The next definition is basic to the characterization of those polynomial equations whose solutions can be expressed in terms of radicals.

18.19 Definition A group G is **solvable** if it has a composition series $\{H_i\}$ such that all factor groups H_{i+1}/H_i are abelian. ■

By the Jordan–Hölder theorem, we see that for a solvable group, *every* composition series $\{H_i\}$ must have abelian factor groups H_{i+1}/H_i.

18.20 Example The group S_3 is solvable, because the composition series

$$\{e\} < A_3 < S_3$$

has factor groups isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_2$, which are abelian. The group S_5 is not solvable, for since A_5 is simple, the series

$$\{e\} < A_5 < S_5$$

is a composition series, and $A_5/\{e\}$, which is isomorphic to A_5, is not abelian. *This group A_5 of order* 60 *can be shown to be the smallest group that is not solvable*. This fact is closely connected with the fact that a polynomial equation of degree 5 is not in general solvable by radicals, but a polynomial equation of degree ≤ 4 is. ▲

The Ascending Central Series

We mention one subnormal series for a group G that can be formed using centers of groups. Recall from Section 13 that the center $Z(G)$ of a group G is defined by

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

and that $Z(G)$ is a normal subgroup of G. If we have the table for a finite group G, it is easy to find the center. An element a is in the center of G if and only if the row with header a and the column with header a list the elements of G in the same order.

Now let G be a group, and let $Z(G)$ be the center of G. Since $Z(G)$ is normal in G, we can form the factor group $G/Z(G)$ and find the center $Z(G/Z(G))$ of this factor group. Since $Z(G/Z(G))$ is normal in $G/Z(G)$, if $\gamma : G \to G/Z(G)$ is the canonical map, then by Theorem 13.18, $\gamma^{-1}[Z(G/Z(G))]$ is a normal subgroup $Z_1(G)$ of G. We can then form the factor group $G/Z_1(G)$ and find its center, take $(\gamma_1)^{-1}$ of it to get $Z_2(G)$, and so on.

18.21 Definition The series

$$\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

described in the preceding discussion is the **ascending central series of the group** G. ■

18.22 Example For $n \geq 3$, the center of S_n is just the identity ι. Thus the ascending central series of S_n is

$$\{\iota\} \leq \{\iota\} \leq \{\iota\} \leq \cdots.$$

The center of the dihedral group D_4 is $\{\iota, \rho^2\}$. The factor group $D_4/\{\iota, \rho^2\}$ has order 4, and each element has order 1 or 2, so $D_4/\{\iota, \rho^2\}$ is isomorphic with the Klein 4-group, which is abelian. Therefore the center of $D_4/\{\iota, \rho^2\}$ is the whole group, and the central series for D_4 is

$$\{\iota\} \leq \{\iota, \rho^2\} \leq D_4 \leq D_4 \leq D_4 \leq \cdots.$$ ▲

EXERCISES 18

Computations

In Exercises 1 through 5, give isomorphic refinements of the two series.

1. $\{0\} < 10\mathbb{Z} < \mathbb{Z}$ and $\{0\} < 25\mathbb{Z} < \mathbb{Z}$

2. $\{0\} < 60\mathbb{Z} < 20\mathbb{Z} < \mathbb{Z}$ and $\{0\} < 245\mathbb{Z} < 49\mathbb{Z} < \mathbb{Z}$

3. $\{0\} < \langle 9\rangle < \mathbb{Z}_{54}$ and $\{0\} < \langle 2\rangle < \mathbb{Z}_{54}$

4. $\{0\} < \langle 9\rangle < \langle 3\rangle < \mathbb{Z}_{72}$ and $\{0\} < \langle 36\rangle < \langle 12\rangle < \mathbb{Z}_{72}$

5. $\{(0,0)\} < (60\mathbb{Z}) \times \mathbb{Z} < (10\mathbb{Z}) \times \mathbb{Z} < \mathbb{Z} \times \mathbb{Z}$ and $\{(0,0)\} < \mathbb{Z} \times (80\mathbb{Z}) < \mathbb{Z} \times (20\mathbb{Z}) < \mathbb{Z} \times \mathbb{Z}$

