*6. Let $a \leftrightarrow a'$ be an isomorphism between two groups G and G' of permutations, and let S consist of those permutations of G leaving one letter fixed. Does the set S' of all elements of G' corresponding to a's in S necessarily form a subgroup of G'? Must the set S' leave a letter fixed? Illustrate.

7. Prove that the center of any group G is a subgroup of G.

8. Find the center of the group of the square—of the equilateral triangle.

*9. Do the same for the group of a regular polygon of n sides.

*10. Show that the elements of finite order in any commutative group G form a subgroup.

8. Lagrange's Theorem

We now come to a far-reaching concept of abstract group theory: the idea that any subgroup S of a group G decomposes G into cosets.

Definition. *By the* order *of a group or subgroup is meant the number of its elements. By a right coset (left coset) of a subgroup S of a group G is meant any set Sa (or aS) of all the right-multiples sa (left-multiples as) of the elements s of S by a fixed element a in G. The number of distinct right cosets is called the "index" of S in G.*

Since $Se = S$, S is a right coset of itself. Moreover, one has

Lemma 1. *If S is finite, each right coset Sa of S has exactly as many elements as S does.*

For the transformation $s \to sa$ is one-one: each element $t = sa$ of the coset Sa is the image of one and only one element $s = ta^{-1}$ of S. (Cf. also Theorem 8.)

Lemma 2. *Two right cosets Sa and Sb of S are either identical or without common elements.*

For suppose Sa and Sb have an element $c = s'a = s''b$ (s', s'' in S) in common. Then Sb contains every element $sa = ss'^{-1}s'a = (ss'^{-1}s'')b$ of Sa, and similarly Sa contains every element of Sb. Consequently, $Sa = Sb$.

It is easy to illustrate these results. Thus, if G is the group of symmetries of the square, the subgroup $S = [I, H]$ has the four right cosets

$$[I, H]I = [I, H], \qquad [I, H]R = [R, HR] = [R, D'],$$
$$[I, H]R' = [R', HR'] = [R', V], \qquad [I, H]R'' = [R'', HR''] = [R'', D].$$

Each coset has two elements, and every element of the group falls into one of the four right cosets.

Again, if G is the additive group of the integers, the subgroup of multiples $\pm 5n$ of 5 has for right cosets the different residue classes modulo five. Finally, let G be the symmetric group of all permutations of the symbols $1, \cdots, 6$, while S is the subgroup leaving the symbol 1 fixed. Then

$1\phi = k$ implies for all $\psi \in S$ that $1(\psi\phi) = (1\psi)\phi = 1\phi = k$. Hence the coset $S\phi$ contains only (and so by Lemma 1 all) the 5! permutations carrying $1 \to k$. Therefore the right cosets of S are the subsets carrying $1 \to 1$, $1 \to 2$, $\cdots$, $1 \to 6$, respectively.

From the preceding lemmas, we obtain a classic result which is of fundamental importance for the theory of finite groups. Since any right coset Sa always contains $a = ea$, any group G is exhausted by its right cosets. Therefore G is decomposed by S into nonoverlapping subsets, each of which has exactly as many elements as S. If G is finite,† the conclusion is:

Theorem 14 (Lagrange). *The order of a finite group G is a multiple of the order of every one of its subgroups.*

Each element a of G generates a cyclic subgroup, whose order is (Theorem 9) simply the order of a. Therefore we have

Corollary 1. *Every element of a finite group G has as order a divisor of the order of G.*

Corollary 2. *Every group G of prime order p is cyclic.*

For the cyclic subgroup A generated by any element $a \neq e$ in such a group has an order $n > 1$ dividing p. But this implies $n = p$, and so $G = A$ is cyclic.

More generally, Lagrange's Theorem can be applied to the determination of all groups of any low order. As an example, define the *four group* as the group with four commuting elements: e (the identity) and a, b, $c = ab$, the latter each of order two. It will be shown in §9 that this group is isomorphic to the group of symmetries of a rectangle. We now prove

Corollary 3. *The only abstract groups of order four are the cyclic group of that order and the four group.*

Proof. If a group G of order 4 contains an element of order 4, it is cyclic. Otherwise, by Corollary 1, all elements of G except e must have order 2. Call them a, b, c. By the cancellation law, ab cannot be either $ae = a$, $eb = b$, or $aa = e$; hence $ab = c$. By symmetry, $ac = ca = b$, $bc = cb = a$, $ba = c$. But these, together with $a^2 = b^2 = c^2 = e$, and $ex = xe = x$ for all x, give the multiplication table of the four group.

