CHAPTER II

GROUP ACTIONS ON SETS

1. Group Actions

Let X be a set and let G be a group. As before, we say that G *acts* on X if we have a representation $\rho : G \to S(X)$ or equivalently there is a binary operation $G \times X \to X$ satisfying the rules

$$1x = x \qquad \text{for all } x \in X,$$
$$(gh)x = g(hx) \qquad \text{for all} g, h \in G, x \in X.$$

Given such an action, define a relation on X by $x \sim y$ if and only if $\exists g \in G$ such that $y = gx$. It is not hard to see that this defines an equivalence relation on X. (See the Exercises.) It follows that X is partitioned into disjoint equivalence classes which are also called orbits. The equivalence class containing x is $Gx = \{gx \mid g \in G\}$, and is called the *orbit* of x. If there is only one orbit, the action is said to be *transitive*. This is equivalent to the assertion: for each $x, y \in G$, $\exists g \in G$ such that $y = gx$.

Since any set breaks up into a disjoint union of equivalence classes under an equivalence relation, it follows that if G acts on X, then X is a union of disjoint orbits.

Examples.

1. *Left multiplication*. Let $H \leq G$. Then G acts on $X = G/H$ by $g(xH) = (gx)H$ where $g, x \in G$. Note that if $xH = yH$ are the same coset, then $(gx)^{-1}(gy) = x^{-1}g^{-1}gy = x^{-1}y \in H$, so $(gx)H = (gy)H$. In other words, this action is well defined. It is also clear that $1(xH) = xH$ and $(gh)(xH) = g(h(xH))$, so it does define an action. Let $\overline{1}$ denote the trivial coset H. Then clearly $X = G\overline{1}$ so the action is transitive.

2. *Conjugation*. Let $X = G$ and let G act on itself by ${}^g x = gxg^{-1}$ where we use pre-exponential notation as indicated previously for the binary operation. The orbits of this action are called the *conjugacy* classes of G.

3. (a) More generally, let X be the set of all subsets of G (denoted in set theory by 2^G). Let G act on X by ${}^g S = gSg^{-1}$ for $S \in X$, i.e., for $S \subseteq G$. (b) Alternately, let X be the set of all *subgroups* of G and let G act the same way.

4. Let G be the group of 3×3 real, orthogonal matrices, i.e., 3×3 real matrices A such that $AA^t = A^tA = I$. It is not hard to see that the set of all such matrices forms a group, called the *orthogonal group* and denoted $O(3)$ or $O(3, \mathbf{R})$, Such matrices determine linear transformations of $\mathbf{R}^3$ with preserve lengths. Hence, we get an action of the orthogonal group $G = O(3)$ on Euclidean 3-space $\mathbf{R}^3$. The orbits are spheres centered at the origin.

Suppose G acts on the set X. For $x \in X$, we set

$$G_x = \{g \in G \mid gx = x\}.$$

G_x is a subgroup of G. For, certainly $1 \in G_x$, and if $gx = x$ and $hx = x$, it is clear that $ghx = gx = x$. Moreover, $gx = x$ implies $x = g^{-1}x$.

G_x is called the *isotropy* subgroup or *stabilizer* of x. Note that G_x is not generally a normal subgroup of G. In fact, we have

$$gG_xg^{-1} = G_{gx}.$$

For, $h \in G_{gx} \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x \Leftrightarrow h \in gG_xg^{-1}$ as claimed.

PROPOSITION. *Let G be a group acting on a set X and let $x \in X$. The mapping $gG_x \mapsto gx$ provides a one-to-one correspondence between G/G_x and Gx. Moreover, this correspondence is consistent with the actions of G on both sets. In particular, if G is finite, then $|Gx| = (G : G_x) = |G|/|G_x|$.*

PROOF. First, note that the map is well defined. For,

$$hG_x = gG_x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow g^{-1}hx = x \Leftrightarrow hx = gx.$$

In fact, this argument read backwards, shows also that the map is one-to-one. The map is clearly onto. Finally,

$$h(gG_x) = (hg)G_x \mapsto (hg)x = h(gx)$$

so the mapping is consistent with the two actions. □

COROLLARY. *If G is a finite group acting on a set X, then every orbit is a finite set and its cardinality divides the order $|G|$ of the group.*

Let G be a group, finite or infinite. Among the sets on which G acts, we may distinguish the coset spaces G/H for H a subgroup G. G acts *transitively* on such a set, and the proposition tells us that up to one-to-one action preserving correspondences, every set X on which G acts transitively may be assumed to be of this form. So up to such correspondence, any set on which G acts may be thought of as a disjoint union of coset spaces.

