Fraleigh Excerpts

April 15, 2023

of ambiguity, $*$ is **not well defined**. If Condition 2 is violated, then S is **not closed under** $*$.

Following are several illustrations of attempts to define binary operations on sets. Some of them are worthless. The symbol $*$ is used for the attempted operation in all these examples.

2.19 Example On $\mathbb{Q}$, let $a * b = a/b$. Here $*$ is *not everywhere defined* on $\mathbb{Q}$, for no rational number is assigned by this rule to the pair (2, 0). ▲

2.20 Example On $\mathbb{Q}^+$, let $a * b = a/b$. Here both Conditions 1 and 2 are satisfied, and $*$ is a binary operation on $\mathbb{Q}^+$. ▲

2.21 Example On $\mathbb{Z}^+$, let $a * b = a/b$. Here Condition 2 fails, for $1 * 3$ is not in $\mathbb{Z}^+$. Thus $*$ is not a binary operation on $\mathbb{Z}^+$, since $\mathbb{Z}^+$ is *not closed under* $*$. ▲

2.22 Example Let F be the set of all real-valued functions with domain $\mathbb{R}$ as in Example 2.7. Suppose we "define" $*$ to give the usual quotient of f by g, that is, $f * g = h$, where $h(x) = f(x)/g(x)$. Here Condition 2 is violated, for the functions in F were to be defined for *all* real numbers, and for some $g \in F$, $g(x)$ will be zero for some values of x in $\mathbb{R}$ and $h(x)$ would not be defined at those numbers in $\mathbb{R}$. For example, if $f(x) = \cos x$ and $g(x) = x^2$, then $h(0)$ is undefined, so $h \notin F$. ▲

2.23 Example Let F be as in Example 2.22 and let $f * g = h$, where h is the function greater than both f and g. This "definition" is completely worthless. In the first place, we have not defined what it means for one function to be greater than another. Even if we had, any sensible definition would result in there being many functions greater than both f and g, and $*$ would still be *not well defined.* ▲

2.24 Example Let S be a set consisting of 20 people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the tallest person among the 20 in S. This is a perfectly good binary operation on the set, although not a particularly interesting one. ▲

2.25 Example Let S be as in Example 2.24 and let $a * b = c$, where c is the shortest person in S who is taller than both a and b. This $*$ is *not everywhere defined,* since if either a or b is the tallest person in the set, $a * b$ is not determined. ▲

EXERCISES 2

Computations

Exercises 1 through 4 concern the binary operation $*$ defined on $S = \{a, b, c, d, e\}$ by means of Table 2.26.

1. Compute $b * d$, $c * c$, and $[(a * c) * e] * a$.
2. Compute $(a * b) * c$ and $a * (b * c)$. Can you say on the basis of this computations whether $*$ is associative?
3. Compute $(b * d) * c$ and $b * (d * c)$. Can you say on the basis of this computation whether $*$ is associative?

2.26 Table

$*$	a	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

2.27 Table

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

2.28 Table

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

4. Is $*$ commutative? Why?

5. Complete Table 2.27 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d\}$.

6. Table 2.28 can be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries.

In Exercises 7 through 11, determine whether the binary operation $*$ defined is commutative and whether $*$ is associative.

7. $*$ defined on $\mathbb{Z}$ by letting $a * b = a - b$

8. $*$ defined on $\mathbb{Q}$ by letting $a * b = ab + 1$

9. $*$ defined on $\mathbb{Q}$ by letting $a * b = ab/2$

10. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = 2^{ab}$

11. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = a^b$

12. Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.

13. How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements?

Concepts

In Exercises 14 through 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.

14. A binary operation $*$ is *commutative* if and only if $a * b = b * a$.

15. A binary operation $*$ on a set S is *associative* if and only if, for all $a, b, c \in S$, we have $(b * c) * a = b * (c * a)$.

16. A subset H of a set S is *closed* under a binary operation $*$ on S if and only if $(a * b) \in H$ for all $a, b \in S$.

In Exercises 17 through 22, determine whether the definition of $*$ does give a binary operation on the set. In the event that $*$ is not a binary operation, state whether Condition 1, Condition 2, or both of these conditions on page 24 are violated.

17. On $\mathbb{Z}^+$, define $*$ by letting $a * b = a - b$.

18. On $\mathbb{Z}^+$, define $*$ by letting $a * b = a^b$.

19. On $\mathbb{R}$, define $*$ by letting $a * b = a - b$.

20. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is the smallest integer greater than both a and b.

Now suppose that G' is any other group of three elements and imagine a table for G' with identity element appearing first. Since our filling out of the table for $G = \{e, a, b\}$ could be done in only one way, we see that if we take the table for G' and rename the identity e, the next element listed a, and the last element b, the resulting table for G' must be the same as the one we had for G. As explained in Section 3, this renaming gives an isomorphism of the group G' with the group G. Definition 3.7 defined the notion of *isomorphism* and of *isomorphic binary structures*. Groups are just certain types of binary structures, so the same definition pertains to them. Thus our work above can be summarized by saying that all groups with a single element are isomorphic, all groups with just two elements are isomorphic, and all groups with just three elements are isomorphic. We use the phrase *up to isomorphism* to express this identification using the equivalence relation $\simeq$. Thus we may say, "There is only one group of three elements, up to isomorphism."

