Lemma 17.12 is another result that counts something, so do not underestimate it. The lemma will be used in the following way: A finite group G cannot have subgroups H and K that are too large with intersections that are too small, or the order of HK would have to exceed the order of G, which is impossible. For example, a group of order 24 cannot have two subgroups of orders 12 and 8 with an intersection of order 2.

The remainder of this section consists of several examples illustrating techniques of proving that all groups of certain orders are abelian or that they have nontrivial proper normal subgroups, that is, that they are not simple. We recall that a subgroup H of index 2 in a finite group G is a normal subgroup. This is because the two left cosets of H in G are H and the set of all elements in G that are not in H. But these are also the right cosets, which says that H is a normal subgroup of G.

17.13 Example   No group of order p^r for $r > 1$ is simple, where p is a prime. For by Theorem 17.4 such a group G contains a subgroup of order p^{r-1} normal in a subgroup of order p^r, which must be all of G. Thus a group of order 16 is not simple; it has a normal subgroup of order 8.   ▲

17.14 Example   No group of order 20 is simple, for such a group G contains Sylow 5-subgroups in number congruent to 1 modulo 5 and a divisor of 4, hence only 1. This Sylow 5-subgroup is then normal, since all conjugates of it must be itself.   ▲

17.15 Example   No group of order 30 is simple. We have seen that if there is only one Sylow p-subgroup for some prime p dividing 30, we are done. By Theorem 17.7 the possibilities for the number of Sylow 5-subgroups are 1 or 6, and those for Sylow 3-subgroups are 1 or 10. But if G has six Sylow 5-subgroups, then the intersection of any two is a subgroup of each of order dividing 5, and hence just $\{e\}$. Thus each contains 4 elements of order 5 that are in none of the others. Hence G must contain 24 elements of order 5. Similarly, if G has 10 Sylow 3-subgroups, it has at least 20 elements of order 3. The two types of Sylow subgroups together would require at least 44 elements in G. Thus there is a normal subgroup either of order 5 or of order 3.   ▲

17.16 Example   No group of order 48 is simple. Indeed, we shall show that a group G of order 48 has a normal subgroup of either order 16 or order 8. By Theorem 17.7 G has either one or three Sylow 2-subgroups of order 16. If there is only one subgroup of order 16, it is normal in G, by now a familiar argument.

Suppose that there are three subgroups of order 16, and let H and K be two of them. Then $H \cap K$ must be of order 8, for if $H \cap K$ were of order ≤ 4, then by Lemma 17.12 HK would have at least $(16)(16)/4 = 64$ elements, contradicting the fact that G has only 48 elements. Therefore, $H \cap K$ is normal in both H and K (being of index 2, or by Theorem 17.4). Hence the normalizer of $H \cap K$ contains both H and K and must have order a multiple >1 of 16 and a divisor of 48, therefore 48. Thus $H \cap K$ must be normal in G.   ▲

17.17 Example   No group of order 36 is simple. Such a group G has either one or four subgroups of order 9. If there is only one such subgroup, it is normal in G. If there are four such subgroups, let H and K be two of them. As in Example 17.16, $H \cap K$ must have at least 3 elements, or HK would have to have 81 elements, which is impossible. Thus the normalizer of $H \cap K$ has as order a multiple of >1 of 9 and a divisor of 36; hence the order must be either 18 or 36. If the order is 18, the normalizer is then of index 2 and therefore is normal in G. If the order is 36, then $H \cap K$ is normal in G.   ▲

