1 · Permutation Groups

'... it will afford me much satisfaction if, by means of this book, I shall succeed in arousing interest among English mathematicians in a branch of pure mathematics which becomes the more fascinating the more it is studied.'

W. Burnside, in his preface to Theory of groups of finite order, 1897.

1.1 Preliminary definitions

It is presumed that the reader will already be familiar with the contents of this section. He is advised to read it quickly, in order to accustom himself to the notation which will be used throughout the rest of the book.

If X is a finite set, a permutation of X is a one-to-one correspondence (bijection) $\alpha : X \to X$. Two such permutations α, β can be composed to give the permutation $\alpha\beta : X \to X$, which we shall define by the rule $\alpha\beta(x) = \alpha(\beta(x))$. That is, we shall write functions on the left, and compose in the order compatible with this convention. Under the operation of composition the set of all permutations of X forms a group $\mathrm{Sym}(X)$, the symmetric group on X. If X is the set $\{1, 2, \ldots, n\}$, we write S_n for $\mathrm{Sym}(X)$, and we have $|S_n| = n!$ where we use $|\ |$ to denote cardinality.

If G is a subgroup of $\mathrm{Sym}(X)$, then we shall say that the pair (G, X) is a permutation group of degree $|X|$, and that G acts on X. More generally, we shall meet the situation where there is a homomorphism $g \mapsto \hat{g}$ of a group G into $\mathrm{Sym}(X)$: this will be called a permutation representation of G. When the homomorphism $g \to \hat{g}$ is a monomorphism, we say that the representation is faithful; in this case it is convenient to identify G with its image in $\mathrm{Sym}(X)$, so that we recover the case of a permutation group (G, X).

Any permutation α in $\mathrm{Sym}(X)$ may be decomposed, in an

essentially unique way, into disjoint cycles:

$$\alpha = (a_1 a_2 \ldots a_k)(b_1 b_2 \ldots b_l) \ldots .$$

This notation means that $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, $\ldots$ $\alpha(a_k) = a_1$, and so on. A transposition is a cycle (ab); since $(x_1 x_2 \ldots x_r)$ is equal to the composite $(x_1 x_r)(x_1 x_{r-1}) \ldots (x_1 x_2)$, any permutation can be expressed as the composite of (not necessarily disjoint) transpositions. This expression is not unique, but if

$$\alpha = \tau_1 \tau_2 \ldots \tau_k = \sigma_1 \sigma_2 \ldots \sigma_l ,$$

where the τs and σs are transpositions, then $k \equiv l \pmod 2$. When $k \equiv 0 \pmod 2$ we say that α is even and write $\mathrm{sgn}(\alpha) = 1$, and when $k \equiv 1 \pmod 2$ we say that α is odd and write $\mathrm{sgn}(\alpha) = -1$. The sgn function is a homomorphism of $\mathrm{Sym}(X)$ into the multiplicative group $\{1, -1\}$ and its kernel, the set of even permutations, is a normal subgroup of $\mathrm{Sym}(X)$, known as the alternating group $\mathrm{Alt}(X)$. We write A_n for the alternating subgroup of S_n. It is easy to see that

$$|\mathrm{Sym}(X) : \mathrm{Alt}(X)| = 2, \quad \text{and} \quad |A_n| = \tfrac{1}{2} n! .$$

If α and π are in $\mathrm{Sym}(X)$, and α has the cycle decomposition given above, then

$$\pi \alpha \pi^{-1} = (\pi a_1 \pi a_2 \ldots \pi a_k)(\pi b_1 \pi b_2 \ldots \pi b_l) \ldots .$$

We say that $\pi \alpha \pi^{-1}$ is the conjugate of α by π: two elements of $\mathrm{Sym}(X)$ are conjugate in $\mathrm{Sym}(X)$ if and only if they have the same cycle shape. Thus the number of conjugacy classes in S_n is just the number of partitions of n. For example, in S_5 we have

Partition	Class representative	Number in class
1,1,1,1,1	Identity	1
1,1,1,2	(12)	10
1,1,3	(123)	20
1,4	(1234)	30
5	(12345)	24
1,2,2	(12)(34)	15
2,3	(12)(345)	20
		$120 = 5!$.

Here, as is customary, we have suppressed cycles of length one.

