Action of a Group on a Set

Suppose G is a group, S is a set, and A(S) is the group of all permutations on S (bijections of S on itself).

Definition. A homomorphism $\theta : G \to A(S)$ is called a *permutation representation* of G on S, and G is said to *act* on S .

Notation. If $a \in G$, we write θ_a for the image of a under θ , rather than $\theta(a)$, so that θ_a is a map of S to S, and, if $s \in S$, $\theta_a(s)$ is the image of s under θ_a .

Note that, if $a, b \in G$, and e is the identity element of G, then

$$(*) \qquad \theta_{ab} = \theta_a\theta_b \ , \ \ \theta_e = i_S \text{ (the identity map on S).}$$

Conversely, if G is a group, S is a set, and for every element a in G there is defined a map $\theta_a : S \to S$, in such a way that (*) is satisfied, then in fact each θ_a must be a bijection, and we have a permutation representation θ of G on S . (Exercise.)

Examples.

(1) $G = \mathbf{R}$ (the group of real numbers under addition), $S = \mathbf{C}$ (the complex plane), $\theta_a(s) = se^{ia}$. (θ_a = rotation through angle a about the origin).
(2) G any group, S = G , $\theta_a(s) = as$. (G acts on G by *left translation.*)
(2') G any group, S = set of all subsets of G , $\theta_a(s) = as = \{ax | x \in s\}$.
(3) G any group, S = G , $\theta_a(s) = asa^{-1}$. (G acts on G by *conjugation.*)
(3') G any group, S = set of all subsets of G , $\theta_a(s) = asa^{-1} = \{axa^{-1} | x \in s\}$.

Orbits. Suppose G acts on S , $\theta : G \to A(S)$. If $s, t \in S$, it may or may not be possible to find an element a of G such that $\theta_a(s) = t$. Define a relation on S by setting

$$s \sim t \text{ if there exists an element a of G such that } \theta_a(s) = t .$$

This is an equivalence relation on S . (Exercise.)
The equivalence class of an element s of S is called its *orbit* under G ,

$$Orb_G(s) = \{\theta_a(s) | a \in G\} .$$

From work on equivalence relations, we have the first part of the
Proposition. (i) The orbits of elements of S form a partition of S .
(ii) If $b \in G$, then θ_b maps each orbit $Orb_G(s)$ into itself, so that G may be considered to act on $Orb_G(s)$. (Exercise.)

Examples. (Numbers refer to the list of examples given before.)
(1) Orbits are circles centered at the origin.

(2) There is just one orbit, the whole of G .

(2') Suppose H is a subgroup of G (so H is an element of S). Then $Orb_G(H)$ is the set of all left cosets aH of H in G .

(3), (3') The orbit of an element x or a subset x of G under conjugation is called the *conjugacy class* of x in G ,

$$cl_G(x) = \{axa^{-1} | a \in G\} .$$

Stabilizers. Suppose G acts on S , $\theta : G \to A(S)$. If $s \in S$, its *stabilizer* in G is

$$Stab_G(s) = \{a \in G | \theta_a(s) = s\} .$$

This is a subgroup of G . (Exercise.) Since the identity map on S is the map which fixes every element s of S , it follows that

Ker θ is the intersection of the stabilizers of all the elements of S .

Examples.

(1) If $s \neq 0$, $Stab_G(s)$ consists of all integer multiples of 2π .

(2) $Stab_G(s) = \{e\}$, for every element s of G .

(2') If H is a subgroup of G , then $Stab_G(H) = H$; more generally, $Stab_G(aH) = aHa^{-1}$. (Exercise.)

(3) The stabilizer in G of an element x (under conjugation) is called the *centralizer* of x in G , denoted $C_G(x)$, and

$$C_G(x) = \{a \in G | ax = xa\} .$$

(3') The stabilizer in G of a subset X (under conjugation) is called the *normalizer* of X in G , denoted $N_G(X)$, and

$$N_G(X) = \{a \in G | aXa^{-1} = X\} .$$

Remark. Application of part (ii) of the last proposition to example (2') shows that, if a group G has a subgroup H of index n , then there is a permutation representation of G on the set of n left cosets of H in G , given by left translation, i.e., a homomorphism

$$\phi : G \to S_n \text{ (the symmetric group of degree n).}$$

Since the stabilizer of H is H , the kernel K of ϕ is a normal subgroup of G contained in H , and G/K is isomorphic with a subgroup of S_n . This generalizes Cayley's theorem.