17.18 Example   We show every group of order $255 = (3)(5)(17)$ is abelian (hence cyclic by the Fundamental Theorem 9.12 and not simple, since 255 is not a prime). By Theorem 17.7 such a group G has only one subgroup H of order 17. Then G/H has order 15 and is abelian

by Theorem 17.10. By Theorem 13.22, we see that the commutator subgroup C of G is contained in H. Thus as a subgroup of H, C has either order 1 or 17. Theorem 17.7 also shows that G has either 1 or 85 subgroups of order 3 and either 1 or 51 subgroups of order 5. However, 85 subgroups of order 3 would require 170 elements of order 3, and 51 subgroups of order 5 would require 204 elements of order 5 in G; both together would then require 375 elements in G, which is impossible. Hence there is a subgroup K having either order 3 or order 5 and normal in G. Then G/K has either order $(5)(17)$ or order $(3)(17)$, and in either case Theorem 17.10 shows that G/K is abelian. Thus $C \leq K$ and has order either 3, 5, or 1. Since $C \leq H$ showed that C has order 17 or 1, we conclude that C has order 1. Hence $C = \{e\}$, and $G/C \simeq G$ is abelian. The Fundamental Theorem 9.12 then shows that G is cyclic.   ▲

■ EXERCISES 17

Computations

In Exercises 1 through 4, determine the values of n_i that make each statement true.

1. A Sylow 3-subgroup of a group of order 12 has order n_1.

2. A Sylow 3-subgroup of a group of order 54 has order n_1.

3. A group of order 24 must have either n_1 or n_2 Sylow 2-subgroups. (Use only the information given in Theorem 17.7.)

4. A group of order $255 = (3)(5)(17)$ must have either n_1 or n_2 Sylow 3-subgroups and n_3 or n_4 Sylow 5-subgroups. (Use only the information given in Theorem 17.7.)

5. Find all Sylow 3-subgroups of S_4 and demonstrate that they are all conjugate.

6. Find two Sylow 2-subgroups of S_4 and show that they are conjugate.

7. Determine for which $n \leq 20$ any group of order n is abelian.

8. Determine for which $n \leq 20$ any group of order n is cyclic.

Concepts

In Exercises 9 through 11, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

9. Let p be a prime. A *p-group* is a group with the property that every element has order p.

10. The *normalizer N[H]* of a subgroup H of a group G is the set of all inner automorphisms that carry H onto itself.

11. Let G be a group whose order is divisible by a prime p. The *Sylow p-subgroup* of a group is the largest subgroup P of G with the property that P has some power of p as its order.

12. Determine whether each of the following is true or false.

    a. Any two Sylow p-subgroups of a finite group are conjugate.
    b. Theorem 17.7 shows that a group of order 15 has only one Sylow 5-subgroup.
    c. Every Sylow p-subgroup of a finite group has order a power of p.
    d. Every p-subgroup of every finite group is a Sylow p-subgroup.
    e. Every finite abelian group has exactly one Sylow p-subgroup for each prime p dividing the order of G.
    f. The normalizer in G of a subgroup H of G is always a normal subgroup of G.
    g. If H is a subgroup of G, then H is always a normal subgroup of $N[H]$.
    h. A Sylow p-subgroup of a finite group G is normal in G if and only if it is the only Sylow p-subgroup of G.
    i. If G is an abelian group and H is a subgroup of G, then $N[H] = H$.
    j. A group of prime-power order p^n has no Sylow p-subgroup.

13. Determine whether each of the following is true or false.

   a. Every group of order 159 is cyclic.

   b. Every group of order 102 has a nontrivial proper normal subgroup.

   c. Every group of order p^3 is abelian, assuming that p is a prime number.

   d. There is a simple group of order 1128.

   e. It would be quite tedious to show that no group of nonprime order between 60 and 168 is simple by the methods illustrated in the text.

   f. No group of order 21 is simple.

   g. Every group of 125 elements has at least 5 elements that commute with every element in the group.

   h. Every group of order 42 has a normal subgroup of order 7.

   i. Every group of order 42 has a normal subgroup of order 3.

   j. The only simple groups are the groups $\mathbb{Z}_p$ and A_n, where p is a prime and $n > 4$.

Theory

14. Let H be a subgroup of a group G. Show that $G_H = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G without using Theorem 14.13.

15. Let G be a finite group and let primes p and $q \neq p$ divide $|G|$. Prove that if G has precisely one proper Sylow p-subgroup, it is a normal subgroup, so G is not simple.

