13.16 Definition A group is **simple** if it is nontrivial and has no proper nontrivial normal subgroup. ■

13.17 Theorem The alternating group A_n is simple for $n \geq 5$.

Proof See Exercise 41. ◆

There are many simple groups other than those given above. For example, A_5 is of order 60 and A_6 is of order 360, and there is a simple group of nonprime order, namely 168, between these orders.

The complete determination and classification of all finite simple groups is one of the mathematical triumphs of the twentieth century. Hundreds of mathematicians worked on this task from 1950 to 1980. It can be shown that a finite group has a sort of factorization into simple groups, where the factors are unique up to order. The situation is similar to the factorization of positive integers into primes. The knowledge of all finite simple groups can be used to solve some problems of finite group theory and combinatorics.

We have seen in this text that a finite simple abelian group is isomorphic to $\mathbb{Z}_p$ for some prime p. In 1963, Thompson and Feit [21] published their proof of a long-standing conjecture of Burnside, showing that every finite nonabelian simple group is of even order. Further great strides toward the complete classification were made by Aschbacher in the 1970s. Early in 1980, Griess announced that he had constructed a predicted "monster" simple group of order

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,$$
$$000,000,000.$$

Aschbacher added the final details of the classification in August 1980. The research papers contributing to the entire classification fill roughly 5000 journal pages.

We turn to the characterization of those normal subgroups N of a group G for which G/N is a simple group. First we state an addendum to Theorem 8.5 on properties of a group homomorphism. The proof is left to Exercises 37 and 38.

13.18 Theorem Let $\phi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G. ◆

Theorem 13.18 should be viewed as saying that a homomorphism $\phi : G \to G'$ preserves normal subgroups between G and $\phi[G]$. It is important to note that $\phi[N]$ may not be normal in G', even though N is normal in G. For example, $\phi : \mathbb{Z}_2 \to S_3$, where $\phi(0) = \iota$ and $\phi(1) = (1, 2)$ is a homomorphism, and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\iota, (1, 2)\}$ is not a normal subgroup of S_3.

We can now characterize when G/N is a simple group.

13.19 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

13.20 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

Proof Let M be a maximal normal subgroup of G. Consider the canonical homomorphism $\gamma : G \to G/M$ given by Theorem 12.12. Now γ^{-1} of any nontrivial proper normal subgroup of G/M is a proper normal subgroup of G properly containing M. But M is maximal, so this cannot happen. Thus G/M is simple.

Conversely, Theorem 13.18 shows that if N is a normal subgroup of G properly containing M, then $\gamma[N]$ is normal in G/M. If also $N \neq G$, then

$$\gamma[N] \neq G/M \qquad \text{and} \qquad \gamma[N] \neq \{M\}.$$

Thus, if G/M is simple so that no such $\gamma[N]$ can exist, no such N can exist, and M is maximal. ◆

The Center and Commutator Subgroups

Every nonabelian group G has two important normal subgroups, the *center* $Z(G)$ of G and the *commutator subgroup* C of G. (The letter Z comes from the German word *zentrum,* meaning center.) The center $Z(G)$ is defined by

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Exercise 59 of Section 5 shows that $Z(G)$ is an abelian subgroup of G. Since for each $g \in G$ and $z \in Z(G)$ we have $gzg^{-1} = zgg^{-1} = ze = z$, we see at once that $Z(G)$ is a normal subgroup of G. If G is abelian, then $Z(G) = G$; in this case, the center is not useful.

