\}$ with all non-identity elements having order 2 and $w = uv$ (remember also that K is abelian).

Now $H \lhd G$, therefore $uxu^{-1} = x^a$ and $vxv^{-1} = x^b$, where $a, b = \pm 1$. Note that $wxw^{-1} = ab$.

If $a = b = ab = 1$ then G is abelian and $G \simeq H \times K \simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$.

So suppose that two of a, b, ab equal -1 and the other equals 1. We can assume, without loss of generality, that $uxu^{-1} = x$, $vxv^{-1} = x^{-1} = x^2$ (therefore $vx = x^2 v$) and $wxw^{-1} = x^{-1} = x^2$. Let $z = ux = xu$. Then $|z| = 6$, z and v generate G, and G can be described as

$$G =< v, z | z^6 = v^2 = 1, vz = z^{-1} v >$$

(the last relation arises since $vz = vux = uvx = ux^2 v = z^{-1} v$). But this means that G is ismorphic to the dihedral group D_6.

Case 2: $n_3 = 4$

Any two of these four Sylow 3-subgroups intersect only in the identity (why?) therefore between them they account for eight elements from $G - \{1\}$. Therefore ther can be only one subgroup K of order 4, and so $K \lhd G$. (Note also that G cannot be abelian since it contains distinct subgroups which are conjugate.)

We note first that K cannot be cyclic — because let $K =< y >$ and let $x \in G - K$. Then $xyx^{-1} \in K$. But if $xyx^{-1} = y$, G would be abelian, which is impossible; xyx^{-1} cannot be equal to y^2 since $|y| \neq |y^2|$; and if $xyx^{-1} = y^3$ then $y = x^3 y x^{-3} = y^{27} = y^3$, which is also impossible.

Therefore let $K = \{1, u, v, w\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, with u, v, w as above. Let $x \in G$, $|x| = 3$. Then K, Kx, Kx^2 make up a partition of G. Therefore G is generated

by u, v, x. Now, since $K \lhd G$, conjugation by x permutes the elements u, v, w between them. This permutation cannot be the identity on u, v, w, otherwise G would be abelian. Also, since $|x| = 3$, the order of the permutation is 3, that is, it is a 3-cycle (that is, it permutes u, v, w cyclically). Suppose, without loss of generality, that $xux^{-1} = v, xvx^{-1} = w, xwx^{-1} = u$. Then G is isomorphic to the alternating group A_4, the isomorphism mapping u into the element $(1,2)(3,4)$ of A_4, v into $(1,3)(2,4)$ and x into $(2,3,4)$.

(The alternating groups are discussed in more detail in Appendix 6. At this stage just note that the alternating group A_4 is the group of permutations of the set $\{1,2,3,4\}$ given in Problem 1 of Section 8. This group also arises as the group of permutations on the vertices $1, 2, 3, 4$ of a regular tetrahedron induced by the symmetries of the tetrahedron.)

Conclusion: *A group of order twelve is isomorphic to one of the following groups*

$$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, D_6, A_4, \text{ dicyclic order 12 .}$$

10 Finite abelian groups

Although it is not possible to give the classification of all groups of any finite order, this classification is possible for finite abelian groups. Although we shall not give the proof of the result, the student should stiil be familiar with what it says.

Basically, any finite abelian group is isomorphic to the direct product of cyclic groups. This decomposition as a direct product arises as follows. Let G be an abelian group and let $|G| = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where the p_i are distinct primes. Then $G \simeq G_1 \times G_2 \times \cdots \times G_r$, where each $|G_i| = p_i^{e_i}$. Now, we have to describe the structure of a typical G_i, that is, of an abelian p-group. So let H be an abelian group of order p^n. Then H is isomorphic to some direct product $K_1 \times K_2 \times \cdots \times K_t$ where each K_i is a cyclic group of order p^{n_i}, $n_1 \geq n_2 \geq \cdots \geq n_t$ and of course $n_1 + n_2 + \cdots + n_t = n$. Moreover, this decomposition is unique.

Notation: Let $n, n_1, \dots, n_t$ be natural numbers such that $n = n_1 + n_2 + \cdots + n_t$. Then $n_1, n_2, \dots, n_t$ are said to give a *partition* of n. The number of partitions of n is denoted by $p(n)$. Note that, when counting partitions of n, two partitions which differ only in the order of terms are considered to be the same partition. Therefore we can consider any partition to be given in the standard order $n_1 \geq n_2 \geq \cdots \geq n_t$. In general, finding $p(n)$ is not an easy task, and no simple formula is known. However, for small values of n, $p(n)$ can be found by listing all posiibilities.

Example. Classify all abelian groups of order $2^3.5^2.7^6$.

Solution. Let G be an abelian group of order $2^3.5^2.7^6$. Then $G \simeq G_1 \times G_2 \times G_3$ where $|G_1| = 2^3$, $|G_2| = 5^2$ and $|G_3| = 7^6$.

Therefore G_1 is isomorphic to $\mathbb{Z}_{2^3}$ or $\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; G_2 is isomorphic to $\mathbb{Z}_{5^2}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5$; and G_3 is isomorphic to $\mathbb{Z}_{7^6}$ or $\mathbb{Z}_7 \times \mathbb{Z}_{7^5}$ or $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{7^4}$, etc.

(There are eleven possibilities for G_3, corresponding to the fact that $p(6) = 11$; you are invited to list them all.)