16. Show that every group of order 45 has a normal subgroup of order 9.

17. Let G be a finite group and let p be a prime dividing $|G|$. Let P be a Sylow p-subgroup of G. Show that $N[N[P]] = N[P]$. [*Hint:* Argue that P is the only Sylow p-subgroup of $N[N[P]]$, and use Theorem 17.6.]

18. Let G be a finite group and let a prime p divide $|G|$. Let P be a Sylow p-subgroup of G and let H be any p-subgroup of G. Show there exists $g \in G$ such that $gHg^{-1} \leq P$.

19. Show that every group of order $(35)^3$ has a normal subgroup of order 125.

20. Show that there are no simple groups of order $255 = (3)(5)(17)$.

21. Show that there are no simple groups of order $p^r m$, where p is a prime, r is a positive integer, and $m < p$.

22. Prove that all simple groups of order at most 20 are cyclic.

23. Let p be a prime. Show that a finite group of order p^n contains *normal* subgroups H_i for $0 \leq i \leq n$ such that $|H_i| = p^i$ and $H_i < H_{i+1}$ for $0 \leq i < n$. [*Hint:* See Theorem 14.24.]

24. Let G be a finite group and let P be a normal p-subgroup of G. Show that P is contained in every Sylow p-subgroup of G.

25. Prove that if $p \geq 3$ is a prime number and $k \geq 1$, then any group G of order $2p^k$ is not simple.

26. Prove that every group of order $(5)(7)(47)$ is abelian and cyclic.

27. Prove that no group of order 96 is simple.

28. Show that every group of order 30 contains a subgroup of order 15. [*Hint:* Use the last sentence in Example 17.15 and go to the factor group.]

29. Prove that no group of order 160 is simple.

30. Let G be a finite group and suppose that for each k that divides $|G|$, G has at most one subgroup of order k. Prove that G is cyclic.

31. Let G be a finite group. Use the group action of G on G given by conjugation, $g * x = gxg^{-1}$, to prove the formula $|G| = |Z(G)| + n_1 + n_2 + \cdots + n_k$, where $Z(G)$ is the center of G and $n_1, n_2, \ldots, n_k$ are the orbit sizes for the orbits containing at least two elements. This formula is called the **class equation**.

32. By arguments similar to those used in the examples of this section, convince yourself that the only simple groups of order less than 60 are cyclic. You need not write out all the details.

33. Show that for every positive integer $n < 15$, if every group of order n is cyclic, then n is prime.

SECTION 18   SERIES OF GROUPS

Subnormal and Normal Series

This section is concerned with the notion of a *series* of a group G, which gives insight into the structure of G. The results hold for both abelian and nonabelian groups. They are not too important for finitely generated abelian groups because of the Fundamental Theorem of Finitely Generated Abelian Groups. Many of our illustrations will be taken from abelian groups, however, for ease of computation.

18.1 Definition   A **subnormal** (or **subinvariant**) **series of a group** G is a finite sequence $H_0, H_1, \cdots, H_n$ of subgroups of G such that $H_i < H_{i+1}$ and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = G$. A **normal** (or **invariant**) **series of** G is a finite sequence $H_0, H_1, \cdots, H_n$ of normal subgroups of G such that $H_i < H_{i+1}, H_0 = \{e\}$, and $H_n = G$.   ∎

Note that for abelian groups the notions of subnormal and normal series coincide, since every subgroup is normal. A normal series is always subnormal, but the converse need not be true. We defined a subnormal series before a normal series, since the concept of a subnormal series is more important for our work.

18.2 Example   Two examples of normal series of $\mathbb{Z}$ under addition are

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

and

$$\{0\} < 9\mathbb{Z} < \mathbb{Z}.$$ ▲

18.3 Example   We let $G = D_4$, the dihedral group. The series

$$\{\iota\} < \{\iota, \mu\} < \{\iota, \mu, \rho^2, \mu\rho^2\} < D_4$$

is a subnormal series since each subgroup is normal in the one to its right. The subgroup $\{\iota, \mu\}$ is not a normal subgroup of D_4 since $\rho\mu\rho^{-1} = \mu\rho^2 \notin \{\iota, \mu\}$. So this series is a subnormal series, but not a normal series.   ▲

