24. Find the second permutation representation of S_3. Verify directly from the permutations obtained here and in Problem 20 that $\lambda_a\tau_b = \tau_b\lambda_a$ for all $a, b \in S_3$.

25. Find the second permutation representation of the group G defined in Problem 21.

26. Find the second permutation representation of the dihedral group of order $2n$.

If H is a subgroup of G, let us call the mapping $\{t_g \mid g \in G\}$ defined in the discussion preceding Theorem 2.9.2 the *coset representation* of G by H. This also realizes G as a group of permutations, but not necessarily isomorphically, merely homomorphically (see Theorem 2.9.2).

27. Let $G = (a)$ be a cyclic group of order 8 and let $H = (a^4)$ be its subgroup of order 2. Find the coset representation of G by H.

28. Let G be the dihedral group of order $2n$ generated by elements a, b such that $a^2 = b^n = e$, $ab = b^{-1}a$. Let $H = \{e, a\}$. Find the coset representation of G by H.

29. Let G be the group of Problem 21 and let $H = \{e, \theta\}$. Find the coset representation of G by H.

30. Let G be S_n, the symmetric group of order n, acting as permutations on the set $\{1, 2, \ldots, n\}$. Let $H = \{\sigma \in G \mid n\sigma = n\}$.
    (a) Prove that H is isomorphic to S_{n-1}.
    (b) Find a set of elements $a_1, \ldots, a_n \in G$ such that $Ha_1, \ldots, Ha_n$ give all the right cosets of H in G.
    (c) Find the coset representation of G by H.

2.11 Another Counting Principle

Mathematics is rich in technique and arguments. In this great variety one of the most basic tools is counting. Yet, strangely enough, it is one of the most difficult. Of course, by counting we do not mean the creation of tables of logarithms or addition tables; rather, we mean the process of precisely accounting for all possibilities in highly complex situations. This can sometimes be done by a brute force case-by-case exhaustion, but such a routine is invariably dull and violates a mathematician's sense of aesthetics. One prefers the light, deft, delicate touch to the hammer blow. But the most serious objection to case-by-case division is that it works far too rarely. Thus in various phases of mathematics we find neat counting devices which tell us exactly how many elements, in some fairly broad context, satisfy certain conditions. A great favorite with mathematicians is the process of counting up a given situation in two different ways; the comparison of the two counts is then used as a means of drawing conclusions. Generally speaking, one introduces an equivalence relation on a finite set, measures the size of the equivalence classes under this relation, and then equates the number of elements in the set to the sum of the orders of these equivalence classes. This kind of an approach will be illustrated in this section. We shall introduce a relation, prove it is an equivalence relation, and then find a neat algebraic description for the size of each equivalence class. From this simple description there will flow a stream of beautiful and powerful results about finite groups.

DEFINITION If $a, b \in G$, then b is said to be a *conjugate* of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$.

We shall write, for this, $a \sim b$ and shall refer to this relation as *conjugacy*.

LEMMA 2.11.1 *Conjugacy is an equivalence relation on G.*

Proof. As usual, in order to establish this, we must prove that

1. $a \sim a$;
2. $a \sim b$ implies that $b \sim a$;
3. $a \sim b$, $b \sim c$ implies that $a \sim c$

for all a, b, c in G.

We prove each of these in turn.

1. Since $a = e^{-1}ae$, $a \sim a$, with $c = e$ serving as the c in the definition of conjugacy.
2. If $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$, hence, $a = (x^{-1})^{-1}b(x^{-1})$, and since $y = x^{-1} \in G$ and $a = y^{-1}by$, $b \sim a$ follows.
3. Suppose that $a \sim b$ and $b \sim c$ where $a, b, c \in G$. Then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$; since $xy \in G$, $a \sim c$ is a consequence.

For $a \in G$ let $C(a) = \{x \in G \mid a \sim x\}$. $C(a)$, the equivalence class of a in G under our relation, is usually called the *conjugate class* of a in G; it consists of the set of all distinct elements of the form $y^{-1}ay$ as y ranges over G.

Our attention now narrows to the case in which G is a finite group. Suppose that $C(a)$ has c_a elements. We seek an alternative description of c_a. Before doing so, note that $o(G) = \sum c_a$ where the sum runs over a set of $a \in G$ using one a from each conjugate class. This remark is, of course, merely a restatement of the fact that our equivalence relation—conjugacy—

induces a decomposition of G into disjoint equivalence classes—the conjugate classes. Of paramount interest now is an evaluation of c_a.