All these decompositions give nonisomorphic groups (by the uniqueness in the above result). Therefore the number of abelian groups of order $2^3.5^2.7^6$ equals $p(3) \times p(2) \times p(6) = 3 \times 2 \times 11 = 66$.

11 Automorphisms

We have seen various examples of bijections on a group G, for example, left translation or conjugacy. We now focus our attention on those bijections which preserve the algebraic structure of G, that is, which are homomorphisms. A bijective homomorphism $\theta : G \to G$ is said to be an *automorphism* of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}G$. As can be expected, $\mathrm{Aut}G$ is a group under composition of functions (Easy exercise!), that is $\mathrm{Aut}G < S_G$. It is called the *automorphism group* of G.

Recall the following elementary facts: (i) $\theta(a^{-1}) = \theta(a)^{-1}$; (ii) $\theta(1) = 1$; (iii) $|\theta(a)| = |a|$; and, (iv) $\theta(a)$ is a generator of G iff a is a generator of G.

Examples

1. The function θ defined by $\theta(a) = a^{-1}$ is an automorphism of G iff G is abelian.

Proof. If G is abelian then clearly θ is a homomorphism. For the converse, suppose θ as given is an automorphism. Then

$$\theta(ab) = (ab)^{-1} = \theta(a)\theta(b) = a^{-1}b^{-1}$$

therefore $ab = ba$.

2. *The automorphism group of the infinite cyclic group*

We shall determine Aut$\mathbb{Z}$. Note that, for any automorphism θ of $\mathbb{Z}$, $\theta(1) = \pm 1$, since a generator must be mapped into a generator.

But if $\theta(1) = 1$ then $\theta(n) = \theta(1 + 1 + \cdots + 1) = \theta(1) + \theta(1) + \cdots + \theta(1) = n$. Therefore θ is just the identity. If $\theta(1) = -1$ then, proceeding as above, $\theta(n) = -n$.

Therefore there are only two possible automorphisms, that is, Aut$\mathbb{Z} \simeq \mathbb{Z}_2$.

3. *The automorphism group of the cyclic group of order n*

We shall determine Aut$\mathbb{Z}_n$. First of all we need to define a group under multiplication modulo n. This is defined as the set U_n of all nonzero positive integers less than n and relatively prime to n. That U_n is in fact a group under multiplication modulo n is given as an exercise below.

As examples, note that, if n is prime, $U_n = \{1, 2, \ldots, n-1\}$. Also, $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. In general, $|U_n|$ is denoted by $\phi(n)$ (Euler's ϕ-function). We have just seen that, if n is prime, $\phi(n) = n - 1$ and $\phi(15) = 8$. A formula for $\phi(n)$ has been derived in the discrete mathematics course.

Now back to Aut$\mathbb{Z}_n$. We use the fact that if θ is an automorphism then $\theta(1)$ must be a generator of $\mathbb{Z}_n$ and, conversely, if $r = \theta(1)$ is a generator of $\mathbb{Z}_n$ then θ can be extended to an automorphism of $\mathbb{Z}_n$ by defining $\theta(s) = sr$. But an element a of $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff it is relatively prime to n (Exercise!), that is, iff

$a \in U_n$. Hence, the elements of Aut$\mathbb{Z}_n$ are in one-one correspondence with those of U_n.

In fact, Aut$\mathbb{Z}_n \simeq U_n$. For let $\theta_i \in$ Aut$\mathbb{Z}_n$, $\theta_i(1) = i \in U_n$. Define $f :$ Aut$\mathbb{Z}_n \to U_n$ by $f(\theta_i) = i$. Then

$$\theta_i \circ \theta_j(1) = \theta_i(j) = ij = \theta_{ij}(1)$$

where the product ij is computed modulo n. Therefore $\theta_i \circ \theta_j = \theta_{ij}$ and so $f(\theta_i \circ \theta_j) = ij(\mod n) = f(\theta_i)f(\theta_j)$.

Exercise. Prove that U_n is a group under multiplication modulo n.

Conjugation

Let $g \in G$, and let θ_g denote the permutation $\theta_g(x) = gxg^{-1}$, that is, conjugation by g. We already know that θ_g is a permutation of G (we have previously denoted θ_g by $\widehat{g}$. In fact this mapping is an automorphism because

$$\theta_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \theta_g(x)\theta_g(y).$$

This automrphism is called an *inner automorphism* and the set of all inner automorphisms is denoted by Inn$G$.

In fact, Inn$G$ is a group, that is, Inn$G \leq$ Aut$G$, because let $\theta_g, \theta_h \in$ Inn$G$. Then

$$\theta_g \circ \theta_h(x) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \theta_{gh}(x)$$

that is, $\theta_g \circ \theta_h = \theta_{gh} \in$ Inn$G$, giving closure.

Also,

$$\theta_g \circ \theta_{g^{-1}}(x) = gg^{-1}xxgg^{-1} = x$$

that is, $\theta_g \circ \theta_{g^{-1}} =$id. Hence ${\theta_g}^{-1} = \theta_{g^{-1}} \in$ Inn$G$.

If G is abelian, Inn$G$ is trivial (just the identity). The next theorem says more.

Theorem 1. Inn$G \simeq \frac{G}{Z(G)}$.

Proof. Define $f : G \to$ Inn$G$ by $f(g) = \theta_g$. Note that f is a homomorphism since $f(gh) = \theta_{gh} = \theta_g \circ \theta_h = f(g) \circ f(h)$. Also, f is surjective since, given $\theta_g \in$ Inn$G$ there clearly exists $g \in G$ such that $f(g) = \theta_g$.