Let G act on X. As mentioned before, we may associate to this action a representation $\rho : G \to S(X)$. The kernel of this representation is the set of all $g \in G$ which act as the identity on all of X. That is,

$$\operatorname{Ker} \rho = \bigcap_{x \in X} G_x$$

is the intersection of all stabilizers of points in X.

Exercises.

1. Let the group G act on the set X.
   (a) Show that the relation $x \sim y$ defined in the section is an equivalence relation.
   (b) Suppose G were only a monoid but we defined the notion of G acting on X the same way. Would $\sim$ still be an equivalence relation?
2. Let the group $Gl(n, \mathbf{R})$ of all $n \times n$ invertible real matrices act on R^n the usual way where $\mathbf{R}^n$ is exhibited as the set of all $n \times 1$ column vectors. What are the orbits? For each orbit, pick a point in that orbit and describe the isotropy group. (If you pick the point properly, the description should be relatively simple.)
3. Let $O(n)$ denote the group of all $n \times n$ real orthogonal matrices, and let $O(n)$ act on $\mathbf{R}^n$ the usual way.
   (a) Show that the orbits of $O(n)$ are $n - 1$ spheres of different radii in $\mathbf{R}^n$.
   (b) What is the isotropy group of the unit vector $\mathbf{e}_1$ with first coordinate one and other coordinates zero.

2. Centralizers, Normalizers, and the Class Equation

We consider some important examples of groups acting on sets.
(1) Let G act on the set X of subsets of G by conjugation

$$^gS = gSg^{-1}.$$

The orbits of the action are families of conjugates subsets. The most interesting case is that in which the set is a subgroup H and the orbit is the set of all subgroups conjugate to H. The isotropy subgroup G_S of the subset S is also denoted

$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}$$

and is called the *normalizer* of S in G. Note that if H is a subgroup of G, then H is a subgroup of $N_G(H)$ and in fact $N_G(H)$ is the largest subgroup of G in which H is normal. (See the Exercises.) It follows from our basic proposition on the isotropy subgroup that in the case of a finite group, *the number of distinct conjugates of a given subset S is $(G : N_G(S))$, so that number divides $|G|$.*
(2) Let G act on $X = G$ by conjugation of elements: ${}^g x = gxg^{-1}$. The orbit of the element $x \in G$ is the set of all elements of G conjugate to x. The isotropy subgroup is denoted

$$C_G(x) = \{g \in G \mid gx = xg\}$$

and is called the *centralizer* of x in G. As above, the *number of distinct conjugates of an element x is $(G : C_G(x))$ so it divides $|G|$.*

The intersection of all the centralizers of elements of G is denoted

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

and is called the *center* of the group G. Note that $Z(G)$ is the kernel of the representation $\rho : G \to \mathrm{Aut}(G)$ defined by

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

THEOREM. (The class equation) *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum_{x \in T} (G : C_G(x)).$$

where T is a set of distinct representatives of the conjugacy classes of G of size larger than one.

PROOF. Let G act on itself by conjugation. Then G decomposes as a disjoint union of orbits, i.e., conjugacy classes. The number of elements in the class containing x is as above $(G : C_G(x))$. However, this index is one if and only if $G = C_G(x)$, i.e., every element of G commutes with x, i.e., $x \in Z(G)$. The above equation then just reflects the decomposition of G into this disjoint union. □

COROLLARY. *Let $|G| = p^n$ where p is a prime. Then p divides $|Z(G)|$. In particular, $Z(G)$ is not the trivial subgroup.*

PROOF. Use the class equation. The left hand side is a power of p. The terms in the sum on the right are all non-trivial divisors of p^n, so they are all divisible by p. It follows that $|Z(G)|$ is divisible by p. □

COROLLARY. *Let p be a prime. Every group of order p^2 is abelian.*

PROOF. The center Z of G has order at least p. If $|Z| = p^2$, then $G = Z$ and we are done, so assume $|Z| = p$. Then G/Z has order p. However, any group of order p is cyclic so we can choose $x \in G$ such that xZ generates G/Z. It follows that $1, x, x^2, \ldots, x^{p-1}$ is a complete set of coset representatives of Z in G. Any element $g \in G$ is in some coset so it has the form $g = x^i z$ where $z \in Z$. However, a simple computation shows that any two such elements commute, whence G is abelian. □

Exercises.