In order to carry this out we recall a concept introduced in Problem 13, Section 2.5. Since this concept is important—far too important to leave to the off-chance that the student solved the particular problem—we go over what may very well be familiar ground to many of the readers.

DEFINITION If $a \in G$, then $N(a)$, the *normalizer of a in G*, is the set $N(a) = \{x \in G \mid xa = ax\}$.

$N(a)$ consists of precisely those elements in G which commute with a.

LEMMA 2.11.2 *$N(a)$ is a subgroup of G.*

Proof. In this result the order of G, whether it be finite or infinite, is of no relevance, and so we put no restrictions on the order of G.

Suppose that $x, y \in N(a)$. Thus $xa = ax$ and $ya = ay$. Therefore, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, in consequence of which $xy \in N(a)$. From $ax = xa$ it follows that $x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$, so that x^{-1} is also in $N(a)$. But then $N(a)$ has been demonstrated to be a subgroup of G.

We are now in a position to enunciate our counting principle.

THEOREM 2.11.1 *If G is a finite group, then $c_a = o(G)/o(N(a))$; in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.*

Proof. To begin with, the conjugate class of a in G, $C(a)$, consists exactly of all the elements $x^{-1}ax$ as x ranges over G. c_a measures the number of distinct $x^{-1}ax$'s. Our method of proof will be to show that two elements in the same right coset of $N(a)$ in G yield the same conjugate of a whereas two elements in different right cosets of $N(a)$ in G give rise to different conjugates of a. In this way we shall have a one-to-one correspondence between conjugates of a and right cosets of $N(a)$.

Suppose that $x, y \in G$ are in the same right coset of $N(a)$ in G. Thus $y = nx$, where $n \in N(a)$, and so $na = an$. Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax$, whence x and y result in the same conjugate of a.

If, on the other hand, x and y are in different right cosets of $N(a)$ in G we claim that $x^{-1}ax \neq y^{-1}ay$. Were this not the case, from $x^{-1}ax = y^{-1}ay$ we would deduce that $yx^{-1}a = ayx^{-1}$; this in turn would imply that $yx^{-1} \in N(a)$. However, this declares x and y to be in the same right coset of $N(a)$ in G, contradicting the fact that they are in different cosets. The proof is now complete.

COROLLARY

$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

where this sum runs over one element a in each conjugate class.

Proof. Since $o(G) = \sum c_a$, using the theorem the corollary becomes immediate.

The equation in this corollary is usually referred to as the *class equation* of G. Before going on to the applications of these results let us examine these concepts in some specific group. There is no point in looking at abelian groups because there two elements are conjugate if and only if they are equal (that is, $c_a = 1$ for every a). So we turn to our familiar friend, the group S_3. Its elements are e, $(1, 2)$, $(1, 3)$, $(2, 3)$, $(1, 2, 3)$, $(1, 3, 2)$. We enumerate the conjugate classes:

$$C(e) = \{e\}$$

$$\begin{aligned} C(1, 2) &= \{(1, 2), (1, 3)^{-1}(1, 2)(1, 3), (2, 3)^{-1}(1, 2)(2, 3), \\ &\qquad (1, 2, 3)^{-1}(1, 2)(1, 2, 3), (1, 3, 2)^{-1}(1, 2)(1, 3, 2)\} \\ &= \{(1, 2), (1, 3), (2, 3)\} \quad \text{(Verify!)} \end{aligned}$$

$$C(1, 2, 3) = \{(1, 2, 3), (1, 3, 2)\} \quad \text{(after another verification).}$$

The student should verify that $N((1, 2)) = \{e, (1, 2)\}$ and $N((1, 2, 3)) = \{e, (1, 2, 3), (1, 3, 2)\}$, so that $c_{(1,2)} = \frac{6}{2} = 3$, $c_{(1,2,3)} = \frac{6}{3} = 2$.

Applications of Theorem 2.11.1

Theorem 2.11.1 lends itself to immediate and powerful application. We need no artificial constructs to illustrate its use, for the results below which reveal the strength of the theorem are themselves theorems of stature and importance.

Let us recall that the center $Z(G)$ of a group G is the set of all $a \in G$ such that $ax = xa$ for all $x \in G$. Note the

SUBLEMMA *$a \in Z$ if and only if $N(a) = G$. If G is finite, $a \in Z$ if and only if $o(N(a)) = o(G)$.*

Proof. If $a \in Z$, $xa = ax$ for all $x \in G$, whence $N(a) = G$. If, conversely, $N(a) = G$, $xa = ax$ for all $x \in G$, so that $a \in Z$. If G is finite, $o(N(a)) = o(G)$ is equivalent to $N(a) = G$.