Now,

$$\begin{aligned} \text{Ker } f &= \{g \in G : \theta_g = \text{id}\} \\ &= \{g \in G : gxg^{-1} = x \quad \forall x \in G\} \\ &= \{g \in G : gx = xg \quad \forall x \in G\} \\ &= Z(G). \end{aligned}$$

Therefore, by the First Isomorphism Theroem, $\frac{G}{Z(G)} \simeq$ Inn$G$. □

Problems

***1.** Let θ be an automorphism of a finite group G which leaves only the identity of G fixed, and let $S = \{x.\theta(x^{-1}) : x \in G\}$. Prove that $S = G$. [Hint: Show that $|S| = |G|$.]

NOW LET α BE AN AUTOMORPHISM OF A FINITE GROUP G WHICH LEAVES ONLY THE IDENTITY OF G FIXED, AND LET $\alpha^2 = \mathrm{id}$. PROVE THAT G IS ABELIAN.

***2.** PROVE THAT IF $|G| > 2$ THEN $\mathrm{Aut}G$ IS NOT TRIVIAL.

3. PROVE THAT IF $H \leq G$, $|G| > 4$, THEN THERE IS A NONTRIVIAL AUTOMORPHISM θ OF G SUCH THAT $\theta(H) = H$.

Semi-direct products: A very brief note

Let $H \trianglelefteq G$, and let $g \in G$. Then θ_g is an automorphism of G which fixes H setwise, that is, $\theta_g(H) = H$. Restricted to H, θ_g is an automorphism of H. With this is mind, let us look back at some of our earlier work on the classification of small groups.

Recall that an important construction for describing a group in terms of smaller groups was the direct product. We used the fact that, if $H, K \lhd G, H \cap K = \{1\}$ and $G = HK$, then G was isomorphic to the direct product $H \times K$. The normality of H and K is needed so that that elements of H commute with those of K, and therefore, if $g_1, g_2 \in G, g_1 = h_1k_1, g_2 = h_2k_2$, then

$$g_1g_2 = h_1k_1h_2k_2 = h_1h_2k_1k_2.$$

Hence multiplication in G is imitating multiplication in $H \times K$.

Often however, we are not so fortunate as to have both H and K normal in G, and this leads to groups which cannot be described in terms of direct products of subgroups. Suppose only H is normal. Then every $k \in K$ determines an automorphism θ_k of H defined by $\theta_k(h) = khk^{-1}$. That is, $kh = \theta_k(h)k$. Therefore, although h and k might not commute, kh can be replaced by $h'k$ where $h' = \theta_k(h)$ is at least in H even if it might not be equal to h. Therefore, with g_1, g_2 as above,

$$\begin{aligned} g_1g_2 = h_1k_1h_2k_2 &= h_1\theta_{k_1}(h_2)k_1k_2 \\ &= h_1h_2'k_1k_2 \in HK \end{aligned}$$

and this leads to what is called a *semi-direct product* of H and K.

We shall not go into any more details of what a semi-direct product is. We shall limit ourselves to two examples from earlier work reviewed in the light of the above discussion, and one other example which completes what we had started about groups of order pq.

Examples

1. *The dihedral groups*

Let $G =< r, s | r^n = s^2 = 1, srs^{-1} = r^{-1} = r^{n-1} >$. Let $H =< r >$ and $K =< s >$. Clearly, $H \lhd G$. The last relation above gives the result of conjugation by s on H and it can be written as $sr = r^{-1}s$. If it had been $sr = rs$ instead, then G would have been isomorphic to the direct product of H and K. As it is, we only have a semi-direct product of H and K, because only one of H, K is normal in G.

2. *The dicyclic group of order 12*

Let $G =< x, y | x^3 = y^4 = 1, yxy^{-1} = x^2 >$. Let $H =< x >$ and $K =< y >$. Again, the last relation above describes conjugation on H by y, and it can be written

as $yx = x^2y$ — if it had been $yx = xy$, G would have been the direct product of H and K. As it is, G is a semi-direct product. Note that G is made up of all products x^iy^j (i mod 3 and j mod 4), making up twelve terms in all. Multiplication is computed using the relation $yx = x^2y$, for example,

$$\begin{aligned} xy^3x^2y^2 = xy^2x^2yxy^2 = xy^2x^4y^3 &= xy^2xy^3 \\ &= \cdots = x^2y. \end{aligned}$$

All this works well because the mapping $x \mapsto x^2$ resulting from conjugation by y is an automorphism of G. Note that if G had been the direct product of H and K then $xy^3x^2y^2$ would simply have been equal to $x^3y^5 = y$.

3. *Groups of order* $pq, p < q, q = 1 \bmod p$

(This completes the discussion started in Example 2 of Section 8.) Again we have that, since n_q divides p, $n_q = 1 + kp$, and $q > p$, then $n_q = 1$, and therefore G has a unique (hence normal) subgroup H of order q.

But now consider n_p. We have that n_p divides q, therefore $n_p = 1$ or q. If $n_p = 1$, then G has a normal subgroup K of order p and G would then be the direct product of H and K, giving $G \simeq \mathbb{Z}_{pq}$, as in Example 2 which we have just cited.