Special case. Suppose G is a finite group, and H is a subgroup of index p in G , where p is the smallest prime number dividing the order |G| . Then H is a normal subgroup of G .

Proof. The remark above gives a normal subgroup K of G contained in H , such that G/K is isomorphic with a subgroup of S_p . By Lagrange's theorem, |G/K| divides p! However,

$$|G/K| = |G|/|K| = (|G|/|H|)(|H|/|K|) = p(|H|/|K|) ,$$

and so (|H|/|K|) divides (p - 1)! But (|H|/|K|) is a divisor of |G| , so it has no prime divisor less than p . It follows that (|H|/|K|) = 1 , so H = K , so H is normal in G .

Homework

1. Suppose that G is a group, S is a set, and for every element a in G there is defined a map $\theta_a : S \to S$, in such a way that

$$\theta_{ab} = \theta_a\theta_b \text{ , for all } a , b \in G ,$$

$$\text{and } \theta_e = i_S \text{ (the identity map on S).}$$

Show that each θ_a must be a bijection.

2. Suppose G acts on S , $\theta : G \to A(S)$. Show that the relation defined by setting

$$s \sim t \text{ if there exists an element a of G such that } \theta_a(s) = t$$

is an equivalence relation on S .

3. Suppose G acts on S , $\theta : G \to A(S)$. If $b \in G$, $s \in S$, show that θ_b maps the orbit $Orb_G(s)$ into itself.

4. Consider the action of a group G on the set of all its subsets, by left translation. Let H be a subgroup of G , $a \in G$. Show that the stabilizer $Stab_G(aH)$ of the left coset aH is aHa^{-1} .

Relation between orbits and stabilizers

Theorem. Suppose G acts on S , $\theta : G \to A(S)$. Let $s \in S$. There is a 1-1 correspondence between the orbit $Orb_G(s)$ and the set of all left cosets of the stabilizer $Stab_G(s)$ in G , in which $\theta_a(s)$ corresponds to $aStab_G(s)$ $(a \in G)$.

Proof. Define a map f from $Orb_G(s) = \{\theta_a(s) | a \in G\}$ to the set $\{aStab_G(s) | a \in G\}$ of left cosets, by setting $f(\theta_a(s)) = aStab_G(s)$. Since an element of $Orb_G(s)$ can be given as $\theta_a(s)$ for more than one element a of G , we need to show that f is well-defined. This means that, if $\theta_a(s) = \theta_b(s)$, then $aStab_G(s) = bStab_G(s)$.

So, suppose that $\theta_a(s) = \theta_b(s)$. Then, $\theta_b^{-1}\theta_a(s) = s$, so $\theta_{b^{-1}a}(s) = s$ (since θ is a homomorphism). Thus, $b^{-1}a \in Stab_G(s)$, so $aStab_G(s) = bStab_G(s)$. So, f is well-defined.

Running the argument in reverse shows that f is injective. Since f is clearly surjective, this proves the theorem.

Note. If $g \in G$, then in the action of G on S , g maps $\theta_a(s)$ on $\theta_g\theta_a(s) = \theta_{ga}(s)$, while, in the action of G on the set of left cosets of $Stab_G(s)$, g maps $aStab_G(s)$ on $gaStab_G(s)$, and $\theta_{ga}(s)$ and $gaStab_G(s)$ correspond under f . So the action of G on the orbit $Orb_G(s)$ is "the same" as the action of G on the set of left cosets of $Stab_G(s)$ in G .

Corollary to Theorem. If a is an element of a group G , the number of elements of the conjugacy class $cl_G(a)$ of a in G is equal to the index $[G:C_G(a)]$ in G of the centralizer $C_G(a)$. If G is finite, this is a divisor of the order $|G|$.