1. Let S be a subset of a group G. Define the centralizer of S by

$$C_G(S) = \{g \in G \mid gx = xg \text{ for all } x \in S\}.$$

Show that it is a subgroup of G. Can you find an interpretation of this subgroup in terms of a group action on an appropriate set?

2. Let G be a p-group. Show that every normal subgroup of order p lies in the center of G. Later, we shall show that any normal subgroup of a p-group intersects its center nontrivially. Don't use this result here.

3. Sylow Theorems

Let p be a prime. A finite group G of order p^k is called a p-group. If $|G| = p^a n'$ where n' is relatively prime to p, then any subgroup of order p^a is called a *p-Sylow subgroup* of G. Such subgroups of course are those p-subgroups of G of maximal possible order. The p-Sylow subgroups of a finite groups for the different primes p dividing the order $|G|$ play an important role in determining the structure of the group. In this section, we explore some of the important facts about p-Sylow subgroups.

We start with a generalization of the argument used to derive the class equation. Let G act on the set X. The subset

$$X^G = \{x \in X \mid gx = x \quad \text{for all } g \in G\}$$

of X is called the *fixed point set* of the action. It may also be viewed as the union of all single element orbits, i.e., orbits for which $(G : G_x) = 1$. Let T be a set of distinct representatives of the orbits of size greater than one.

PROPOSITION. *With the notation as above, X can be decomposed as as disjoint union*

$$X = X^G \cup \bigcup_{x \in T} Gx.$$

If X is finite, then

$$|X| = |X^G| + \sum_{x \in T} (G : G_X). \tag{A}$$

PROOF. Apply the same reasoning used to derive the class equation. □

COROLLARY. *Let G be a finite p-group acting on a finite set X. Then*

$$|X| \equiv |X^G| \bmod p.$$

PROOF. Take the cardinalities of the sets on both sides of the equation (A). On the right, each term except the first is divisible by p. (Note this is just a generalization of the argument that the center of a p-group is non-trivial.) □

We are now ready to state and prove the basic result of this section.

THEOREM. (Sylow) *Let G be a finite group and suppose p is prime. Let $n = |G| = p^a n'$ where $(n', p) = 1$.*

(a) There exists a subgroup P of G of order p^a (so P is a p-Sylow subgroup.)

(b) Let P be a p-Sylow subgroup of G, and let H be any p-subgroup of G. Then $\exists g \in G$ such that $gHg^{-1} \leq P$. In particular, any two p-Sylow subgroups of G are necessarily conjugate.

(c) The number k of p-Sylow subgroups of G is a divisor of n', and also $k \equiv 1$ mod p.

PROOF. If $a = 0$, the facts are clear so we assume $a > 0$, i.e., p divides $|G|$.

(a) Let X be the set of all subsets S of G with exactly p^a elements. We have $|X| = \binom{n}{p^a}$ which is the number of ways to pick p^a objects from n objects. However, this number is also a binomial coefficient, in particular, it is the coefficient of the p^ath power of t in

$$(1 + t)^n = (1 + t)^{p^a n'}.$$

However,

$$(1 + t)^p \equiv 1 + t^p \mod p$$

in the sense that coefficients of corresponding powers of t are congruent. (The simplest way to prove this is to note that the binomial coefficients $\binom{p}{i} = p!/(p - i)!i!$ are divisible by p for $i = 1, 2, \ldots, p - 1$.) Hence, iteration yields

$$(1 + t)^n \equiv (1 + t^{p^a})^{n'} \mod p$$

and the term on the right expanded yields

$$= 1 + n't^{p^a} + \text{higher powers of } t.$$

Expanding directly on the left and comparing coefficients of corresponding powers of t yields

$$\binom{n}{p^a} \equiv n' \mod p$$

which is not divisible by p. So $|X|$ is relatively prime to p.