But the case under consideration, the possibility $n_p = q$ is not excluded by Sylow's Theorems, because since $q = 1 \bmod p$, the condition $n_p = 1 \bmod q$ would be satisfied. Let us then consider this case in more detail: G would have a Sylow p-subgroup K which would, however, not be normal in G. Therefore G would not be the direct product of H and K. But H is a normal subgroup of G. Therefore let $K \in K, k \neq 1$ (k generates K since $|K| = p$). The mapping $\theta_k : h \mapsto khk^{-1}$ (h any generator of H) defines an automorphism on H, by the normality of H. We must have that $khk^{-1} = h^r$, for some r. What values can r take? If $r = 1$ we get $kh = hk$ and we are back to the direct product of H and K (because elements of H would commute with those of K). Therefore suppose $r \neq 1 \bmod q$. Now, since $\theta_k(h) = h^r$ then $\theta_k^j(h) = h^{r^j}$ (use induction and the fact that θ_k is a homomorphism). In particular, if $j = p$ then $\theta_k^p(h) = h^{r^p}$. But $\theta_k^p(h) = k^phk^{-p} = h$. Therefore r^p must equal $1 \bmod q$. Therefore G can be described as the group

$$< h, k | h^q = k^p = 1, kh = h^rk >$$

with the condition that $r^p = 1 \bmod q$. Note that, as in the previous two examples, this description of G allows us to write any element of G in the form $h^ik^j \in HK$, even when $r \neq 1 \bmod q$ (that is, $kh \neq hk$). Note also that a number $r \neq 1 \bmod q$ satisfying $r^p = 1 \bmod q$ can only be found because $q = 1 \bmod p$.

Finally, one might ask how many such groups are there? The answer would seem to depend on how many different r we can find satisfying the above condition. Certainly, if we take two values $r_1 = 1$ and some $r_2 \neq 1 \bmod q$ (but satisfying the condition), then we would obtain nonisomorphic groups because $r = r_1$ would give $\mathbb{Z}_{pq}$ and $r = r_2$ would give a nonabelian group. However, with a little more work it can be shown that any other appropriate value of r not equal to $1 \bmod q$ would

give a group isomorphic to the one we would obtain with r_2. Therefore there are two groups of order pq ($p < q$ prime, $q = 1 \bmod p$) and these are as described above with $r = 1$ (the cyclic case) and any other value of r not equal to $1 \bmod q$, provided $r^p = 1 \bmod q$.

Problem.

Consider groups of order $21 = 3.7$. Find two values of r such that $r \neq 1 \bmod 7$ and $r^3 = 1 \bmod 7$, and show that these values of r give isomorphic groups of order 21.

Appendix 1. Checklist of topics from first year

1. Axioms, elementary results, examples.
Cyclic groups, infinite and finite.
Order of an element.
Groups of order ≤ 5.
Permutations (bijections on a set) under the operation of composition of functions; the group S_3.

Exercise. Investigate the multiplication table of the group of symmetries of each of the following three solids:

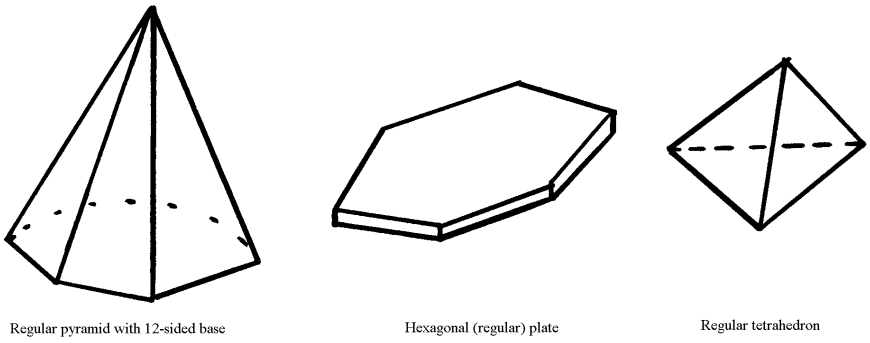


Figure 1: Three solid figures with the same number of symmetries

2. Subgroups, cosets, Lagrange's Theorem, applications.

3. Normal subgroups, quotient groups.

4. Homomorphisms, kernels, isomorphisms, isomorphic groups, automorphisms.

Theorem. *Let $\phi : G \to H$ be a homomorphism with kernel K. Then K is a normal subgroup of G.*

Theorem. *Let G be a group and let $N \trianglelefteq G$. Then $\phi : G \to G/N$ defined by $(g) = Ng$ is a homomorphism with kernel N.*

5. The First Isomorphism Theorem. *Let $\phi : G \to H$ be a surjective (onto) homomorphism with kernel K. Then $G/K \simeq H$.*

Exercise. Let $|G| = 12$ and $|H| = 49$. Prove that the only homomorphism $\phi : G \to H$ is the trivial homomorphism, that is, $\phi(g) = 1, \forall g \in G$, (where 1 is the identity element in H).

6. Permutations, cycle notation.

Theorem. *Any permutation can be written as a product of disjoint cycles.*

7. Cayley's Theorem. *Let G be a group. Then G is isomorphic to a subgroup of S_G.*

Sketch of proof. For $g \in G$, define $f_g : G \to G$ by $f_g(x) = gx$. The set $G' = \{f_g : g \in G\}$ is a subgroup of S_G. The function $\phi : G \to G'$ defined by $\phi(g) = f_g$ is a bijective homomorphism, that is, $G \simeq G'$.