1.2 Counting principles

A basic technique of combinatorial mathematics is to count the same set in two different ways and equate the answers. Precisely, let U and V be finite sets, S a subset of $U \times V$, and define

$$S(a, \cdot) = \{v \in V \mid (a, v) \in S\},$$

$$S(\cdot, b) = \{u \in U \mid (u, b) \in S\}.$$

Then $S(a, \cdot)$ is in one-to-one correspondence with the subset of S consisting of the pairs (u, v) with $u = a$, and these subsets, for $a \in U$, partition S. The analogous result holds for the sets $S(\cdot, b)$. Hence

$$1.2.1 \quad |S| = \sum_{a \in U} |S(a, \cdot)| = \sum_{b \in V} |S(\cdot, b)| .$$

If, in a particular example, we can show that $|S(a, \cdot)| = r$, and $|S(\cdot, b)| = s$, independent of a and b respectively, then it follows that

$$1.2.2 \quad r|U| = s|V| .$$

We apply this method to the action of the permutation group G on a finite set X. Introduce the temporary notation

$$G(x \mapsto y) = \{g \in G \mid g(x) = y\} .$$

We check that the statement "$G(x \mapsto y)$ is not empty" defines an equivalence relation on X, and denote the equivalence class of x by Gx. If $y \in Gx$, then choosing any g in $G(x \mapsto y)$ gives us a one-to-one correspondence:

$$G(x \mapsto x) \longleftrightarrow G(x \mapsto y) \quad \text{defined by} \quad h \longleftrightarrow gh.$$

Now the counting principle applies: fix x in X and let P_x denote the subset of $G \times X$ consisting of those pairs (g, y) for which $y = g(x)$. Then $P_x(\cdot, y)$ is just $G(x \mapsto y)$, and so

$$|P_x(\cdot, y)| = \begin{cases} |G(x \mapsto x)| & \text{if } y \in Gx, \\ 0 & \text{if } y \notin Gx. \end{cases}$$

Also, $|P_x(g, \cdot)| = 1$ for all g in G. Hence 1.2.1 implies that

$$1.2.3 \quad |G(x \mapsto x)|\,|Gx| = |G|.$$

This is the fundamental relation of the theory of permutation groups. The set Gx is called the orbit of x, and $G(x \mapsto x)$ is called the stabilizer of x - it is a subgroup of G and is usually written G_x. Thus 1.2.3 becomes

$$1.2.4 \quad |Gx| = |G : G_x|.$$

In order to find the number of orbits of G on X, we may use a formula involving the set $F(g)$ of fixed points of g; that is, the set of all x for which $g(x) = x$. The result is often called 'Burnside's Lemma', although its origin is with Frobenius.

1.2.5 **Theorem.** Let t denote the number of orbits of (G, X). Then

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

Proof. Let $E = \{(g, x) \in G \times X \mid g(x) = x\}$. Then

$$E(g, \cdot) = F(g), \quad E(\cdot, x) = G_x.$$

Applying the counting principle 1.2.1, we get

$$\sum_{g \in G} |F(g)| = \sum_{x \in X} |G_x| .$$

Now let $x_1, x_2, \ldots, x_t$ be representatives of the t orbits. If x belongs to the orbit Gx_i, and g is any member of $G(x \mapsto x_i)$, then the stabilizer G_x is simply $g^{-1}G_{x_i}g$, so that $|G_x| = |G_{x_i}|$. Thus we may collect the like terms on the right-hand-side above, yielding

$$\begin{aligned} \sum_{g \in G} |F(g)| &= \sum_{i=1}^{t} \sum_{x \in Gx_i} |G_x| \\ &= \sum_{i=1}^{t} |Gx_i||G_{x_i}| \\ &= \sum_{i=1}^{t} |G| \qquad \text{(by 1.2.4)} \\ &= t|G|. \quad // \end{aligned}$$

For example, let $X = \{1, 2, 3, 4\}$ be the set of corners of a square, given in clockwise order, and let $G = D_8$ (dihedral group of order 8) be the permutations of X which can be realised by rotations or reflections in a plane. The elements of G, and their numbers of fixed points, are as follows:

g :	Identity	(13)	(24)	(13)(24)	(1234)	(1432)	(12)(34)	(14)(23)
$\|F(g)\|$:	4	2	2	0	0	0	0	0

Hence $t = (1/8)(4 + 2 + 2) = 1$, and there is just one orbit.

1.3 Transitivity

1.3.1 Definition. The permutation group (G, X) is transitive if there is just one orbit in the action of G on X.

We may use Burnside's lemma, as in the example at the end of the previous section, to check whether a given permutation group is transitive. A more direct method is to pick one element x of X and search for elements of G taking x to every other element y in X. In the example,

the existence of the permutation (1234) (and its powers) is sufficient to ensure transitivity. We remark that, in the transitive case, the basic results 1.2.4 and 1.2.5 become

$$1.3.2 \quad |X| = |G : G_x|, \quad |G| = \sum_{g \in G} |F(g)| .$$

We now consider the action of G_x on X.