18.4 Definition   A subnormal (normal) series $\{K_j\}$ is a **refinement of a subnormal (normal) series** $\{H_i\}$ of a group G if $\{H_i\} \subseteq \{K_j\}$, that is, if each H_i is one of the K_j.   ∎

18.5 Example   The series

$$\{0\} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

is a refinement of the series

$$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}.$$

Two new terms, $4\mathbb{Z}$ and $24\mathbb{Z}$, have been inserted.   ▲

Of interest in studying the structure of G are the factor groups H_{i+1}/H_i. These are defined for both normal and subnormal series, since H_i is normal in H_{i+1} in either case.

18.6 Definition   Two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of the same group G are **isomorphic** if there is a one-to-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that corresponding factor groups are isomorphic.   ∎

Clearly, two isomorphic subnormal (normal) series must have the same number of groups.

18.7 Example   The two series of $\mathbb{Z}_{15}$,

$$\{0\} < \langle 5 \rangle < \mathbb{Z}_{15}$$

and

$$\{0\} < \langle 3 \rangle < \mathbb{Z}_{15},$$

are isomorphic. Both $\mathbb{Z}_{15}/\langle 5 \rangle$ and $\langle 3 \rangle/\{0\}$ are isomorphic to $\mathbb{Z}_5$, and $\mathbb{Z}_{15}/\langle 3 \rangle$ is isomorphic to $\langle 5 \rangle/\{0\}$, or to $\mathbb{Z}_3$.   ▲

The Schreier Theorem

We proceed to prove that two subnormal series of a group G have isomorphic refinements. This is a fundamental result in the theory of series. Although the proof is a little technical, it is broken up into smaller pieces that make it easier to follow. Before starting the proof, we give an example to illustrate the goal of our investigation.

18.8 Example   Let us try to find isomorphic refinements of the series

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

and

$$\{0\} < 9\mathbb{Z} < \mathbb{Z}$$

given in Example 18.2. Consider the refinement

$$\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$$

of $\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$ and the refinement

$$\{0\} < 72\mathbb{Z} < 18\mathbb{Z} < 9\mathbb{Z} < \mathbb{Z}$$

of $\{0\} < 9\mathbb{Z} < \mathbb{Z}$. In both cases the refinements have four factor groups isomorphic to $\mathbb{Z}_4, \mathbb{Z}_2, \mathbb{Z}_9$, and $72\mathbb{Z}$ or $\mathbb{Z}$. The *order* in which the factor groups occur is different to be sure.   ▲

We start with a rather technical lemma developed by Zassenhaus. This lemma is sometimes called the *butterfly lemma*, since Fig. 18.9, which accompanies the lemma, has a butterfly shape.

18.10 Lemma   **(Zassenhaus Lemma)**   Let $H, K \leq G$ be subgroups and $H^* \trianglelefteq H$, $K^* \trianglelefteq K$ be normal subgroups of H and K, respectively. Then

1. $H^*(H \cap K^*)$ is a normal subgroup of $H^*(H \cap K)$,
2. $K^*(H^* \cap K)$ is a normal subgroup of $K^*(H \cap K)$, and
3. The factor groups $H^*(H \cap K)/H^*(H \cap K^*)$, $K^*(H \cap K)/K^*(H^* \cap K)$, and $(H \cap K)/[(H^* \cap K)(H \cap K^*)]$ are all isomorphic.