If S is an element of X, i.e. $|S| = p^a$, then the set

$$gS = \{gy \,|\, y \in S\}$$

is also a subset with $|gS| = p^a$. It is not hard to see that this defines an action of the group G on the set X. Use

$$|X| = \sum (G : G_S)$$

where the summation is taken over a collection of representative subsets S with p^a elements. The left hand side is not divisible by p, so there is at least one orbit of size not divisible by p, i.e., there is at least one subset S with p^a elements such that p does not divide $(G : G_S)$. Let $s \in S$. Since for $g \in G_S$ we have $gS = S$, it follows that $G_S s \subseteq S$ so that $G_S \subseteq Ss^{-1}$. Hence $|G_S| \leq |Ss^{-1}| = p^a$. Since $|G|/|G_S| = (G : G_S)$ is not divisible by p, it follows that $|G_S| = p^a$ so we have found the desired p-Sylow subgroup.

(b) Let P be a p-Sylow subgroup and let H be any p-subgroup of G. Let H act on $Y = G/P$ by left multiplication: $h(gP) = (hg)P$. Since H is a p-group, we have as above

$$n' = |Y| \equiv |Y^H| \mod p,$$

and since the left hand side is not divisible by p, it follows that there is at least one element in Y^H. Thus, there is a coset xP such that $H(xP) = xP$. Hence, $Hx \subseteq HxP = xP$, so $x^{-1}Hx \leq P$ as claimed.

(c) Let $N = N_G(P)$. Since $G \geq N \geq P$, it follows that $(G : N)$ divides $(G : P) = n'$. On the other hand, $(G : N)$ is the number of conjugates of P is by our previous theory. Let $W = G/N$ and let P act on W by left multiplication as above. Then,

$$(G : N) = |W| \equiv |W^P| \mod p.$$

However, a coset $gN \in W^P$ if and only if $zgN = gN$ for every $z \in P$. This in turn implies that $g^{-1}zg \in N$ for every $z \in P$, i.e., that $g^{-1}Pg \leq N$. However, in that case P and $g^{-1}Pg$ are both p-subgroups of N of maximal order, so they are p-Sylow subgroups of N. By (b) applied to N, they are conjugate by an element $u \in N$. But, P is normal in N, so it is the *only* conjugate of itself in N and $P = g^{-1}Pg$. Thus, $g \in N$ (which is the normalizer of P), so $gN = N$. The upshot of this argument is that N is the only coset of N fixed by P and $|W^P| = 1$ as required. □

Example. We illustrate Sylow's Theorem by determining all groups of order 12.

Each such group G has a 2-Sylow subgroup of order 4 and a 3-Sylow subgroup of order 3. The number of 2-Sylow subgroups is clearly 1 or 3 since these are the only divisors of $n' = 3$ which are congruent to 1 mod 2. Similarly, the number of 3-Sylow subgroups is either 1 or 4. Each 3-Sylow subgroup is cyclic of order 3, and the 2-Sylow subgroups are all cyclic of order 4 or are isomorphic to the Klein 4-group (the direct product of two cyclic groups of order 2.)

Assume G has four 3-Sylow subgroups. Since each such subgroup has order 3, it follows that any two of them intersect only in the trivial subgroup. Hence, the number of elements in the union of all the 3-Sylow subgroups exclusive of 1 is $4 \times 2 = 8$. That means there are only 4 remaining elements (including 1) so that there is only one 2-Sylow subgroup. Let H be the unique 2-Sylow subgroup. Since every conjugate of H is H, it follows that H is normal. Let K be any of the four 3-Sylow subgroups. Since $H \cap K = \{1\}$ (by

order considerations), it follows that $|HK| = |H||K| = 12$ so $G = HK$, and from an exercise we know that G is isomorphic to the semidirect product $K \rtimes H$. The only remaining item of data is the homomorphism $\alpha : K \to \text{Aut}(H)$. Since K is cyclic of order 3, the image of α has order 1 or 3. In the former case, we would have $\alpha(k)(h) = khk^{-1} = h$ for all $k \in K$ and $h \in H$ so that in fact the product would be the direct product. However, that would imply that K is also a normal subgroup of G which is not consistent with the existence of 4 conjugates of K. Hence, the image of α in $\text{Aut}(H)$ has order 3.