6. Find all composition series of $\mathbb{Z}_{90}$ and show that they are isomorphic.

7. Find all composition series of $\mathbb{Z}_{48}$ and show that they are isomorphic.

8. Find all composition series of $\mathbb{Z}_5 \times \mathbb{Z}_5$.

9. Find all composition series of $S_3 \times \mathbb{Z}_2$.

10. Find all composition series of $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

11. Find the center of $S_3 \times \mathbb{Z}_4$.

12. Find the center of $S_3 \times D_4$.

13. Find the ascending central series of $S_3 \times \mathbb{Z}_4$.

14. Find the ascending central series of $S_3 \times D_4$.

Concepts

In Exercises 15 and 16, 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.

15. A *composition series* of a group G is a finite sequence

$$\{e\} = H_0 < H_1 < H_2 < \cdots < H_{n-1} < H_n = G$$

of subgroups of G such that H_i is a maximal normal subgroup of H_{i+1} for $i = 0, 1, 2, \cdots, n-1$.

16. A *solvable group* is one that has a composition series of abelian groups.

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

a. Every normal series is also subnormal.
b. Every subnormal series is also normal.
c. Every principal series is a composition series.
d. Every composition series is a principal series.
e. Every abelian group has exactly one composition series.
f. Every finite group has a composition series.
g. A group is solvable if and only if it has a composition series with simple factor groups.
h. S_7 is a solvable group.
i. The Jordan–Hölder theorem has some similarity with the Fundamental Theorem of Arithmetic, which states that every positive integer greater than 1 can be factored into a product of primes uniquely up to order.
j. Every finite group of prime order is solvable.

18. Find a composition series of $S_3 \times S_3$. Is $S_3 \times S_3$ solvable?

19. Is the dihedral group D_4 solvable?

20. Let G be $\mathbb{Z}_{36}$. Refer to the proof of Theorem 18.11. Let the subnormal series (1) be

$$\{0\} < \langle 12\rangle < \langle 3\rangle < \mathbb{Z}_{36}$$

and let the subnormal series (2) be

$$\{0\} < \langle 18\rangle < \mathbb{Z}_{36}.$$

Find chains (3) and (4) and exhibit the isomorphic factor groups as described in the proof. Write chains (3) and (4) in the rectangular array shown in the text.

21. Repeat Exercise 20 for the group $\mathbb{Z}_{24}$ with the subnormal series (1)

$$\{0\} < \langle 12\rangle < \langle 4\rangle < \mathbb{Z}_{24}$$

and (2)

$$\{0\} < \langle 6\rangle < \langle 3\rangle < \mathbb{Z}_{24}.$$

Theory

22. Let H^*, H, and K be subgroups of G with H^* normal in H. Show that $H^* \cap K$ is normal in $H \cap K$.

23. Show that if

$$H_0 = \{e\} < H_1 < H_2 < \cdots < H_n = G$$

is a subnormal (normal) series for a group G, and if H_{i+1}/H_i is of finite order s_{i+1}, then G is of finite order $s_1 s_2 \cdots s_n$.

24. Show that an infinite abelian group can have no composition series. [*Hint:* Use Exercise 23, together with the fact that an infinite abelian group always has a proper nontrivial subgroup.]

25. Show that a finite direct product of solvable groups is solvable.

26. Show that if $H \trianglelefteq G$ is a normal subgroup, H is solvable, and G/H is solvable, then G is solvable.

27. Show that for $n \geq 3$, D_n is solvable.

28. Show that a subgroup K of a solvable group G is solvable. [*Hint:* Let $H_0 = \{e\} < H_1 < \cdots < H_n = G$ be a composition series for G. Show that the distinct groups among $K \cap H_i$ for $i = 0, \cdots, n$ form a composition series for K. Observe that

$$(K \cap H_i)/(K \cap H_{i-1}) \simeq [H_{i-1}(K \cap H_i)]/[H_{i-1}],$$

by Theorem 16.5, with $H = K \cap H_i$ and $N = H_{i-1}$, and that $H_{i-1}(K \cap H_i) \leq H_i$.]