Appendix 2. Direct products

Let G, H be two groups. Then $G \times H$ (the set of all ordered pairs $(g, h), g \in G, h \in H$) can be turned into a group by defining a product as follows:

$$(g_1, h_1).(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

It is an easy exercise to show that, with the above operation, $G \times H$ is indeed a group. This group is called the *direct product* or the *external direct product* of G and H. Note that $G \times H$ contains two subgroups, the set of all pairs $(g, 1)$ and the set of all pairs $(1, h)$, the first being isomorphic to G and the second isomorphic to H. Note also that if G and H are abelian, then so is $G \times H$.

Exercises.

***1.** List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. Show that the first is isomorphic to $\mathbb{Z}_6$ but the second is not isomorphic to $\mathbb{Z}_8$.

***2.** Show that $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ iff m and n are relatively prime.

***3.** Let $H, K \leq G$. Suppose that

(i) $H \cap K = \{1\}$;

(ii) Every element of H commutes with every element of K; and

(iii) $G = HK$ (that is, every element $g \in G$ can be written as a product $hk, h \in H, k \in K$.

Prove that G is isomorphic to $H \times K$. In this case we say that G is the *internal direct product* of H and K, or, in view of the above isomorphism, simply the direct product of H and K.

***4.** Let $H, K \leq G$. Suppose that

(i) $H \cap K = \{1\}$;

(ii) $H, K \trianglelefteq G$; and

(iii) $G = HK$.

Prove that G is isomorphic to $H \times K$.

***5.** The following result is often helpful in proving that $G = HK$ in conjunction with $H \cap K = \{1\}$.

Let H, K be two subgroups of a finite group G. Then

$$|HK| = \frac{|H|.|K|}{|H \cap K|}.$$

6. Let $G = S_3$. Let H be any subgroup of G of order 3; H is normal in G. Let K be any subgroup of G of order 2. Then $H \cap K = \{1\}$, $G = HK$ but $G \not\simeq H \times K$, since $H \times K \simeq \mathbb{Z}_6$.

Appendix 3. Dihedral and quaternion groups

Consider a flat plate in the form of a regular hexagon. Let r denote a rotation of the plate clockwise through $\pi/3$ about the axis of symmetry perpendicular to the plate, and let s denote rotation through π about an axis of symmetry which lies in the plane of the plate.

Exercises.

***1.** Verify that the group of symmetries of the plate is the set

$$\{1, r, r^2, \ldots, r^5, s, rs, r^2s, \ldots, r^5s\}.$$

Verify also that $r^6 = 1 = s^2$ and $sr = r^5s = r^{-1}s$, that is, $srs^{-1} = srs = r^{-1}$. This group is called the dihedral group of order 12, denoted by D_6 (some books denote it by D_{12}.)

***2.** Let G be a group generated by two elements r, s, that is, G consists of all possible products of r and s, for example, r^2, $s^3r^5sr^{-7}$, etc. Now suppose r and s satisfy the following relations: $r^n = 1 = s^2$ and $sr = r^{-1}s = r^{n-1}s$, n a positive integer. All this is written, in short, as

$$G =< r, s | r^n = s^2 = 1, sr = r^{-1}s > .$$

Show that $|G| = 2n$ and that, in fact,

$$G = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

This group is called the dihedral group of order $2n$, denoted by D_n (in some texts D_{2n}). This group is isomorphic to the group of symmetries of a regular n-gon in view of the faithful action:

$$r^i \mapsto \text{ rot. about perp. axis through } 2\pi i/n$$

$$s \mapsto \text{ rot. about parallel axis through } \pi.$$

3. Take $n = 11$ in the previous exercise. Obtain r^3sr^5s in the form $r^is, 0 \leq i \leq 10$.

4. Let

$$G =< t, s | s^2 = 1, sr = r^{-1}s > .$$

Show that

$$G = \{1, t, t^{-1}, t^2, t^{-2}, \ldots, s, ts, t^{-1}s, t^2s, t^{-2}s, \ldots\}.$$

This is called the *infinite dihedral group*, denoted by D_∞. It has the following faithful action on the real line:

$$t^i \mapsto \text{ the translation mapping } x \text{ into } x+i$$

$$s \mapsto \text{ the reflection mapping } x \text{ into } -x$$

The quaternion group

Consider the eight symbols i, j, k multiplied according to the rules $i^2 = j^2 = k^2 = -1, ij = -ji = k$. Then Q, the quaternion group, is the set of eight symbols $\{\pm 1, \pm i, \pm j, \pm k\}$.

Exercises.

***5.** Draw up the multiplication table of Q. Note that Q is not abelian, and therefore it is not isomorphic to any of $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Also, since only -1 has order 2, Q cannot be ismorphic to D_4 which has five elements of order 2.

6. A concrete example of Q is given by the following:- Let H be the group (under matrix multiplication) generated by the two matrices

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

where $i = \sqrt{-1}$ is the usual complex number. Then $H \simeq Q$, under the isomorphism mapping A into i, B into j and the matrix $\begin{matrix} -i & 0 \\ 0 & i \end{matrix}$ into k.

Appendix 4. The Correspondence Lemma

We present here a result about normal subgroups. This lemma can be seen as belonging to the same family of results as the First Isomorphism Theorem.

The Correspondence Lemma. *Let $K \trianglelefteq G$, and let $G^* = G/K$. Let $S^* \leq G^*$. Then,*
(i) There is a subgroup S, $K \leq S \leq G$, such that $S^* = S/K$;
(ii) If $S^* \trianglelefteq G^*$ then $S \trianglelefteq G$;
(iii) If G is finite then $[G^* : S^*] = [G : S]$.