Choose x such that $K = \langle x \rangle$. Assume first that H is cyclic of order 4 with generator y. Then $\alpha(x)(y) = xyx^{-1} = y^i$ where $0 < i < 4$ and i is odd. However, it is easy to see that $i^3 \equiv 1 \mod 4$ (since $\alpha(x)^3 = id$), and the only i with that property is $i = 1$. In that case $\alpha(x)$ is trivial contrary to our assumption. Hence it follows that H is not cyclic and must be isomorphic to the Klein 4-group. Choose any nontrivial element u in H. Let $v = \alpha(x)(u)$ and let $\alpha(x^2)(u) = w$. It is easy to see that these elements must be different and hence constitute the three nontrivial elements of H—all of order 2. We have now shown there is at most one group of order 12 with four 3-Sylow subgroups. Conversely, it is easy to see that cyclic permutation of the 3 nontrivial elements of the 4-group is in fact an automorphism so we may construct such a group by taking the appropriate semi-direct product.

Assume next that there is exactly one 3-Sylow subgroup which we denote by K. If there is exactly one 2-Sylow subgroup H, both Sylow groups are normal, and it is easy to see as above that G must be isomorphic to the direct product $K \times H$. There are two possibilities depending on whether H is cyclic of order 4 or is the Klein 4-group.

Assume instead that there are exactly three 2-Sylow subgroups and let H be one of them. In that case $G \cong H \rtimes K$ where the homomorphism $\alpha : H \to \text{Aut}(K)$ is definitely non-trivial. Let $K = \langle x \rangle$. The only nontrivial automorphism of K is defined by $x \mapsto x^2$. Hence, all that remains is to investigate the possible homomorphisms of the two possibilities for H onto $\text{Aut}(K)$ which by the above observation is cyclic of order 2. Up to isomorphism, there is one possibility for each possible structure for H. We leave an investigation of the details for an exercise.

It follows from the above discussion that there are five non-isomorphic groups of order 12. (One of these is the alternating group A_4, which shall be discussed later.)

Exercises.

1. Let G be a group with order divisible by p. Prove that G has an element of order p.
2. Let G have order pq where p and q are primes with $p < q$. Show that G has a normal cyclic subgroup $Q = \langle x \rangle$ of order Show also that G has a cyclic subgroup $P = \langle y \rangle$ of order p and $yxy^{-1} = x^i$ where $i = 1, 2, \ldots,$ or $q - 1$. Show that $G \cong P \ltimes Q$ and that the product is in fact the direct product if p does not divide $q - 1$.
3. Let P be a p-Sylow subgroup of the finite group G. Show that $N_G(N_G(P)) = N_G(P)$.
4. Let p be a prime. An infinite group is called a p-group if every element has order a power of p Show that a finite group with this property has order a power of p.

4. Theorems on p-groups

Because of the Sylow theorems, the problem of analyzing the structure of a finite group may be thought of as having two parts. First we may try to determine the structure of its p-Sylow subgroups for different primes, and then we may try to see how these subgroups fit together to form the whole group. Classifying p-groups is in fact quite difficult, but there is a lot known about such groups. In this section, we describe some of these basic facts.

THEOREM. *Let G be a p-group and let K be a normal subgroup of G. Then $Z(G) \cap K$ is nontrivial.*

PROOF. Let G act on K by conjugation. We have

$$|K| \equiv |K^G| \mod p.$$

The left hand side is certainly divisible by p, and the right hand side is not zero, so K^G is non-trivial. But, $K^G = K \cap Z(G)$. $\square$

THEOREM. *Let G be a p-group and let H be a proper subgroup. Then H is strictly contained in $N_G(H)$.*

PROOF. Let H act on $X = G/H$ by left multiplication. We have

$$\begin{aligned} xH \in X^H &\Leftrightarrow HxH = xH \Leftrightarrow Hx \subseteq xH \\ &\Leftrightarrow H \subseteq xHx^{-1} \Leftrightarrow H = xHx^{-1} \Leftrightarrow x \in N_G(H). \end{aligned}$$

It follows that X^H consists of the co-sets of H in $N_G(H)$. Hence,

$$(N_G(H) : H) = |X^H| \equiv |X| \mod p,$$

and since $|X| = (G : H)$ is divisible by p, it follows that $(N_G(H) : H) > 1$ as claimed. □

THEOREM. *Let G be a p-group. A subgroup H of G is a maximal proper subgroup if and only if it is of index p. Every such subgroup is normal.*

PROOF. Clearly any subgroup H with $(G : H) = p$ is a maximal proper subgroup since any larger subgroup would have index dividing p. Conversely, let H be any maximal proper subgroup. By the previous theorem, $H < N_G(H)$, so by maximality, $N_G(H) = G$. Thus, H is normal in G. Consider the factor group G/H, and let $\tilde{Z}$ be any proper nontrivial subgroup. Since $\tilde{Z} < G/H$, by the third isomorphism theorem, we may pull $\tilde{Z}$ back to a proper subgroup Z of G strictly containing H, which was assumed to be maximal. Hence, G/H does not have any proper nontrivial subgroups. Hence, it is cyclic of prime order. (See the Exercises.) □

Exercises.