29. Let $H_0 = \{e\} < H_1 < \cdots < H_n = G$ be a composition series for a group G. Let N be a normal subgroup of G, and suppose that N is a simple group. Show that the distinct groups among H_0, H_iN for $i = 0, \cdots, n$ also form a composition series for G. [*Hint:* H_iN is a group by Lemma 16.4. Show that $H_{i-1}N$ is normal in H_iN. By Theorem 16.5

$$(H_iN)/(H_{i-1}N) \simeq H_i/[H_i \cap (H_{i-1}N)],$$

and the latter group is isomorphic to

$$[H_i/H_{i-1}]/[(H_i \cap (H_{i-1}N))/H_{i-1}],$$

by Theorem 16.8. But H_i/H_{i-1} is simple.]

30. Let G be a group, and let $H_0 = \{e\} < H_1 < \cdots < H_n = G$ be a composition series for G. Let N be a normal subgroup of G, and let $\gamma : G \to G/N$ be the canonical map. Show that the distinct groups among $\gamma[H_i]$ for $i = 0, \cdots, n$, form a composition series for G/N. [*Hint:* Observe that the map

$$\psi : H_iN \to \gamma[H_i]/\gamma[H_{i-1}]$$

defined by

$$\psi(h_in) = \gamma(h_in)\gamma[H_{i-1}]$$

is a homomorphism with kernel $H_{i-1}N$. By Theorem 16.2.

$$\gamma[H_i]/\gamma[H_{i-1}] \simeq (H_iN)/(H_{i-1}N).$$

Proceed via Theorem 16.5, as shown in the hint for Exercise 29.]

31. Prove that a homomorphic image of a solvable group is solvable. [*Hint:* Apply Exercise 30 to get a composition series for the homomorphic image. The hints for Exercises 29 and 30 then show how the factor groups of this composition series in the image look.]

32. Prove that a finite p-group is solvable.

33. Prove that a group G with $2^n p^k$ elements is solvable if $p > 2^n$ is a prime.

SECTION 19 Free Abelian Groups

In this section we introduce the concept of free abelian groups and prove some results concerning them. The section concludes with a demonstration of the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 9.12).

Free Abelian Groups

We should review the notions of a generating set for a group G and a finitely generated group, as given in Section 7. In this section we shall deal exclusively with abelian groups and use the standard additive notations as follows:

$$\begin{aligned}
&0 \text{ for the identity, } + \text{ for the operation,}\\
&\left.\begin{aligned} na &= \underbrace{a + a + \cdots + a}_{n \text{ summands}} \\ -na &= \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ summands}} \end{aligned}\right\} \text{ for } n \in \mathbb{Z}^+ \text{ and } a \in G.\\
&0a = 0 \text{ for the first 0 in } \mathbb{Z} \text{ and the second in } G.
\end{aligned}$$

We shall continue to use the symbol × for direct product of groups rather than change to direct sum notation.

Notice that $\{(1, 0), (0, 1)\}$ is a generating set for the group $\mathbb{Z} \times \mathbb{Z}$ since $(n, m) = n(1, 0) + m(0, 1)$ for any (n, m) in $\mathbb{Z} \times \mathbb{Z}$. This generating set has the property that each element of $\mathbb{Z} \times \mathbb{Z}$ can be *uniquely* expressed in the form $n(1, 0) + m(0, 1)$. That is, the coefficients n and m in $\mathbb{Z}$ are unique.

19.1 Theorem Let X be a subset of a nonzero abelian group G. The following conditions on X are equivalent.

1. Each nonzero element a in G can be expressed *uniquely* (up to order of summands) in the form $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ for $n_i \neq 0$ in $\mathbb{Z}$ and distinct x_i in X.
2. X generates G, and $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ for $n_i \in \mathbb{Z}$ and distinct $x_i \in X$ if and only if $n_1 = n_2 = \cdots = n_r = 0$.