Lagrange's Theorem can also be applied to number theory.

Corollary 4 (Fermat). *If a is an integer, p a prime, then $a^p \equiv a \pmod{p}$.*

Proof. The multiplication group mod p (excluding zero) has $p - 1$ elements. The order of any element a of this group is then a divisor of

† The extension to the infinite case follows immediately from the discussion of Chap. XII —but the importance of the result disappears.

$p - 1$, by Corollary 1, so that $a^{p-1} \equiv 1 \pmod{p}$ whenever $a \not\equiv 0 \pmod{p}$. If we multiply by a on both sides, we obtain the desired congruence, except for the case $a \equiv 0 \pmod{p}$, for which the conclusion is trivially true.

EXERCISES

1. Check Fermat's Theorem for $p = 7$ and $a = 2, 3, 6$.
2. (a) Enumerate the subgroups of the dihedral group (§6, Ex. 10) of order 26. How many are there?
   (b) Generalize your result.
3. Prove: the number of right cosets of any subgroup of a finite group equals the number of its left cosets. (*Hint:* Use the correspondence $x \to x^{-1}$.)
4. Determine the cosets of the subgroup $[I, D]$ of the group of the square.
5. If S is any subgroup of a group G, let SaS denote the set of all products sas' for s, s' in S. Prove that either $SaS \cap SbS$ is void, or $SaS = SbS$, for any $a, b \in G$.
6. For a subgroup S, let $x \equiv y \pmod{S}$ be defined to mean $xy^{-1} \in S$.
   (a) Prove that this relation is reflexive, symmetric, and transitive, and show that $x \equiv y \pmod{S}$ if and only if x and y lie in the same right coset of S.
   (b) Show that $x \equiv y \pmod{S}$ implies $xa \equiv ya \pmod{S}$ for all a.
7. Let G be the group of a regular hexagon, S the subgroup leaving one vertex fixed. Find the right and left cosets of S.
8. Prove that a group of order p^m, where p is a prime, must contain a subgroup of order p.
9. (a) If G is the group of all transformations $x \to ax + b$ of $\mathbf{R}$, where $a \neq 0$ and b are real, while S is the subgroup of all such transformations with $a = 1$, describe the right and left cosets of S in G.
   (b) Do the same for the subgroup T of all transformations with $b = 0$.

*10. (a) Show that, in any commutative ring R, the units (those elements with multiplicative inverses) form a group G.
   (b) Show that, if $R = \mathbf{Z}_n$, then G consists of the positive integers $k < n$ relatively prime to n.
   (c) The *order* of G, in case $R = \mathbf{Z}_n$, is denoted $\phi(n)$ and called Euler's ϕ-function. Show that $\phi(p) = p - 1$ if $n = p$ is a prime, and compute $\phi(12)$, $\phi(16)$, $\phi(30)$.
   (d) Using Lagrange's Theorem, infer that if $(k, n) = 1$, then $k^{\phi(n)} \equiv 1 \pmod{n}$.

*11. If S and T are subgroups of orders s and t of a group G, and if u and v are the orders of $S \cap T$ and $S \cup T$, prove that $st \leqq uv$.

*12. Prove that the only abstract groups of order 6 are the cyclic group and the symmetric group on three letters.

*13. Let $2^h + 1$ be a prime p.
   (a) Prove that in the multiplicative group mod p, the order of 2 is $2h$.
   (b) Using Fermat's Theorem, infer that $2h$ divides $p - 1 = 2^h$.
   (c) Conclude that h is a power of 2.

9. Permutation Groups

A *permutation* is a one-one transformation of a finite set into itself.

For instance, the set might consist of the five digits 1, 2, 3, 4, 5. One permutation might be the transformation ϕ,

(10) $1\phi = 2, \quad 2\phi = 3, \quad 3\phi = 4, \quad 4\phi = 5, \quad 5\phi = 1.$

Another might be the transformation ϕ' with

(11) $1\phi' = 2, \quad 2\phi' = 3, \quad 3\phi' = 1, \quad 4\phi' = 5, \quad 5\phi' = 4.$

The reader will find it instructive to compute $\phi\phi'$, $\phi'\phi$, and to note that $\phi\phi' \neq \phi'\phi$.