13.21 Example The center of a group G always contains the identity element e. It may be that $Z(G) = \{e\}$, in which case we say that **the center of G is trivial**. For example, examination of Table 4.15 for the group S_3 shows us that $Z(S_3) = \{\iota\}$, so the center of S_3 is trivial. (This is a special case of Exercise 40, which shows that the center of every nonabelian group of order pq for primes p and q is trivial.) Consequently, the center of $S_3 \times \mathbb{Z}_5$ must be $\{\iota\} \times \mathbb{Z}_5$, which is isomorphic to $\mathbb{Z}_5$. ▲

Turning to the commutator subgroup, recall that in forming a factor group of G modulo a normal subgroup N, we are essentially putting every element in G that is in N equal to e, for N forms our new identity in the factor group. This indicates another use for factor groups. Suppose, for example, that we are studying the structure of a nonabelian group G. Since Theorem 9.12 gives complete information about the structure of all finitely generated abelian groups, it might be of interest to try to form an abelian group as much like G as possible, an *abelianized version* of G, by starting with G and then requiring that $ab = ba$ for all a and b in our new group structure. To require that $ab = ba$ is to say that $aba^{-1}b^{-1} = e$ in our new group. An element $aba^{-1}b^{-1}$ in a group is a **commutator of the group.** Thus we wish to attempt to form an abelianized version of G by replacing every commutator of G by e. By the first observation of this paragraph, we should then attempt to form the factor group of G modulo the smallest normal subgroup we can find that contains all commutators of G.

13.22 Theorem Let G be a group. The set of all commutators $aba^{-1}b^{-1}$ for $a, b \in G$ generates a subgroup C (the **commutator subgroup**) of G. This subgroup C is a normal subgroup of G. Furthermore, if N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

Proof The commutators certainly generate a subgroup C; we must show that it is normal in G. Note that the inverse $(aba^{-1}b^{-1})^{-1}$ of a commutator is again a commutator, namely, $bab^{-1}a^{-1}$. Also $e = eee^{-1}e^{-1}$ is a commutator. Theorem 7.7 then shows that C consists precisely of all finite products of commutators. For $x \in C$, we must show that $g^{-1}xg \in C$ for all $g \in G$, or that if x is a product of commutators, so is $g^{-1}xg$ for all $g \in G$. By inserting $e = gg^{-1}$ between each product of commutators occurring in x, we see that it is sufficient to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C. But

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})(e)(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g], \end{aligned}$$

which is in C. Thus C is normal in G.

The rest of the theorem is obvious if we have acquired the proper feeling for factor groups. One doesn't visualize in this way, but writing out that G/C is abelian follows from

$$\begin{aligned}(aC)(bC) &= abC = ab(b^{-1}a^{-1}ba)C \\ &= (abb^{-1}a^{-1})baC = baC = (bC)(aC).\end{aligned}$$

Furthermore, if N is a normal subgroup of G and G/N is abelian, then $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$; that is, $aba^{-1}b^{-1}N = N$, so $aba^{-1}b^{-1} \in N$, and $C \leq N$. Finally, if $C \leq N$, then

$$\begin{aligned}(aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN).\end{aligned}$$

◆

13.23 Example Using cycle notation in the symmetric group S_3, one commutator is

$$(1,2,3)(2,3)(1,2,3)^{-1}(2,3)^{-1} = (1,2,3)(2,3)(1,3,2)(2,3) = (1,3,2).$$

So the commutator subgroup C contains $\langle(1,3,2)\rangle = A_3$, the alternating group. Since S_3/A_3 is abelian (isomorphic with $\mathbb{Z}_2$), Theorem 13.22 says that $C \leq A_3$. Therefore, A_3 is the commutator subgroup. ▲

EXERCISES 13

Computations

In Exercises 1 through 14, classify the given group according to the fundamental theorem of finitely generated abelian groups.

1. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,1)\rangle$

2. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,2)\rangle$

3. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle$

4. $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$

5. $(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2,4)\rangle$

6. $(\mathbb{Z} \times \mathbb{Z})/\langle(0,1)\rangle$

7. $(\mathbb{Z} \times \mathbb{Z})/\langle(0,2)\rangle$

8. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(1,1,1)\rangle$

9. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_4)/\langle(3,0,0)\rangle$

10. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle(0,4,0)\rangle$

11. $(\mathbb{Z} \times \mathbb{Z})/\langle(2,2)\rangle$

12. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(3,3,3)\rangle$

13. $(\mathbb{Z} \times \mathbb{Z})/\langle(2,6)\rangle$

14. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2)/\langle(1,1,1)\rangle$