Proof   It may be helpful to follow along with Figure 18.9 to visualize the subgroups that we refer to in the proof. Before beginning the proof of normality, we need to verify that the sets involved are in fact subgroups of G. All three sets H^*, $H \cap K^*$, and $H \cap K$ are subgroups of H. Furthermore, H^* is a normal subgroup of H, so by Lemma 16.4, $H^*(H \cap K^*)$ and $H^*(H \cap K)$ are subgroups of H. Thus $H^*(H \cap K^*)$ and $H^*(H \cap K)$ are also subgroups of G. Clearly, $H^*(H \cap K^*)$ is a subgroup of $H^*(H \cap K)$.
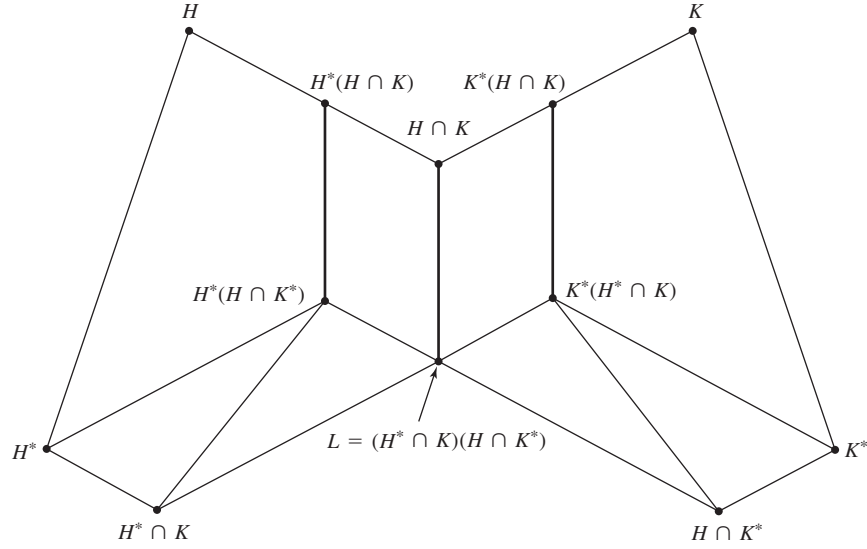
18.9 Figure

We now show that $H^*(H \cap K^*)$ is a normal subgroup of $H^*(H \cap K)$. We let $w \in H^*(H \cap K^*)$ and $y \in H^*(H \cap K)$. We need to verify that $ywy^{-1} \in H^*(H \cap K^*)$. By definition, $w = h_1 x$ and $y \in h_2 g$ for some $h_1, h_2 \in H^*$, $x \in H \cap K^*$, and $g \in H \cap K$. We write

$$ywy^{-1} = h_2 g h_1 x g^{-1} h_2^{-1}$$
$$= h_2 (g h_1 g^{-1}) g x g^{-1} h_2^{-1}$$
$$= h_2 h_3 g x g^{-1} h_2^{-1}$$

for some $h_3 \in H^*$ since H^* is a normal subgroup of H. We note that h_2^{-1} and $h_2 h_3$ are both elements of $H^* \leq H^*(H \cap K^*)$. Furthermore $g x g^{-1} \in K^*$ since $g \in K$ and K^* is a normal subgroup of K. Also $g x g^{-1} \in H$ since both g and x are elements of H. Thus, $g x g^{-1} \in H \cap K^* \leq K^*(H \cap K^*)$. So, ywy^{-1} is the product of elements in the group $H^*(H \cap K^*)$, which implies that $ywy^{-1} \in H^*(H \cap K^*)$. Thus we have shown Part 1 of the Theorem.

We use the Second Isomorphism Theorem (16.5) to prove the third part of the Lemma. Let $N' = H^*(H \cap K^*)$ and $H' = H \cap K$. So N' is a normal subgroup of $H^*(H \cap K)$ and H' is a subgroup of $H^*(H \cup K)$. By Lemma 16.4 $N'H'$ is a group and

$$N'H' = H^*(H \cap K^*)(H \cap K)$$
$$= H^*(H \cap K).$$

The Second Isomorphism Theorem says that $N'H'/N' \simeq H'/(H' \cap N')$. We have

$$N'H'/N' = H^*(H \cap K)/H^*(H \cap K^*)$$

and

$$H'/(H' \cap N') = (H \cap K)/(H^*(H \cap K^*) \cap (H \cap K)).$$

Exercise 11 in Section 16 shows that

$$H^*(H \cap K^*) \cap (H \cap K) = (H^* \cap K)(H \cap K^*).$$

Thus

$$H^*(H \cap K)/(H^*(H \cap K^*)) \simeq (H \cap K)/((H^* \cap K)(H \cap K^*)).$$