Corollary (*The class equation*) If G is a finite group, then

$$|G| = |Z(G)| + \sum_a [G:C_G(a)] \ ,$$

where a runs over a set of representatives of the conjugacy classes of noncentral elements of G , and Z(G) is the center of G ..

Proof. Since the conjugacy classes partition G , the number of elements in G is the sum of the numbers of elements in the conjugacy classes. From the previous result,

$$|G| = \sum_a [G:C_G(a)] \ ,$$

where a runs over a set of representatives of all the conjugacy classes of G . Split the sum up into those terms which are 1 and those which are greater than 1. Since $cl_G(a)$ contains just one element, a itself, if and only if $a \in Z(G)$ (Exercise), the sum of the terms which are 1 is the order $|Z(G)|$.

Example. If p is a prime number, a group whose order is a power of p is called a *p-group.* If G is a p-group, not the trivial group {e}, then each term $[G:C_G(a)]$ in the class equation is a power of p since it divides |G| , and so is divisible by p , if a is noncentral. Since |G| is also divisible by p , it follows that |Z(G)| is divisible by p . Thus, *the center of a nontrivial p-group is also nontrivial.* This fact makes it possible to prove many results about p-groups, by induction on the order. (See p.104 of the textbook.)

Sylow's Theorem

If G is a finite group, and m is a divisor of the order |G| , G may not have a subgroup of order m , so Lagrange's theorem does not have a full converse. However, there is a partial converse.

Theorem (*First Sylow Theorem*) If G is a finite group, p a prime number, and p^k divides |G| , then G has at least one subgroup of order p^k .

Proof The result is true if |G| = 1 . Use induction on |G| ; assume that it is true for all groups of order less than |G| .
The result is also true if k = 0 . Assume k > 0 , so that p divides |G| .
Case 1. Suppose p divides |Z(G)| . By Cauchy's theorem applied to the abelian group Z(G) , Z(G) has a subgroup H of order p . Then H is a normal subgroup of G , and p^{k-1} divides |G/H| . By induction hypothesis, G/H has a subgroup of order p^{k-1} . By the correspondence theorem, this has the form K/H , where K is a subgroup of G containing H. Then $|K| = |K/H|\,|H| = p^{k-1}p = p^k$.
Case 2. Suppose p does not divide |Z(G)| . From the class equation, there exists a noncentral element a such that p does not divide $[G:C_G(a)]$. Then $|C_G(a)| < |G|$, and also $|G| = [G:C_G(a)]\,|C_G(a)|$ shows that p^k divides $|C_G(a)|$. By induction hypothesis, $C_G(a)$ has a subgroup of order p^k .

Remarks (1) It can be shown that the number of subgroups of order p^k is of the form 1 + rp , for some integer r .
(2) Two subgroups of the same order p^k in G are not necessarily isomorphic. However, if k is the largest integer such that p^k divides |G| , a subgroup of order p^k is called a *Sylow p-subgroup* (or p-Sylow subgroup) of G , and it can be shown that any two Sylow p-subgroups of G are necessarily conjugate in G , and in particular are isomorphic.
(3) It can be shown that if H is any p-subgroup of G (subgroup of order a power of p), then there exists at least one Sylow p-subgroup of G which contains H .

Example Suppose G is a group of order pq^b , where p and q are prime numbers, and p < q . Then G has a Sylow q-subgroup H , and the index of H in G is p . Since p is the smallest prime divisor of |G| , H is a normal subgroup of G , so G is not a simple group. A famous (among group-theorists) theorem of Burnside (1911) shows that a group of order $p^a q^b$ cannot be simple.

Homework

1. Let a be an element of a group G . Show that the following are equivalent:

(1) The conjugacy class $cl_G(a)$ of a in G consists of just one element.

(2) The centralizer $C_G(a)$ of a in G is equal to G .

(3) a is an element of the center Z(G) of G .

2. If P is a Sylow p-subgroup of a finite group G and it happens to be a normal subgroup of G , show that every p-subgroup H of G must be contained in P . (Hint: One way to proceed is to use the natural homomorphism θ of G onto G/P . Show that θ must map H to the identity subgroup.)