Permutations which, like the permutation ϕ defined above give a circular rearrangement of the symbols permuted (Figure 5), are called *cyclic* permutations or *cycles*. There is a suggestive notation for cyclic permutations—simply write down inside parentheses first any letter involved, then its transform, $\cdots$, and finally the letter transformed into the original letter. Thus, the permutation ϕ of (10) might be written in any one of the equivalent forms (12345), (23451), (34512), (45123), or (51234).

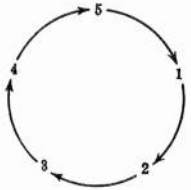

Figure 5

Theorem 15. *A cyclic permutation of n symbols has order n.*

Proof. The cyclic permutation $\gamma = (a_1 a_2 \cdots a_n)$ carries a_i into a_{i+1}. Hence γ^2 has the doubled effect of carrying each a_i into a_{i+2}, and generally γ^k carries a_i into a_{i+k}, where all subscripts are to be reduced modulo n. We have in γ^k the identity I if and only if a_{i+k} equals a_i; that is, if and only if $k \equiv 0 \pmod{n}$. The smallest k with $\gamma^k = I$ is then n itself, so γ does have the order n (see the definition in §6). The cycle γ is said to have length n.

The notation for a cyclic permutation can be extended to any permutation. For example, the permutation ϕ' in (11) cyclically permutes the digits 1, 2, and 3 by themselves, and 4 and 5 by themselves. Thus, it is the product of these two cycles,

$$(123)(45) = (45)(123).$$

This product may be written in either order, since the symbols permuted by (123) are left unchanged by (45), which means that successive application of these permutations in either order gives the same result.

Theorem 16. *Any permutation ϕ can be written as a product of cycles, acting on disjoint sets of symbols (more briefly: a product of disjoint† cycles).*

† Two sets are called *disjoint* when they have no element in common.

Proof. Select any symbol, denote it by a_1. Denote $a_1\phi$ by a_2, $a_2\phi$ by $a_3, \cdots, a_{n-1}\phi$ by a_n, until $a_n\phi = a_i$ is some element already named. Since the antecedent of any a_i $(i > 1)$ is a_{i-1}, $a_n\phi$ must be a_1. Thus the effect of ϕ on the letters $a_1, \cdots, a_n$ is the cycle $(a_1a_2 \cdots a_n)$. Moreover, $(a_1 \cdots a_n)$ contains, with any symbol a_i, its antecedent; hence ϕ permutes the remaining symbols among themselves. The result now follows by induction on the number of symbols. In particular, the identity permutation on m letters is represented by m "cycles," each of length one.

Conversely, evidently any product of disjoint cycles represents a permutation. Moreover, one may obtain

Theorem 17. *The order of any permutation ϕ is the least common multiple of the lengths of its disjoint cycles.*

Proof. Write the permutation ϕ as the product $\phi = \gamma_1 \cdots \gamma_r$ of disjoint cycles γ_i. If $i \neq j$, then γ_i and γ_j are disjoint; hence $\gamma_i\gamma_j = \gamma_j\gamma_i$, and the factors γ_i may be rearranged in ϕ and in its powers, to give $\phi^n = \gamma_1^n \cdots \gamma_r^n$ for all n. Therefore, $\phi^n = I$ if and only if every γ_i^n is the identity. But by Theorem 15, this means $\phi^n = I$ if and only if n is a common multiple of the lengths of the γ_i, from which the conclusion of Theorem 17 follows immediately. Q.E.D.

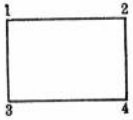

Figure 6

Every finite group is isomorphic with one or more groups of permutations, by Theorem 8 of §5. In particular, this is true of finite groups of symmetries of geometrical figures, as we now illustrate by two examples.

Consider the group of symmetries of the rectangle (Figure 6). Under it, the vertices are transformed by the four permutations

$$I = (1)(2)(3)(4), \qquad R = (14)(23), \qquad H = (13)(24), \qquad V = (12)(34).$$

This group is known as the *four group*. According to Theorem 8 it is isomorphic with the group of permutations $\phi_I = (I)(R)(V)(H)$, $\phi_R = (IR)(HV)$, $\phi_H = (IH)(RV)$, $\phi_V = (IV)(RH)$.