Proof. Let

$$S = \{x \in G : xK \in S^*\}.$$

(i) Let $s_1, s_2 \in S$. Therefore $s_1K, s_2K \in S^*$, therefore $s_1s_2K \in S^*$ (closure in S^*), and so $s_1s_2 \in S$. Similarly, ${s_1}^{-1} \in S$, therefore $S \leq G$. Also, $K \subseteq S$ since if $k \in K$ then $kK = K \in S^*$ (the identity in S^*), therefore $k \in S$.

Now, let $aK \in S/K$. Then $a \in S$, therefore $aK \in S^*$, therefore $S/K \subseteq S^*$. Let $aK \in S^*$. Then $a \in S$, therefore $aK \in S/K$, therefore $S^* \subseteq S/K$. Therefore $S^* = S/K$.

(ii) If $g \in G$ and $s \in S$ (that is, $sK \in S^*$), then $gsg^{-1}K = gKsKg^{-1}K \in S^*$ (by the normality of S^* in G^*), therefore $gsg^{-1} \in S$, that is, $S \trianglelefteq G$.

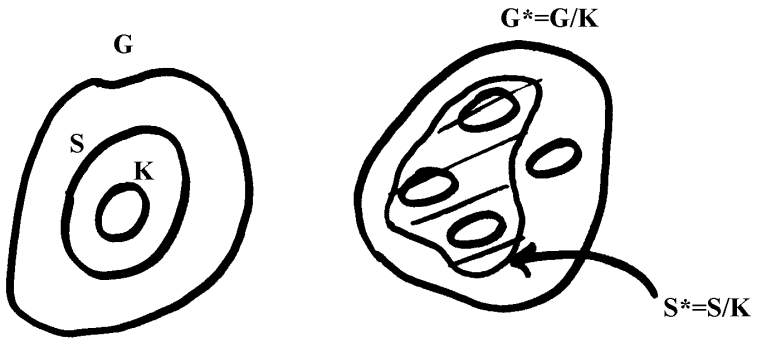


Figure 2: Illustrating the Correspondence Lemma

(iii)

$$[G^* : S^*] = \frac{|G^*|}{|S^*|} = \frac{|G|}{|K|}.\frac{|K|}{|S|} = \frac{|G|}{|S|} = [G : S].$$

□

The Correspondence Lemma together with the fact that a p-group has a nontrivial centre will now be used to show that the converse of Lagrange's Theorem holds for p-groups. Notice the simple but powerful use of normal subgroups in order to obtain a group (the quotient group) of order less than $|G|$ so that induction can be applied.

Theorem 1. *Let G be a group of order p^n, p prime. Then for every $0 \leq k \leq n$ G contains a subgroup of order p^k.*

Proof. By induction on n, the result being clearly true for $n = 1$. Therefore let $n > 1$. Since $|Z(G)| > 1$, $|Z(G)| = p^r$ for some $r \geq 1$. Therefore, by Cauchy's Theorem, there is some element $g \in Z(G)$ whose order is p.

Let $K =< g >$, the cyclic group generated by g. Since $K \subseteq Z(G)$, it follows that $K \trianglelefteq G$. Let $G^* = G/K$; $|G^*| = p^{n-1}$, therefore by the induction hypothesis, G^* contains a subgroup S^* of order p^{n-2}. Therefore there exists S, $K \leq S \leq G$, such that $S^* = S/K$, and $|S| = |S^*|.|K| = p^{n-1}$.

Therefore G certainly contains a subgroup S of order p^{n-1}. Applying the induction hypothesis again, this time on S, gives that S, and hence G, contains subgroups of order p^k for all $0 \leq k \leq n-1$. □

Problem. Prove the converse of Lagrange's Theorem for *abelian* groups, that is, prove that if G is an abelian group and k divides $|G|$, then G has a subgroup of order k. [Hint: Let $m = |G|/k$ and let p be a prime which divides m. Let K be a subgroup generated

BY AN ELEMENT OF ORDER p AND APPLY THE INDUCTION HYPOTHESIS ON $G^* = G/K$. THEN USE THE CORRESPONDENCE LEMMA.]

Appendix 5. Normalisers and centralisers

In the proof of Sylow Theorem 1 we saw an instance of an action defined not on the elements of G but on all subsets of G of a certain size; that is, we concentrated on how the subsets were permuted amongst each other rather than on how the individual elements were permuted. In the above context, the stabilser of a set B consisted of all those $\widehat{g}$ such that $\widehat{g}(B) = B$, and this does not mean that, for $b \in B$, $\widehat{g}(b) = b$, but it means that $\widehat{g}(b) \in B$. We sometimes say that this is the *setwise stabiliser* of B. The set of all those $\widehat{g}$ such that, for all $b \in B$, $\widehat{g}(b) = b$ would be called the *pointwise stabilser* of B.