APPLICATION 1

THEOREM 2.11.2 *If $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.*

Proof. If $a \in G$, since $N(a)$ is a subgroup of G, $o(N(a))$, being a divisor of $o(G) = p^n$, must be of the form $o(N(a)) = p^{n_a}$; $a \in Z(G)$ if and only if $n_a = n$. Write out the class equation for this G, letting $z = o(Z(G))$. We get $p^n = o(G) = \sum(p^n/p^{n_a})$; however, since there are exactly z elements such that $n_a = n$, we find that

$$p^n = z + \sum_{n_a < n} \frac{p^n}{p^{n_a}}.$$

Now look at this! p is a divisor of the left-hand side; since $n_a < n$ for each term in the $\sum$ of the right side,

$$p \,\Big|\, \frac{p^n}{p^{n_a}} = p^{n-n_a}$$

so that p is a divisor of each term of this sum, hence a divisor of this sum. Therefore,

$$p \,\Big|\, \left(p^n - \sum_{n_a<n} \frac{p^n}{p^{n_a}}\right) = z.$$

Since $e \in Z(G)$, $z \neq 0$; thus z is a positive integer divisible by the prime p. Therefore, $z > 1$! But then there must be an element, besides e, in $Z(G)$! This is the contention of the theorem.

Rephrasing, the theorem states that a group of prime-power order must always have a nontrivial center.

We can now simply prove, as a corollary for this, a result given in an earlier problem.

COROLLARY *If $o(G) = p^2$ where p is a prime number, then G is abelian.*

Proof. Our aim is to show that $Z(G) = G$. At any rate, we already know that $Z(G) \neq (e)$ is a subgroup of G so that $o(Z(G)) = p$ or p^2. If $o(Z(G)) = p^2$, then $Z(G) = G$ and we are done. Suppose that $o(Z(G)) = p$; let $a \in G$, $a \notin Z(G)$. Thus $N(a)$ is a subgroup of G, $Z(G) \subset N(a)$, $a \in N(a)$, so that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) \mid o(G) = p^2$. The only way out is for $o(N(a)) = p^2$, implying that $a \in Z(G)$, a contradiction. Thus $o(Z(G)) = p$ is not an actual possibility.

APPLICATION 2 We now use Theorem 2.11.1 to prove an important theorem due to Cauchy. The reader may remember that this theorem was already proved for abelian groups as an application of the results developed in the section on homomorphisms. In fact, we shall make use of this special case in the proof below. But, to be frank, we shall prove, in the very next section, a much stronger result, due to Sylow, which has Cauchy's theorem as an immediate corollary, in a manner which completely avoids Theorem 2.11.1. To continue our candor, were Cauchy's theorem itself our ultimate and only goal, we could prove it, using the barest essentials of group theory, in a few lines. [The reader should look up the charming, one-paragraph proof of Cauchy's theorem found by McKay and published in the *American Mathematical Monthly*, Vol. 66 (1959), page 119.] Yet, despite all these counter-arguments we present Cauchy's theorem here as a striking illustration of Theorem 2.11.1.

THEOREM 2.11.3 (Cauchy) *If p is a prime number and $p \mid o(G)$, then G has an element of order p.*

Proof. We seek an element $a \neq e \in G$ satisfying $a^p = e$. To prove its existence we proceed by induction on $o(G)$; that is, we assume the theorem to be true for all groups T such that $o(T) < o(G)$. We need not worry about starting the induction for the result is vacuously true for groups of order 1.

If for any subgroup W of G, $W \neq G$, were it to happen that $p \mid o(W)$, then by our induction hypothesis there would exist an element of order p in W, and thus there would be such an element in G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G. In particular, if $a \notin Z(G)$, since $N(a) \neq G$, $p \nmid o(N(a))$. Let us write down the class equation:

$$o(G) = o(Z(G)) + \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}.$$

Since $p \mid o(G)$, $p \nmid o(N(a))$ we have that

$$p \,\Big|\, \frac{o(G)}{o(N(a))},$$

and so

$$p \,\Big|\, \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))};$$

since we also have that $p \mid o(G)$, we conclude that

$$p \,\Big|\, \left(o(G) - \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}\right) = o(Z(G)).$$

$Z(G)$ is thus a subgroup of G whose order is divisible by p. But, after all, we have assumed that p is not a divisor of the order of any proper subgroup of G, so that $Z(G)$ cannot be a proper subgroup of G. We are forced to accept the only possibility left us, namely, that $Z(G) = G$. But then G is abelian; now we invoke the result already established for abelian groups to complete the induction. This proves the theorem.

