

which proves the first assertion of (3). The second assertion of (3) comes from observing first that $\ker \pi_H \leq G$ and $\ker \pi_H \leq H$. If now N is any normal subgroup of G contained in H then we have $N = xN x^{-1} \leq xHx^{-1}$ for all $x \in G$ so that

$$N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H.$$

This shows that $\ker \pi_H$ is the largest normal subgroup of G contained in H .

Corollary 4. (Cayley's Theorem) Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n , then G is isomorphic to a subgroup of S_n .

Proof: Let $H = 1$ and apply the preceding theorem to obtain a homomorphism of G into S_G (here we are identifying the cosets of the identity subgroup with the elements of G). Since the kernel of this homomorphism is contained in $H = 1$, G is isomorphic to its image in S_G .

Note that G is isomorphic to a *subgroup* of a symmetric group, not to the full symmetric group itself. For example, we exhibited an isomorphism of the Klein 4-group with the subgroup $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ of S_4 . Recall that subgroups of symmetric groups are called *permutation groups* so Cayley's Theorem states that every group is isomorphic to a permutation group. The permutation representation afforded by left multiplication on the elements of G (cosets of $H = 1$) is called the *left regular representation* of G . One might think that we could study all groups more effectively by simply studying subgroups of symmetric groups (and all finite groups by studying subgroups of S_n , for all n). This approach alone is neither computationally nor theoretically practical, since to study groups of order n we would have to work in the much larger group S_n (cf. Exercise 7, for example).

Historically, finite groups were first studied not in an axiomatic setting as we have developed but as subgroups of S_n . Thus Cayley's Theorem proves that the historical notion of a group and the modern (axiomatic) one are equivalent. One advantage of the modern approach is that we are not, in our study of a given group, restricted to considering that group as a subgroup of some *particular* symmetric group (so in some sense our groups are "coordinate free").

The next result generalizes our result on the normality of subgroups of index 2.

Corollary 5. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Remark: In general, a group of order n need not have a subgroup of index p (for example, A_4 has no subgroup of index 2).

Proof: Suppose $H \leq G$ and $|G : H| = p$. Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G , let $K = \ker \pi_H$ and let $|H : K| = k$. Then $|G : K| = |G : H||H : K| = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p (namely, the image of G under π_H) by the First Isomorphism Theorem. By Lagrange's Theorem, $pk = |G/K|$ divides $p!$.

Thus $k \mid \frac{p!}{p} = (p - 1)!$. But all prime divisors of $(p - 1)!$ are less than p and by the minimality of p , every prime divisor of k is greater than or equal to p . This forces $k = 1$, so $H = K \trianglelefteq G$, completing the proof.

EXERCISES

Let G be a group and let H be a subgroup of G .

1. Let $G = \{1, a, b, c\}$ be the Klein 4-group whose group table is written out in Section 2.5.
 - (a) Label $1, a, b, c$ with the integers 1,2,4,3, respectively, and prove that under the left regular representation of G into S_4 the nonidentity elements are mapped as follows:

$$a \mapsto (1 \ 2)(3 \ 4) \quad b \mapsto (1 \ 4)(2 \ 3) \quad c \mapsto (1 \ 3)(2 \ 4).$$
 - (b) Relabel $1, a, b, c$ as 1,4,2,3, respectively, and compute the image of each element of G under the left regular representation of G into S_4 . Show that the image of G in S_4 under this labelling is the same *subgroup* as the image of G in part (a) (even though the nonidentity elements individually map to different permutations under the two different labellings).
2. List the elements of S_3 as $1, (1 \ 2), (2 \ 3), (1 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2)$ and label these with the integers 1,2,3,4,5,6 respectively. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6 .
3. Let r and s be the usual generators for the dihedral group of order 8.
 - (a) List the elements of D_8 as $1, r, r^2, r^3, s, sr, sr^2, sr^3$ and label these with the integers 1, 2, ..., 8 respectively. Exhibit the image of each element of D_8 under the left regular representation of D_8 into S_8 .
 - (b) Relabel this same list of elements of D_8 with the integers 1, 3, 5, 7, 2, 4, 6, 8 respectively and recompute the image of each element of D_8 under the left regular representation with respect to this new labelling. Show that the two subgroups of S_8 obtained in parts (a) and (b) are different.
4. Use the left regular representation of Q_8 to produce two elements of S_8 which generate a subgroup of S_8 isomorphic to the quaternion group Q_8 .
5. Let r and s be the usual generators for the dihedral group of order 8 and let $H = \langle s \rangle$. List the left cosets of H in D_8 as $1H, rH, r^2H$ and r^3H .
 - (a) Label these cosets with the integers 1,2,3,4, respectively. Exhibit the image of each element of D_8 under the representation π_H of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of H in D_8 . Deduce that this representation is faithful (i.e., the elements of S_4 obtained form a subgroup isomorphic to D_8).
 - (b) Repeat part (a) with the list of cosets relabelled by the integers 1,3,2,4, respectively. Show that the permutations obtained from this labelling form a subgroup of S_4 that is different from the subgroup obtained in part (a).
 - (c) Let $K = \langle sr \rangle$, list the cosets of K in D_8 as $1K, rK, r^2K$ and r^3K , and label these with the integers 1,2,3,4. Prove that, with respect to this labelling, the image of D_8 under the representation π_K obtained from left multiplication on the cosets of K is the same *subgroup* of S_4 as in part (a) (even though the subgroups H and K are different and some of the elements of D_8 map to different permutations under the two homomorphisms).

6. Let r and s be the usual generators for the dihedral group of order 8 and let $N = \langle r^2 \rangle$. List the left cosets of N in D_8 as $1N, rN, sN$ and srN . Label these cosets with the integers 1,2,3,4 respectively. Exhibit the image of each element of D_8 under the representation π_N of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of N in D_8 . Deduce that this representation is not faithful and prove that $\pi_N(D_8)$ is isomorphic to the Klein 4-group.
7. Let Q_8 be the quaternion group of order 8.
- (a) Prove that Q_8 is isomorphic to a subgroup of S_8 .
 - (b) Prove that Q_8 is not isomorphic to a subgroup of S_n for any $n \leq 7$. [If Q_8 acts on any set A of order ≤ 7 show that the stabilizer of any point $a \in A$ must contain the subgroup $\langle -1 \rangle$.]
8. Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.
9. Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G . Deduce that every group of order p^2 has a normal subgroup of order p .
10. Prove that every non-abelian group of order 6 has a nonnormal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into S_3 .]
11. Let G be a finite group and let $\pi : G \rightarrow S_G$ be the left regular representation. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m n -cycles. Deduce that $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd.
12. Let G and π be as in the preceding exercise. Prove that if $\pi(G)$ contains an odd permutation then G has a subgroup of index 2. [Use Exercise 3 in Section 3.3.]
13. Prove that if $|G| = 2k$ where k is odd then G has a subgroup of index 2. [Use Cauchy's Theorem to produce an element of order 2 and then use the preceding two exercises.]
14. Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n . Prove that G is not simple.

4.3 GROUPS ACTING ON THEMSELVES BY CONJUGATION —THE CLASS EQUATION

In this section G is any group and we first consider G *acting on itself* (i.e., $A = G$) by *conjugation*:

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G$$

where gag^{-1} is computed in the group G as usual. This definition satisfies the two axioms for a group action because

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1 g_2)a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

and

$$1 \cdot a = 1a1^{-1} = a$$

for all $g_1, g_2 \in G$ and all $a \in G$.