The group of symmetries of the square (§1) can similarly be represented as a group of permutations of the four vertices. Using Theorem 8, we can also represent it as a group of permutations of the eight symbols which represent the elements of the group. Thus, R corresponds to the permutation effected on right-multiplication of these symbols by "R"; from the column headed "R" in the group table (Figure 3), one sees that this permutation is $(IRR'R'')(HD'VD)$. Similarly, H corresponds to $(IH)(RD)(R'V)(R''D')$.

Two cycles of the same length are closely related. For example, if $\gamma = (1234)$ and $\gamma' = (2143)$, then one may compute that $\gamma' = \phi^{-1}\gamma\phi$, where

$\phi = (12)(34)$ is the permutation taking each digit of the cycle γ into the corresponding digit in γ'. This is a special case of the following result.

Theorem 18. *Let ϕ and γ be permutations of n letters, where γ is a cyclic permutation $\gamma = (a_1, \cdots, a_m)$, and denote by $\gamma' = (a_1\phi, \cdots, a_m\phi)$ the cycle obtained by replacing each letter a_i in the representation of γ by its image under ϕ. Then $\phi^{-1}\gamma\phi = \gamma'$.*

Proof. The product $\phi^{-1}\gamma\phi$ carries each letter $a_i\phi$ in succession into $a_i\phi\phi^{-1} = a_i$; then to $a_i\gamma = a_{i+1}$, then to $a_i\gamma\phi = a_{i+1}\phi$, and hence has the same effect upon $a_i\phi$ as does γ' (call $a_{m+1} = a_1$). Similarly, one computes that $\phi^{-1}\gamma\phi$ and γ' both carry any letter b not of the form $a_i\phi$ into itself. Hence $\phi^{-1}\gamma\phi = \gamma'$, as asserted.

Corollary. *For any permutations ϕ and ψ, if $\psi = \gamma_1 \cdots \gamma_r$ is written as a product of cycles, we have $\phi^{-1}\psi\phi = \gamma_1' \cdots \gamma_r'$, where the γ_i' are obtained from the γ_i as in Theorem 18.*

EXERCISES

1. Express as products of disjoint cycles the permutations
   (a) $1\phi = 4$, $2\phi = 6$, $3\phi = 5$, $4\phi = 1$, $5\phi = 3$, $6\phi = 2$;
   (b) $1\phi = 5$, $2\phi = 3$, $3\phi = 2$, $4\phi = 6$, $5\phi = 4$, $6\phi = 1$;
   (c) $1\phi = 3$, $2\phi = 5$, $3\phi = 6$, $4\phi = 4$, $5\phi = 1$, $6\phi = 2$.
   Find the order of each of these permutations.
2. Represent the following products as products of disjoint cycles:
   $(1234)(567)(261)(47)$; $(12345)(67)(1357)(163)$; $(14)(123)(45)(14)$.
   Find the order of each product.
3. Find the order of $(abcdef)(ghij)(klm)$; of $(abcdef)(abcd)(abc)$.
4. Represent the group of the rhombus (equilateral parallelogram) as a group of permutations of its vertices.
5. Describe the right and left cosets of the subgroup of all those permutations of $x_1, \cdots, x_6$ which carry the set $\{x_1, x_2\}$ into itself.
6. Which symmetric groups are Abelian?
7. Let G be the group of all symmetries of the cube leaving one vertex fixed. Represent G as a group of permutations of the vertices (cf. §3).
8. (a) Prove that every permutation can be written as a product of (not in general disjoint) cycles of length two ("transpositions").
   (*b) How does this relate to the proof of the "generalized commutative law" from the law $ab = ba$ (Chap. I, §5)?
9. Represent the group of symmetries of the equilateral triangle as a group of permutations of (a) three and (b) six letters.
   (*c) Do (b) in two essentially different ways.

*10. Prove that the symmetric group of degree n is generated by the cycles $(1, 2, \cdots, n-1)$ and $(n-1, n)$.

*11. In what sense is the representation of Theorem 16 unique? Prove your answer.