15. Find both the center and the commutator subgroup of D_4.

16. Find both the center and the commutator subgroup of $\mathbb{Z}_3 \times S_3$.

17. Find both the center and the commutator subgroup of $S_3 \times D_4$.

18. Describe all subgroups of order ≤ 4 of $\mathbb{Z}_4 \times \mathbb{Z}_4$, and in each case classify the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup by Theorem 9.12. That is, describe the subgroup and say that the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, or whatever the case may be. [*Hint:* $\mathbb{Z}_4 \times \mathbb{Z}_4$ has six different cyclic subgroups of order 4. Describe them by giving a generator, such as the subgroup $\langle(1,0)\rangle$. There is one subgroup of order 4 that is isomorphic to the Klein 4-group. There are three subgroups of order 2.]

Concepts

In Exercises 19 and 20, 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.

19. The *center* of a group G contains all elements of G that commute with every element of G.

20. The *commutator subgroup* of a group G is $\{a^{-1}b^{-1}ab \mid a, b \in G\}$.

21. Determine whether each of following is true or false.

a. Every factor group of a cyclic group is cyclic.
b. A factor group of a noncyclic group is again noncyclic.
c. $\mathbb{R}/\mathbb{Z}$ under addition has no element of order 3.
d. $\mathbb{R}/\mathbb{Q}$ under addition has no element of order 2.
e. $\mathbb{R}/\mathbb{Z}$ under addition has an infinite number of elements of order 4.
f. If the commutator subgroup C of a group G is $\{e\}$, then G is abelian.
g. If G/H is abelian, then the commutator subgroup C of G contains H.
h. The commutator subgroup of a simple group G must be G itself.
i. The commutator subgroup of a nonabelian simple group G must be G itself.
j. All nontrivial finite simple groups have prime order.

In Exercises 22 through 25, let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let F^* be the multiplicative group of all elements of F that do not assume the value 0 at any point of $\mathbb{R}$.

22. Let K be the subgroup of F consisting of the constant functions. Find a subgroup of F to which F/K is isomorphic.

23. Let K^* be the subgroup of F^* consisting of the nonzero constant functions. Find a subgroup of F^* to which F^*/K^* is isomorphic.

24. Let K be the subgroup of continuous functions in F. Can you find an element of F/K having order 2? Why or why not?

25. Let K^* be the subgroup of F^* consisting of the continuous functions in F^*. Can you find an element of F^*/K^* having order 2? Why or why not?

In Exercises 26 through 28, let U be the multiplicative group $\{z \in \mathbb{C} \mid |z| = 1\}$.

26. Let $z_0 \in U$. Show that $z_0U = \{z_0z \mid z \in U\}$ is a subgroup of U, and compute U/z_0U.

27. To what group we have mentioned in the text is $U/\langle -1 \rangle$ isomorphic?

28. Let $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ where $n \in \mathbb{Z}^+$. To what group we have mentioned is $U/\langle \zeta_n \rangle$ isomorphic?

29. To what group mentioned in the text is the additive group $\mathbb{R}/\mathbb{Z}$ isomorphic?

30. Give an example of a group G having no elements of finite order greater than 1 and a normal subgroup $H \trianglelefteq G$, $H \neq G$, so that in G/H every element has finite order.

31. Let H and K be normal subgroups of a group G. Give an example showing that we may have $H \simeq K$ while G/H is not isomorphic to G/K.

32. Describe the center of every simple

a. abelian group
b. nonabelian group.

33. Describe the commutator subgroup of every simple

a. abelian group
b. nonabelian group.

Proof Synopsis

34. Give a one-sentence synopsis of the proof of Theorem 13.9.

35. Give at most a two-sentence synopsis of the proof of Theorem 13.20.

Theory

36. Show that if a finite group G contains a nontrivial subgroup of index 2 in G, then G is not simple.

37. Let $\phi : G \to G'$ be a group homomorphism, and let N be a normal subgroup of G. Show that $\phi[N]$ is a normal subgroup of $\phi[G]$.