These notions about pointwise and setwise stabilisers are particularly important when the action is conjugacy. Under conjugacy, a set B is mapped onto the set $\widehat{g}(B) = gBg^{-1}$, and if B is finite, then $|B| = |gBg^{-1}|$ (prove this—it is easy). Therefore under conjugacy we again have that certain sets of a fixed size are permuted amongst each other. In this case, the setwise stabilser of B is called the *normaliser* of B and it is denoted by $N_G(B)$ (or simply $N(B)$). Therefore

$$N_G(B) = \{g \in G : gbg^{-1} \in B, \forall b \in B\}.$$

The pointwise stabiliser of B is called the *centraliser* of B and it is denoted by $C_G(B)$ (or simply $C(B)$). Therefore

$$C_G(B) = \{g \in G : gbg^{-1} = b, \forall b \in B\}.$$

That is, the centraliser is the set of all those elements of G which commute with each element in B. Note that if B contains only one element, then its centraliser equals its normaliser and these definitions coincide with the definition of the centraliser of an element given above in the section on conjugacy.

Exercise.

PROVE THE FOLLOWING ELEMENTARY FACTS MOST OF WHICH FOLLOW IMMEDIATELY FROM THE DEFINITIONS

(I) $C_G(B) \leq N_G(B)$;

(II) IF $B \leq G$ THEN $B \trianglelefteq N_G(B)$ AND $B \trianglelefteq G$ IFF $N_G(B) = G$;

(III) BY ANALOGY WITH CONJUGATE ELEMENTS, IF $H, K \leq G$ AND THERE IS AN ELEMENT $g \in G$ SUCH THAT $K = gHg^{-1}$, THEN H AND K ARE SAID TO BE CONJUGATES. SHOW THAT $H \trianglelefteq G$ IFF EVERY CONJUGATE OF H IS EQUAL TO H. SHOW ALSO THAT IF $|H|$ IS FINITE THEN THE ORDER OF ANY CONJUGATE OF H IS EQUAL TO $|H|$.

Appendix 6. Groups of permutation

The idea of an action has been central to our discussion, and an action essentially means the representation of a group as a group of permutations on some set.

It is therefore opportune to look in some more detail at groups whose elements are permutations.

Let $X = \{1, 2, \ldots, n\}$. The group of all permutations (bijections) on X is denoted by S_X. We know that $|S_X| = n!$. This group is called the *symmetric group of degree* n and it is often denoted by S_n because it is the number of elements of X which gives S_n its properties and not the names we give these elements.

One way to represent a permutation is by writing the elements of X in a row and, underneath each one, its image under the given permutation, for example,

$$\begin{pmatrix} 123456 \\ 532146 \end{pmatrix}.$$

But another very important way to write a permutation is in terms of cycles. For example, the above permutation can be written as

$$(154)(23)(6).$$

A cycle of length n is called an *n-cycle*. Often we omit cycles of length 1, so that the above permutation can be written as $(154)(23)$. It is easy to show that any permutation can be written as a product of disjoint cycles. This representation is essentially unique, that is, it is unique up to choice of initial element and consequent cyclic shift within each cycle and up to order of cycles.

Example. If $\alpha = (127)(34)(5)(6)$ and $\beta = (352)(7)(164)$, then $\alpha\beta = (16357)(24)$.

Exercise.

1. Let the permutation α consist of only one cycle, of length l. Show that the order of α is l, that is, l is the least number such that $\alpha^l = \mathrm{id}$. Now suppose that α consists of cycles of length $l_1, l_2, \ldots, l_r$, and let l be the least common multiple of $l_1, l_2, \ldots, l_r$. Show that the order of α is l.

A 2-cycle is called a *transposition*. Any n-cycle can be written out as a product of $n - 1$ transpositions (not disjoint):

$$(a_1 a_2 \ldots a_n) = (a_1 a_n)(a_1 a_{n-1}) \ldots (a_1 a_2).$$

Since every permutation can be written as a product of disjoint cycles it follows that every permutation can be written as a product of transpositions. Note however that this decomposition is not unique. In fact even the number of transpositions is not unique.

Example. The permutation $(136)(2457)$ is equal to $(15)(35)(36)(57)(14)(27)(12)$ and also to $(16)(13)(27)(25)(24)$.

What is however unique in this decomposition of a permutation is whether or not the number of transpositions is odd or even.

Theorem 1. *Suppose the permutation α in S_n can be written as the product of r transpositions and suppose that it can also be written as the product of r' transpositions. Then r and r' are either both odd or both even.*

Proof. Let $c(\alpha)$ denote the number of cycles of α when it is written as a product of disjoint cycles ($c(\alpha)$ is invariant). Let β be any transposition. We shall first determine $c(\beta\alpha)$ in terms of $c(\alpha)$.

Let $\beta = (ab)$. Now, either (i) a, b are in the same cycle in α or (ii) they are not.

(i) Suppose first that a, b are in the same cycle. Then $\alpha = (ax \dots yb \dots z) \dots$, $\beta\alpha = (ax \dots y)(b \dots z) \dots$, and therefore

$$c(\beta\alpha) = c(\alpha) + 1.$$

(ii) Suppose now that a, b are not in the same cycle of α. Let $\alpha = (ax \dots y)(b \dots z) \dots$. Therefore $\beta\alpha = (ax \dots yb \dots z) \dots$. Hence

$$c(\beta\alpha) = c(\alpha) - 1.$$

Now let $\alpha = \beta_r \beta_{r-1} \dots \beta_1$, where the β_i are transpositions. Since β_1 has one 2-cycle and $n-2$ 1-cycles, $c(\beta_1) = 1 + n - 2 = n - 1$. When multiplying β by $\beta_2, \beta_3, \dots$, the number of cycles changes each time by ± 1. Suppose it increases by 1 g times and it decreases by 1 h times. Then