We conclude this section with a consideration of the conjugacy relation in a specific class of groups, namely, the symmetric groups S_n.

Given the integer n we say the sequence of positive integers $n_1, n_2, \ldots, n_r$, $n_1 \leq n_2 \leq \cdots \leq n_r$ constitute a *partition* of n if $n = n_1 + n_2 + \cdots + n_r$. Let $p(n)$ denote the number of partitions of n. Let us determine $p(n)$ for small values of n:

$$p(1) = 1 \text{ since } 1 = 1 \text{ is the only partition of } 1,$$

$$p(2) = 2 \text{ since } 2 = 2 \text{ and } 2 = 1 + 1,$$

$$p(3) = 3 \text{ since } 3 = 3,\ 3 = 1 + 2,\ 3 = 1 + 1 + 1,$$

$$p(4) = 5 \text{ since } 4 = 4,\ 4 = 1 + 3,\ 4 = 1 + 1 + 2,$$
$$4 = 1 + 1 + 1 + 1,\ 4 = 2 + 2.$$

Some others are $p(5) = 7$, $p(6) = 11$, $p(61) = 1{,}121{,}505$. There is a large mathematical literature on $p(n)$.

Every time we break a given permutation in S_n into a product of disjoint cycles we obtain a partition of n; for if the cycles appearing have lengths $n_1, n_2, \ldots, n_r$, respectively, $n_1 \leq n_2 \leq \cdots \leq n_r$, then $n = n_1 + n_2 + \cdots + n_r$. We shall say a permutation $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_r\}$ if it can be written as the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$, $n_1 \leq n_2 \leq \cdots \leq n_r$. Thus in S_9

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 5 & 6 & 4 & 7 & 9 & 8 \end{pmatrix} = (1)(2.\ 3)(4, 5, 6)(7)(8, 9)$$

has cycle decomposition $\{1, 1, 2, 2, 3\}$; note that $1 + 1 + 2 + 2 + 3 = 9$. We now aim to prove that two permutations in S_n are conjugate if and only if they have the same cycle decomposition. Once this is proved, then S_n will have exactly $p(n)$ conjugate classes.

To reach our goal we exhibit a very simple rule for computing the conjugate of a given permutation. Suppose that $\sigma \in S_n$ and that σ sends $i \to j$. How do we find $\theta^{-1}\sigma\theta$ where $\theta \in S_n$? Suppose that θ sends $i \to s$ and $j \to t$; then $\theta^{-1}\sigma\theta$ sends $s \to t$. *In other words, to compute $\theta^{-1}\sigma\theta$ replace every symbol in σ by its image under θ.* For example, to determine $\theta^{-1}\sigma\theta$ where $\theta = (1, 2, 3)(4, 7)$ and $\sigma = (5, 6, 7)(3, 4, 2)$, then, since $\theta{:}5 \to 5$, $6 \to 6$, $7 \to 4$, $3 \to 1$, $4 \to 7$, $2 \to 3$, $\theta^{-1}\sigma\theta$ is obtained from σ by replacing in σ, 5 by 5, 6 by 6, 7 by 4, 3 by 1, 4 by 7, and 2 by 3, so that $\theta^{-1}\sigma\theta = (5, 6, 4)(1, 7, 3)$.

With this algorithm for computing conjugates it becomes clear that two permutations having the same cycle decomposition are conjugate. For if

$\sigma = (a_1, a_2, \ldots, a_{n_1})(b_1, b_2, \ldots, b_{n_2}) \cdots (x_1, x_2, \ldots, x_{n_r})$ and $\tau = (\alpha_1, \alpha_2, \ldots, \alpha_{n_1})(\beta_1, \beta_2, \ldots, \beta_{n_2}) \cdots (\chi_1, \chi_2, \ldots, \chi_{n_r})$, then $\tau = \theta^{-1}\sigma\theta$, where one could use as θ the permutation

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n_1} & b_1 & \cdots & b_{n2} & \cdots & x_1 & \cdots & x_{n_r} \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n_1} & \beta_1 & \cdots & \beta_{n_2} & \cdots & \chi_1 & \cdots & \chi_{n_r} \end{pmatrix}.$$

Thus, for instance, (1, 2)(3, 4, 5)(6, 7, 8) and (7, 5)(1, 3, 6)(2, 4, 8) can be exhibited as conjugates by using the conjugating permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 1 & 3 & 6 & 2 & 4 & 8 \end{pmatrix}.$$

That two conjugates have the same cycle decomposition is now trivial for, by our rule, to compute a conjugate, replace every element in a given cycle by its image under the conjugating permutation.

