13. An abstract algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead, one of the nine integers was inadvertently left out, so that the list appeared as 1, 9, 16, 22, 53, 74, 79, 81. Which integer was left out? (This really happened!)
14. Let G be a group with the following property: Whenever a, b, and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian. ("Cross cancellation" implies commutativity.)
15. (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?
16. (Socks-Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$.
17. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.
18. Prove that in a group, $(a^{-1})^{-1} = a$ for all a.
19. For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.
20. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?
21. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12.
22. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.
23. Prove that every group table is a *Latin square*[†]; that is, each element of the group appears exactly once in each row and each column. (This exercise is referred to in this chapter.)
24. Construct a Cayley table for $U(12)$.
25. Suppose the table below is a group table. Fill in the blank entries.

	e	a	b	c	d
e	e	—	—	—	—
a	—	b	—	—	e
b	—	c	d	e	—
c	—	d	—	a	b
d	—	—	—	—	—

[†]Latin squares are useful in designing statistical experiments. There is also a close connection between Latin squares and finite geometries.

26. Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$.

27. Let a, b, and c be elements of a group. Solve the equation $axb = c$ for x. Solve $a^{-1}xa = c$ for x.

28. Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.

29. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

30. Give an example of a group with elements a, b, c, d, and x such that $axb = cxd$ but $ab \neq cd$. (Hence "middle cancellation" is not valid in groups.)

31. Let R be any rotation in some dihedral group and F any reflection in the same group. Prove that $RFR = F$.

32. Let R be any rotation in some dihedral group and F, any reflection in the same group. Prove that $FRF = R^{-1}$ for all integers k.

33. Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian. ("Middle cancellation" implies commutativity.)

34. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.

a. In D_4, $FR^{-2}FR^5$

b. In D_5, $R^{-3}FR^4FR^{-2}$

c. In D_6, $FR^5FR^{-2}F$

35. Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian. (This exercise is referred to in Chapter 26.)

36. Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group. (Multiplication is defined by

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{bmatrix}.$$

This group, sometimes called the *Heisenberg group* after the Nobel Prize–winning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of quantum physics.)

37. Prove the assertion made in Example 19 that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime.

38. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

39. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinant. (Compare with Example 10.)

Computer Exercises

Almost immediately after the war, Johnny [Von Neumann] and I also began to discuss the possibilities of using computers heuristically to try to obtain insights into questions of pure mathematics. By producing examples and by observing the properties of special mathematical objects, one could hope to obtain clues as to the behavior of general statements which have been tested on examples.

S. M. ULAM, *Adventures of a Mathematician*

Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

1. This software prints the elements of $U(n)$ and the inverse of each element.
2. This software determines the size of $U(k)$. Run the program for $k = 9, 27, 81, 243, 25, 125, 49, 121$. On the basis of this output, try to guess a formula for the size of $U(p^n)$ as a function of the prime p and the integer n. Run the program for $k = 18, 54, 162, 486, 50, 250, 98, 242$. Make a conjecture about the relationship between the size of $U(2p^n)$ and the size of $U(p^n)$, where p is a prime greater than 2.
3. This software computes the inverse of any element in $GL(2, Z_p)$, where p is a prime.
4. This software determines the number of elements in $GL(2, Z_p)$ and $SL(2, Z_p)$. (The technical term for the number of elements in a group is the *order* of the group.) Run the program for $p = 3, 5, 7$, and 11.

Do you see a relationship between the orders of $GL(2, Z_p)$ and $SL(2, Z_p)$ and $p - 1$? Does this relationship hold for $p = 2$? Based on these examples, does it appear that p always divides the order of $SL(2, Z_p)$? What about $p - 1$? What about $p + 1$? Guess a formula for the order of $SL(2, Z_p)$. Guess a formula for the order of $GL(2, Z_p)$.

References

1. Max Born, *My Life: Recollections of a Nobel Laureate*, New York: Charles Scribner's Sons, 1978.
2. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, Vol. 3, New York: Springer-Verlag, 1982.

Suggested Readings

Marcia Ascher, *Ethnomathematics*, Pacific Grove, CA: Brooks/Cole, 1991.

Chapter 3 of this book describes how the dihedral group of order 8 can be used to encode the social structure of the kin system of family relationships among a tribe of native people of Australia.

Arie Bialostocki, "An Application of Elementary Group Theory to Central Solitaire," *The College Mathematics Journal*, May 1998: 208–212.

The author uses properties of groups to analyze the peg board game central solitaire (which also goes by the name peg solitaire).

J. E. White, "Introduction to Group Theory for Chemists," *Journal of Chemical Education* 44 (1967): 128–135.

Students interested in the physical sciences may find this article worthwhile. It begins with easy examples of groups and builds up to applications of group theory concepts and terminology to chemistry.