$$c(\alpha) = n - 1 + g - h.$$

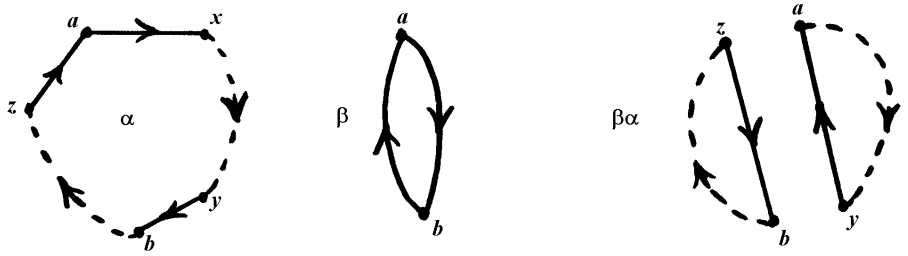
But

$$g + h = r - 1$$

therefore

$$\begin{aligned} r &= g + h + 1 \\ &= 1 + g + (n - 1 + g - c(\alpha)) \\ &= n - c(\alpha) + 2g. \end{aligned}$$

Similarly, if $\alpha = \gamma_{r'} \gamma_{r'-1} \dots \gamma_1$, then $r' = n - c(\alpha) + 2g'$. Therefore $r - r' = 2(g - g')$, which is even. Hence, r and r' are either both odd or both even. □



Illustrating Case (i)

Figure 3: Illustrating part of the proof of Theorem 1

This result therefore makes it legitimate to define an *even* (*odd*) permutation as one which can be written as a product of an even (odd) number of transpositions. The *sign* of a permutation α, denoted by $\text{sgn}(\alpha)$, is defined to be $+1$ if α is even or -1 if α is odd. That is, $\text{sgn}(\alpha) = (-1)^r$ where r is the number of transpositions of α.

This notion of even and odd permutations leads to a very important subgroup of S_n. Note first that if two permutations are both even then so is their product. Therefore, if we define A_n to be the set of all even permutations in S_n, we have closure in A_n. Therefore $A_n \leq S_n$. This subgroup is called the *alternating group of degree* n.

What is the order of A_n? Let H be the group $\{1, -1\}$ under multiplication. Define a function $\phi : S_n \to H$ by $\phi(\alpha) = \text{sgn}(\alpha)$; ϕ is a homomorphism (this is equivalent to saying that the product of two even permutations is an even permutation and the product of an odd permutation with an even permutation is an odd permutation). The kernel of ϕ consists of all those permutation in S_n whose sign is 1; that is, the kernel is A_n. Therefore $A_n \lhd S_n$ and, by the First Isomorphism Theorem, $S_n/A_n \simeq H$, that is, $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

Exercises.

***2.** Look back at the last part of the classification of groups of order 12 and verify that A_4 is, in fact, as given there. Verify also that A_4 is the group of permutations on the four vertices of a regular tetrahedron induced by the group of symmetries of the tetrahedron.

***3.** Show that A_4 has no subgroup of order 6.

***4.** Let G be the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. By Cayley's Theorem, G is isomorphic to the group of permutations on G induced by left translations (that is, every element $g \in G$ corresponds to the permutation $\widehat{g} \in S_G$ where $\widehat{g} : x \mapsto gx$). Obtain a representation of G as a group of permutations. [Represent the elements of G by $1, 2, 3, 4$ and write down in cycle notation what $\widehat{g}$ is for every $g \in G$.]

Do the same for the dihedral group D_n.

5. If a permutation $\alpha \in S_n$ has t_i cycles of length i, $1 \leq i \leq n$, then we say that α is of *type* $[1^{t_1}2^{t_2}\dots n^{t_n}]$. For example, if $n = 8$, the permutation (12734658) has type $[8^1]$ and the permutation (12)(375)(4)(6)(8) has type $[1^3 2^1 3^1]$. The type of a permutation is also called its *cycle structure*.

Prove (or look it up in any text book) that two permutations $\alpha, \beta \in S_n$ are of the same type iff there is a $\gamma \in S_n$ such that $\alpha = \gamma\beta\gamma^{-1}$, that is, iff α and β are conjugates in S_n. Therefore the conjugacy classes in S_n consist precisely of those permutations which have the same type or cycle structure.

***6.** Find the conjugacy classes of S_4 and S_3. Find the conjugacy classes of A_4. (Note that two permutations from A_4 might be conjugate in S_4 but not in A_4.) Give a geometric interpretation of the conjugacy classes of A_4 considered as the group of permutations of the vertices of a regular tetrahedron.

6. Supplementary and Further Reading

The book *Introduction to Group Theory, 2nd Ed* by Lederman and Weir is an excellent companion to this course and it treats the subject, in terms of actions, in much the same way as we do in these notes.

The book *Groups and Symmetry* by M.A. Armstrong is also very good, and also takes the point of view of actions. However, it is more expensive. Suggested chapters from this book and the main things to pick out from them would be: 1) Symmetries of tetrahedron, 2) Axioms, 4) Dihedral group, 5) Subgroups and generators, 10) Product, 11) Lagrange's Theorem, 12) Partitions of a set, 17) Actions, 13) Cauchy's Theorem, 14) Conjugacy, 8) Cayley's Theorem.

The chapters on permutations, groups and group actions in Bigg's *Discrete Mathematics* should all be consulted, especially by those students who will be taking the Combinatorics elective when we shall work more on the applications of group actions to enumeration (Burnside's and Pólya's Theorems).