Proof Suppose Condition 1 is true. Since $G \neq \{0\}$, we have $X \neq \{0\}$. It follows from 1 that $0 \notin X$, for if $x_i = 0$ and $x_j \neq 0$, then $x_j = x_i + x_j$, which would contradict the uniqueness of the expression for x_j. From Condition 1, X generates G, and $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ if $n_1 = n_2 = \cdots = n_r = 0$. Suppose that $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ with some $n_i \neq 0$; by dropping terms with zero coefficients and renumbering, we can assume all $n_i \neq 0$. Then

$$\begin{aligned} x_1 &= x_1 + (n_1x_1 + n_2x_2 + \cdots + n_rx_r) \\ &= (n_1 + 1)x_1 + n_2x_2 + \cdots + n_rx_r, \end{aligned}$$

which gives two ways of writing $x_1 \neq 0$, contradicting the uniqueness assumption in Condition 1. Thus Condition 1 implies Condition 2.

We now show that Condition 2 implies Condition 1. Let $a \in G$. Since X generates G, we see a can be written in the form $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$. Suppose a has another such expression in terms of elements of X. By using some zero coefficients in the two expressions, we can assume they involve the same elements in X and are of the form

$$a = n_1x_1 + n_2x_2 + \cdots n_rx_r$$
$$a = m_1x_1 + m_2x_2 + \cdots m_rx_r.$$

Subtracting, we obtain

$$0 = (n_1 - m_1)x_1 + (n_2 - m_2)x_2 + \cdots + (n_r - m_r)x_r,$$

so $n_i - m_i = 0$ by Condition 2, and $n_i = m_i$ for $i = 1, 2, \cdots, r$. Thus the coefficients are unique. ◆

19.2 Definition An abelian group having a generating set X satisfying the conditions described in Theorem 19.1 is a **free abelian group**, and X is a **basis** for the group. ■

19.3 Example The group $\mathbb{Z} \times \mathbb{Z}$ is free abelian and {(1, 0), (0, 1)} is a basis. Similarly, a basis for the free abelian group $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is {(1, 0, 0), (0, 1, 0), (0, 0, 1)}, and so on. Thus finite direct products of the group $\mathbb{Z}$ with itself are free abelian groups. ▲

19.4 Example The group $\mathbb{Z}_n$ is not free abelian, for $nx = 0$ for every $x \in \mathbb{Z}_n$, and $n \neq 0$, which would contradict Condition 2. ▲

From Example 19.4 it seems reasonable that if G is an abelian group with a nonzero element of finite order, then G is not a free abelian group. Exercise 10 asks you to provide a proof of this fact. However, there are other obstacles that prevent an abelian group from being free. For example, no rational number other than 0 has finite order, but Exercise 13 asks for a proof that $\mathbb{Q}$ is not a free abelian group.

Suppose a free abelian group G has a finite basis $X = \{x_1, x_2, \cdots, x_r\}$. If $a \in G$ and $a \neq 0$, then a has a *unique* expression of the form

$$a = n_1x_1 + n_2x_2 + \cdots + n_rx_r \quad \text{for} \quad n_i \in \mathbb{Z}.$$

(Note that in the preceding expression for a, we included all elements x_i of our finite basis X, as opposed to the expression for a in Condition 1 of Theorem 19.1 where the basis may be infinite. Thus in the preceding expression for a we must allow the possibility that some of the coefficients n_i are zero, whereas in Condition 1 of Theorem 19.1, we specified that each $n_i \neq 0$.)
We define

$$\phi : G \to \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ factors}}$$

by $\phi(a) = (n_1, n_2, \cdots, n_r)$ and $\phi(0) = (0, 0, \cdots, 0)$. It is straightforward to check that ϕ is an isomorphism. We leave the details to the exercises (see Exercise 9) and state the result as a theorem.

19.5 Theorem If G is a nonzero free abelian group with a basis of r elements, then G is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for r factors.

It is a fact that any two bases of a free abelian group G contain the same number of elements. We shall prove this only if G has a finite basis, although it is also true if every basis of G is infinite. The proof is really lovely; it gives an easy characterization of the number of elements in a basis in terms of the size of a factor group.

19.6 Theorem Let $G \neq \{0\}$ be a free abelian group with a finite basis. Then every basis of G is finite, and all bases of G have the same number of elements.