1. Let G be a non-cyclic p-group. Show that G contains at least two distinct maximal subgroups. Hint: Choose a cyclic normal subgroup of order p, and use induction.

5. Symmetric Groups

Recall that we have denoted by S_n the group of all bijections or permutations of the set $X = \{1, 2, 3, \ldots, n\}$ with composition of functions the binary operation. The study of permutation groups has a long history, and certain special concepts which play an important role will be introduced in this section.

Suppose $\{x_1, x_2, \ldots, x_k\}$ is an ordered subset of X but where the elements are not necessarily listed in the usual order. Let $\{y_1, y_2, \ldots, y_{n-k}\}$ be a listing of the remaining elements of X. The permutation

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_k & y_1 & \ldots & y_{n-k} \\ x_2 & x_3 & \ldots & x_1 & y_1 & \ldots & y_{n-k} \end{pmatrix}$$

is called a *cycle of length k*, and it is denoted

$$(x_1\, x_2\, \ldots\, x_k).$$

The notational description of a cycle can be altered to start with any element in the list, as long as the 'cyclic order' is preserved.

For example, for $n = 5$,

$$(2\,4\,3) = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$$

is a cycle of length 3, but we also have

$$(2\,4\,3) = (4\,3\,2) = (3\,2\,4).$$

A cycle clearly has order equal to its length. Two cycles are said to be *disjoint* provided the sets of elements they actually move are disjoint. Clearly, disjoint cycles commute. We sometimes use the notation (i) to stand for the identity where i is any element of the set $\{1, 2, \ldots, n\}$. In other words, all cycles of length one represent the identity.

LEMMA. *Let $\sigma \in S_n$. σ may be written as a product (composition) of disjoint cycles. Except for the order of the factors, such a product is unique.*

PROOF. Consider the action of the subgroup $\langle\sigma\rangle$ on $\{1, 2, \ldots, n\}$. The set breaks up into a disjoint union of orbits, and associated with each orbit is a cycle: if i is in the orbit, take the cycle

$$i \mapsto \sigma(i) \mapsto \sigma^2(i) \mapsto \cdots .$$

It is fairly clear that the product of these cycles has exactly the same effect on $\{1, 2, \ldots, n\}$ as σ. Also, given a product of disjoint cycles, it is easy to see that its orbits are just the sets in the cycles. Hence the representation is unique. □

Example. In S_5, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (1\,2)(3)(4\,5)$$

We could have omitted (3) from the above decomposition since it just stands for the identity, but is is usual to include such terms so that we can see where all the elements go.

PROPOSITION. *σ and $\tau \in S_n$ are conjugate if and only if their decompositions into disjoint cycles can be put in one to one correspondence so that corresponding cycles have the same length.*

PROOF. Let $\tau = \beta\sigma\beta^{-1}$. Then, we also have $\tau^j = \beta\sigma^j\beta^{-1}$. Hence, $\tau^j(\beta(i)) = \beta(\sigma^j(i))$ for $i = 1, 2, \ldots, n$. Thus, the orbits of the cyclic group $\langle\sigma\rangle$ are carried by β into the orbits of the cyclic group $\langle\tau\rangle$. Since in either case, these orbits correspond to the cycles in the cyclic decomposition, this establishes the proposition. For, if we start with conjugate elements, we may use β to establish the desired correspondence. Conversely, if we start with such a correspondence, we may use it to construct an appropriate β. □

A cycle of length 2 is called a *transposition.*

PROPOSITION. *Every permutation can be written as a product of transposition.*

PROOF. In view of the previous proposition, it suffices to prove that for cycles. In fact,

$$(1 \cdots k) = (k-1\,k)(k-2\,k)\cdots(2\,k)(1\,k)$$

and similarly for other cycles with different cyclic orders. □

Permutations are used in many applications. One such application is the general formula for the determinant of an $n \times n$ matrix. One important concept which is needed in such applications is the *sign* of a permutation. We develop this concept by a somewhat indirect approach.