We restate the result proved in the previous discussion as

LEMMA 2.11.3 *The number of conjugate classes in S_n is $p(n)$, the number of partitions of n.*

Since we have such an explicit description of the conjugate classes in S_n we can find all the elements commuting with a given permutation. We illustrate this with a very special and simple case.

Given the permutation (1, 2) in S_n, what elements commute with it? Certainly any permutation leaving both 1 and 2 fixed does. There are $(n - 2)!$ such. Also (1, 2) commutes with itself. This way we get $2(n - 2)!$ elements in the group generated by (1, 2) and the $(n - 2)!$ permutations leaving 1 and 2 fixed. Are there others? There are $n(n - 1)/2$ transpositions and these are precisely all the conjugates of (1, 2). Thus the conjugate class of (1, 2) has in it $n(n - 1)/2$ elements. If the order of the normalizer of (1, 2) is r, then, by our counting principle,

$$\frac{n(n-1)}{2} = \frac{o(S_n)}{r} = \frac{n!}{r}.$$

Thus $r = 2(n - 2)!$. That is, the order of the normalizer of (1, 2) is $2(n - 2)!$. But we exhibited $2(n - 2)!$ elements which commute with (1, 2); thus the general element σ commuting with (1, 2) is $\sigma = (1, 2)^i\tau$, where $i = 0$ or 1, τ is a permutation leaving both 1 and 2 fixed.

As another application consider the permutation $(1, 2, 3, \ldots, n) \in S_n$. We claim this element commutes only with its powers. Certainly it does commute with all its powers, and this gives rise to n elements. Now, any n-cycle is conjugate to $(1, 2, \ldots, n)$ and there are $(n - 1)!$ distinct n-cycles in S_n. Thus if u denotes the order of the normalizer of $(1, 2, \ldots, n)$

in S_n, since $o(S_n)/u$ = number of conjugates of $(1, 2, \ldots, n)$ in S_n = $(n - 1)!$,

$$u = \frac{n!}{(n-1)!} = n.$$

So the order of the normalizer of $(1, 2, \ldots, n)$ in S_n is n. The powers of $(1, 2, \ldots, n)$ having given us n such elements, there is no room left for others and we have proved our contention.

Problems

1. List all the conjugate classes in S_3, find the c_a's, and verify the class equation.
2. List all the conjugate classes in S_4, find the c_a's and verify the class equation.
3. List all the conjugate classes in the group of quaternion units (see Problem 21, Section 2.10), find the c_a's and verify the class equation.
4. List all the conjugate classes in the dihedral group of order $2n$, find the c_a's and verify the class equation. Notice how the answer depends on the parity of n.
5. (a) In S_n prove that there are $\frac{1}{r}\frac{n!}{(n-r)!}$ distinct r cycles.
   (b) Using this, find the number of conjugates that the r-cycle $(1, 2, \ldots, r)$ has in S_n.
   (c) Prove that any element σ in S_n which commutes with $(1, 2, \ldots, r)$ is of the form $\sigma = (1, 2, \ldots, r)^i\tau$, where $i = 0, 1, 2, \ldots, r$, τ is a permutation leaving all of $1, 2, \ldots, r$ fixed.
6. (a) Find the number of conjugates of $(1, 2)(3, 4)$ in S_n, $n \geq 4$.
   (b) Find the form of all elements commuting with $(1, 2)(3, 4)$ in S_n.
7. If p is a prime number, show that in S_p there are $(p - 1)! + 1$ elements x satisfying $x^p = e$.
8. If in a finite group G an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq (e), G$.
9. (a) Find two elements in A_5, the alternating group of degree 5, which are conjugate in S_5 but not in A_5.
   (b) Find all the conjugate classes in A_5 and the number of elements in each conjugate class.
10. (a) If N is a normal subgroup of G and $a \in N$, show that every conjugate of a in G is also in N.
    (b) Prove that $o(N) = \sum c_a$ for some choices of a in N.