1.3.3 **Theorem.** Suppose (G, X) is transitive and let $r(x)$ denote the number of orbits of G_x on X. Then

$$r(x)|G| = \sum_{g \in G} |F(g)|^2 ,$$

and $r(x)$ is independent of x.

Proof. From Burnside's lemma 1.2.5 we have

$$r(x)|G_x| = \sum_{g \in G_x} |F(g)| .$$

The right-hand side of this equation is just the cardinality of the set of pairs $\{(g, w) | g \in G_x, g(w) = w\}$. For any $y \in X$ there is a one-to-one correspondence between this set and the set $\{(k, z) | k \in G_y, k(z) = z\}$, defined by $(g, w) \mapsto (hgh^{-1}, h(w))$, where h is any element of G such that $h(x) = y$. Thus the right-hand side of the equation is independent of x, and since $|G| = |X||G_x|$ we have

$$r(x)|G| = r(x)|X||G_x| = \sum_{x \in X} \sum_{g \in G_x} |F(g)| .$$

Inverting the order of the double sum, we get

$$r(x)|G| = \sum_{g \in G} \sum_{x \in F(g)} |F(g)| = \sum_{g \in G} |F(g)|^2 .$$

Since the right-hand side is independent of x, so is $r(x)$. //

1.3.4 **Definition.** The rank r of the transitive group (G, X) is the number of orbits of G_x on X.

In the action of D_8 on the corners of a square we have

$r = (1/8)(4^2 + 2^2 + 2^2) = 3$. The three orbits of the stabilizer of 1 are $\{1\}$, $\{2, 4\}$, and $\{3\}$.

The case $r = 2$ is especially interesting - here, G_x is itself transitive on $X - \{x\}$, and it follows that there is an element of G taking any distinct pair of elements of X to any other pair. In this vein, we make the following definition.

1.3.5 Definition. The permutation group (G, X) is k-transitive $(k \geq 1)$ if, given any two ordered k-tuples $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ of distinct elements of X, there is some g in G such that

$$g(x_i) = y_i \qquad (1 \leq i \leq k).$$

Clearly, a k-transitive group is also l-transitive, for $1 \leq l \leq k$. Usually, when we say that G is k-transitive on X we imply that k is the largest integer for which this is so. A k-transitive group with $k \geq 2$ is a transitive group of rank two, and we sometimes use the general term multiply transitive in this case; the fixed point formulae 1.2.5 and 1.3.3 become

$$|G| = \sum |F(g)|, \quad 2|G| = \sum |F(g)|^2.$$

The determination and construction of multiply transitive groups is facilitated by the following lemma.

1.3.6 Lemma. *Suppose that G is known to be transitive on X. Then (G, X) is k-transitive if and only if $(G_x, X - \{x\})$ is (k-1)-transitive.*

Proof. Let us suppose that G_x is (k-1)-transitive on $X - \{x\}$. Given any two ordered k-tuples $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ of distinct elements of X, we may select g_1, g_2 in G and h in G_x with the properties

$$g_1(x_1) = x, \quad g_2(y_1) = x,$$
$$h[g_1(x_i)] = g_2(y_i) \qquad (2 \leq i \leq k).$$

Then $g_2^{-1}hg_1$ is an element of G transforming the ordered k-tuples as required. The converse is straightforward. //

Thus, to determine if a given group is multiply transitive, we must examine the successive stabilizers G_x, $G_{xy} = (G_x)_y$, and so on. If G is k-transitive on X, and $|X| = n$, then repeated application of the first part of 1.3.2 yields the useful result

$$1.3.7 \quad |G| = n(n-1)(n-2)\ldots(n-k+1)|G_{x_1 x_2 \ldots x_k}|,$$

where the group on the right-hand side is the pointwise stabilizer of $x_1, x_2, \ldots, x_k$. In particular, we note that the order of G must be divisible by $n(n-1)(n-2)\ldots(n-k+1)$. If G is k-transitive, and the identity is the only permutation fixing k points, then G is said to be sharply k-transitive, and its order is exactly $n(n-1)\ldots(n-k+1)$.

The idea of sharp transitivity is especially important in the case $k = 1$; the group G is then said to be regular on X, and we have $|G| = |X|$. In fact, G and X are in one-to-one correspondence, defined by $g \longleftrightarrow g(x_0)$, for any fixed x_0 in X.