Let F denote the set of real valued functions $f(x_1, \ldots, x_n)$ of n real variables. We let $\sigma \in S_n$ permute the variables by permuting the indices. For $f \in F$ define $\sigma f = f \circ \sigma^{-1}$, i.e.,

$$(\sigma f)(x_1, x_2, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)}).$$

It is easy to check that

$$(*) \qquad (\sigma\tau)f = \sigma(\tau f) \qquad \text{for } \sigma, \tau \in S_n.$$

Define

$$h(x_1, x_2, \ldots, x_n) = \prod_{i<j}(x_i - x_j).$$

For each $\sigma \in S_n$, we clearly have $\sigma h = \pm h$, and we define $\mathrm{Sgn}(\sigma)$ (called the *sign* of σ) to be 1 or -1 accordingly. From the formula (*) above, it is clear that

$$\mathrm{Sgn}(\sigma\tau) = \mathrm{Sgn}(\sigma)\ \mathrm{Sgn}(\tau) \qquad \text{for } \sigma, \tau \in S_n.$$

In other words, $\mathrm{Sgn} : S_n \to \{1, -1\}$ (forming a group of order 2 under multiplication) is a homomorphism.

PROPOSITION. *If τ is a transposition, then Sgn$(\tau) = -1$.*

PROOF. Let $\tau = (k\,l)$, where $k < l$, and look at the terms in the product defining h. Those terms not involving k or l are unaffected. The term $x_k - x_l$ has its sign reversed. $x_i - x_k$ and $x_i - x_l$ with $i < k$ are interchanged, and $x_k - x_j$ and $x_l - x_j$ with $l < j$ are interchanged. Hence the only terms to worry about are $x_k - x_i$ and $x_i - x_l$ with $k < i < l$. These terms are interchanged and their signs are both changed. Hence the net sign change from the transposition is -1. □

THEOREM. *The parity (even or odd) of the number of transposition in a decomposition of an element $\sigma \in S_n$ depends only only on σ not on the decomposition as a product of transpositions.*

PROOF. Sgn$(\sigma) = (-1)^k$ where k is the number of transpositions in a decomposition $\sigma = \tau_1\tau_2\cdots\tau_k$. □

It follows from the above discussion, that the set of even transpositions is a normal subgroup of S_n. (It is Ker Sgn.) We call this subgroup the *alternating* group of degree n, and we denote it A_n. Since $|S_n/A_n| = 2$, it follows that $|A_n| = n!/2$.

It is an important fact that except for $n = 4$, A_n does not have any proper, nontrivial, normal subgroups of its own. We shall now aim towards a proof of this fact.

PROPOSITION. *The alternating group A_n is generated by all 3-cycles of the form $(1\,2\,i)$.*

PROOF. Note that in general, a cycle is even if an only if its length is odd. For $n = 3$ the only even cycles are $(1\,2\,3)$ and $(1\,3\,2) = (1\,2\,3)^2 = (1\,2\,3)^{-1}$. Every other nontrivial element of S_3 is a transposition. Hence, $A_3 = \{id, (1\,2\,3), (1\,3\,2)\}$.

Suppose $n > 3$. Let $\sigma \in A_n$, and let $m = \sigma(n)$. Then $(1\,n\,2)(1\,2\,m)\sigma$ fixes n since

$$n \mapsto m \mapsto 1 \mapsto n.$$

Hence, $(1\,n\,2)(1\,2\,m)\sigma$ may be identified with an element of A_{n-1}. Since $(1\,n\,2) = (1\,2\,n)^{-1}$, it follows inductively that A_n is generated by elements of the desired type. □

THEOREM. *Except in the case $n = 4$, A_n has no normal subgroups except itself and the trivial subgroup.*

PROOF. The case $n = 3$ was dealt with in the proof of the above proposition so we may assume $n \geq 5$.

Let N be a nontrivial normal subgroup of A_n. By the above proposition, it suffices to show that N contains all cycles of the form $(1\,2\,i)$. Choose $\alpha \in N$ not equal to the identity so that the fixed point set of α is as large as possible. Suppose the fixed point set of α has $n - k$ elements where $0 < k \leq n$ so that α moves k elements. Since any non-identity element moves at least two elements and since α is not a transposition, we must have $k > 2$.

If $k = 3$, then $\alpha = (a\,b\,c)$ is a 3-cycle. However,

$$(a\,b)(c\,d)(a\,b\,c)(c\,d)(a\,b) =$$
$$(a\,b)(a\,b\,d)(a\,b) = (b\,a\,d) = (a\,b\,d)^{-1}.$$

So, if $(a\,b\,c) \in N$, it follows that $(a\,b\,d) \in N$ where $d \neq a, b, c$. Thus, if $(a\,b\,c) \in N$, it follows that $(a\,b\,1) = (1\,a\,b) \in N$ and similarly $(1\,2\,b) = (1\,b\,2)^{-1} \in N$, and finally $(1\,2\,i) \in N$ for $2 < i \leq n$. In this case, the proposition tells us that $N = A_n$.

Suppose $k > 3$. Assume first that in the cyclic decomposition of α there is at least one cycle of length 3 or more. If $k = 4$, then in this case $\alpha = (a\,b\,c\,d)$ must be a 4-cycle (since it can't be a product of 2 disjoint transpositions.) However, every 4-cycle is odd and does not belong to A_n. Hence, $k > 4$. Let a, b, c, d, e be 5 elements moved by α, and assume a, b, and c are successive elements in the cycle in α of length ≥ 5. Let

$$\alpha_1 = \beta\alpha\beta^{-1} \in N \text{ where } \beta = (c\,d\,e).$$

We have $\alpha_1(\beta(x)) = \beta(\alpha(x))$. Suppose $\alpha(x) = x$. Since we have assumed α moves c, d, and e, we know x is not one of these, hence $\beta(x) = x$, and it follows that $\alpha_1(x) = x$. In other words, the fixed point set

of α_1 contains the fixed point set of α. From the definition of α_1, it is clear that α and α_1 have the same effect on b (since $\alpha(a) = b$ and β fixes both a and b.) Hence, $\gamma = \alpha_1\alpha^{-1}$ which fixes everything α_1 fixes also fixes b. Hence, the fixed point set of γ is larger than the fixed point set of α. Since $\alpha(b) = c$ and $\alpha_1(b) = d$, $\gamma = \alpha_1\alpha^{-1} \neq id$ so we have a contradiction to the choice of α. We conclude in the present case that $k \leq 4$, and we have already dealt with that.

Assume next that α does not have any cycle of length 3 or larger, i.e., assume that α is a product of disjoint transpositions. Since $k > 3$, we may assume $\alpha = (ab)(cd)\ldots$. Let $\beta = (c\,d\,e)$ where e is different from a, b, c, and d. (That is acceptable since $n > 4$.) Let $\alpha_1 = \beta\alpha\beta^{-1}$. If $\alpha(e) = e$, it is easy to see that α_1 and α have the same effect on everything except c and d. It follows that $\gamma = \alpha_1\alpha^{-1} = (d\,e)(c\,d) = (c\,e\,d)$, so N contains a 3-cycle, and as above it contains A_n. Suppose then that α moves e. In that case we can repeat the argument in the previous paragraph to show that $\gamma = \alpha_1\alpha^{-1}$ has a larger fixed point set than α. However, $\alpha_1(d) = e$ and $\alpha(d) = c$ so $\gamma \neq id$. Hence, we have a contradiction, and it follows that there is no e moved by α which case was already dealt with above. □

Exercises.

1. How many ways can one describe a cycle of length k using the standard notation?

2. Prove for $n \geq 5$ that the only normal subgroup of S_n is A_n.

3. (a) Analyze A_5 using Sylow's Theorem, the fact that it is has no nontrivial proper normal subgroups and anything else you can think of.

(b) Show that the only group of order 60 without proper nontrivial normal subgroups (up to isomorphism) is A_5. Possible hint? Can you show it has to have a subgroup of index 5?

4. In the above discussion, we obtained the Klein four group V as a subgroup of A_4. The Cayley representation of V uses left multiplication to define a monomorphism $\rho : V \to S_4$ if we order the elements of V to place them in one to one correspondence with $\{1, 2, 3, 4\}$. Show that the image of this monomorphism is the subgroup described above.