1.3.8 Theorem. *S_n is n-transitive, and A_n is (n-2)-transitive, in their actions on the set $\{1, 2, \ldots, n\}$ $(n \geq 3)$.*

Proof. The first part is obvious, since S_n contains all permutations of the n-set. In the alternating case, we may proceed by induction. When $n = 3$, A_3 contains (123) and so it is 1-transitive. The stabilizer of the symbol n in A_n is A_{n-1}, and so, by 1.3.6 the induction step is valid. It remains to be shown that A_n cannot be more than (n-2)-transitive. To see this, we remark that the only permutation of $\{1, 2, \ldots, n\}$ which takes the ordered (n-1)-tuple $(1, 2, \ldots, n-2, n-1)$ to $(1, 2, \ldots, n-2, n)$ is the odd permutation $(n-1\ n)$, which is not in A_n. Thus A_n is not (n-1)-transitive. //

We conclude this section with some remarks on the coset decomposition of transitive and multiply transitive groups.

The basic argument of Section 1.2 may be expressed in the following way: if $g, g' \in G$ and $x \in X$, then

$$g' \in gG_x \iff g'(x) = g(x) .$$

Thus the cosets of G_x in G are precisely those sets $G(x \mapsto y)$ which are not empty. When G is transitive a complete set of coset representatives is any family $\{g_y\}$ $(y \in X)$ such that $g_y(x) = y$. We then have

$$G = G_x \cup \left(\bigcup_{y \neq x} g_y G_x \right).$$

When G is multiply transitive there is another decomposition, in terms of the double cosets $G_x g G_x$.

1.3.9 Lemma. *Suppose that G is k-transitive on X $(k \geq 2)$ and $g \notin G_x$. Then $G = G_x \cup G_x g G_x$.*

Proof. Let h be any element of $G - G_x$. Since G is multiply transitive, there is some g_1 in G taking $g^{-1}(x)$ to $h^{-1}(x)$ and fixing x. This implies that hg_1g^{-1} belongs to G_x, that is, h belongs to $G_x g G_x$. //

This lemma will be useful in the construction of multiply transitive groups.

1.4 Applications to group theory

An abstract group G acts on the set 2^G of subsets of G in two especially important ways:

$$\begin{aligned} &\text{(i)} \quad g(K) = gK \\ &\text{(ii)} \quad g(K) = gKg^{-1} \end{aligned} \qquad (g \in G, \quad K \subseteq G) .$$

Many notions and theorems of group theory can be expressed in terms of these actions. For example, if K is a subgroup of G $(K \leq G)$ then the orbit of K in the first action consists of the left cosets of K in G, and the stabilizer of K is K itself. Thus 1.2.3 gives Lagrange's theorem that $|K|$ divides $|G|$, the quotient being the index $|G : K|$ or the number of distinct (left) cosets.

As another example, consider the second action in the case where $K = \{k\}$; then the orbit of K is the conjugacy class containing k. Moreover, the stabilizer G_k is just the centralizer $C(k)$ so that, by 1.2.4:

1.4.1 The number of conjugates of k is $|G : C(k)|$.

In particular, each element in the centre $Z(G)$ is its own conjugacy class. The partition of G induced by this action gives rise to the class equation

$$1.4.2 \quad |G| = |Z(G)| + \sum |G : C(g)| ,$$

where the summation ranges over a complete set of nonconjugate g not in $Z(G)$. It follows directly that a nontrivial p-group has a nontrivial centre. For if g is in $G - Z(G)$, then $C(g)$ is a proper subgroup of G and thus $|G : C(g)|$ is a positive power of p; thus p divides the summation and hence also $|Z(G)|$.

As a final example, we begin the proof of Sylow's theorem. Suppose p^r is the highest power of the prime p which divides $|G|$. Consider all subsets of G with cardinality p^r; there are $\binom{|G|}{p^r}$ of them, and this binomial coefficient is easily seen to be prime to p. Thus there must be at least one orbit (in the action $K \mapsto gK$) whose length m is prime to p, and the stabilizer G_L of a subset L in this orbit has order $|G|/m$, which is divisible by p^r. But if $l \in L$, then $G_L(l) \subseteq L$, and $|G_L| = |G_L(l)| \leq |L| = p^r$, so that $|G_L| = p^r$. Thus we have produced a subgroup (G_L, in fact) of order p^r. The other parts of the theorem can be proved by similar arguments; see 1.8.

Next, we observe the relationship between subgroups of G and transitive permutation representations of G, namely: G has a transitive permutation representation of degree n if and only if G has a subgroup of index n. To see this, first let (G, X) be transitive, of degree n, so that (by 1.3.2) $|G : G_x| = |X| = n$ and G_x is a subgroup of index n. Conversely, if H is a subgroup of index n and $X = \{H, g_2H, \ldots, g_nH\}$ is the set of left cosets of H in G, then G acts transitively on X by defining $g(g_iH)$ to be the coset $(gg_i)H$. As a trivial application of this relationship, we see that S_5 has no transitive permutation representation of degree 4.