4.19 Table

$*$	e	a
e	e	a
a	a	e

4.20 Table

$*$	e	a	b
e	e	a	b
a	a		
b	b		

4.21 Table

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

EXERCISES 4

Computations

In Exercises 1 through 6, determine whether the binary operation $*$ gives a group structure on the given set. If no group results, give the first axiom in the order $\mathscr{G}_1$, $\mathscr{G}_2$, $\mathscr{G}_3$ from Definition 4.1 that does not hold.

1. Let $*$ be defined on $\mathbb{Z}$ by letting $a * b = ab$.
2. Let $*$ be defined on $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ by letting $a * b = a + b$.
3. Let $*$ be defined on $\mathbb{R}^+$ by letting $a * b = \sqrt{ab}$.
4. Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$.
5. Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by letting $a * b = a/b$.
6. Let $*$ be defined on $\mathbb{C}$ by letting $a * b = |ab|$.
7. Give an example of an abelian group G where G has exactly 1000 elements.
8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4(7) + 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.
9. Show that the group $\langle U, \cdot\rangle$ is not isomorphic to either $\langle \mathbb{R}, +\rangle$ or $\langle \mathbb{R}^*, \cdot\rangle$. (All three groups have cardinality $|\mathbb{R}|$.)
10. Let n be a positive integer and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.

    a. Show that $\langle n\mathbb{Z}, +\rangle$ is a group.

    b. Show that $\langle n\mathbb{Z}, +\rangle \simeq \langle \mathbb{Z}, +\rangle$.

In Exercises 11 through 18, determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group. Recall that a **diagonal matrix** is a square matrix whose only nonzero entries lie on the **main diagonal,** from the upper left to the lower right corner. An **upper-triangular matrix** is a square matrix with only zero entries below the main diagonal. Associated with each $n \times n$ matrix A is a number called the determinant of A, denoted by $\det(A)$. If A and B are both $n \times n$ matrices, then $\det(AB) = \det(A)\det(B)$. Also, $\det(I_n) = 1$ and A is invertible if and only if $\det(A) \neq 0$.

11. All $n \times n$ diagonal matrices under matrix addition.

12. All $n \times n$ diagonal matrices under matrix multiplication.

13. All $n \times n$ diagonal matrices with no zero diagonal entry under matrix multiplication.

14. All $n \times n$ diagonal matrices with all diagonal entries 1 or -1 under matrix multiplication.

15. All $n \times n$ upper-triangular matrices under matrix multiplication.

16. All $n \times n$ upper-triangular matrices under matrix addition.

17. All $n \times n$ upper-triangular matrices with determinant 1 under matrix multiplication.

18. All $n \times n$ matrices with determinant either 1 or -1 under matrix multiplication.

19. Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab.$$

a. Show that $*$ gives a binary operation on S.

b. Show that $\langle S, *\rangle$ is a group.

c. Find the solution of the equation $2 * x * 3 = 7$ in S.

20. This exercise shows that there are two nonisomorphic group structures on a set of 4 elements.

Let the set be $\{e, a, b, c\}$, with e the identity element for the group operation. A group table would then have to start in the manner shown in Table 4.22. The square indicated by the question mark cannot be filled in with a. It must be filled in either with the identity element e or with an element different from both e and a. In this latter case, it is no loss of generality to assume that this element is b. If this square is filled in with e, the table can then be completed in two ways to give a group. Find these two tables. (You need not check the associative law.) If this square is filled in with b, then the table can only be completed in one way to give a group. Find this table. (Again, you need not check the associative law.) Of the three tables you now have, two give isomorphic groups. Determine which two tables these are, and give the one-to-one onto renaming function which is an isomorphism.

a. Are all groups of 4 elements commutative?

b. Which table gives a group isomorphic to the group U_4, so that we know the binary operation defined by the table is associative?

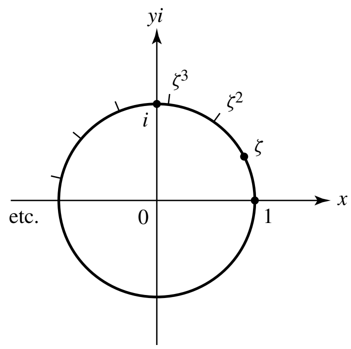
c. Show that the group given by one of the other tables is structurally the same as the group in Exercise 14 for one particular value of n, so that we know that the operation defined by that table is associative also.

21. According to Exercise 12 of Section 2, there are 16 possible binary operations on a set of 2 elements. How many of these give a structure of a group? How many of the 19,683 possible binary operations on a set of 3 elements give a group structure?

Concepts

22. Consider our axioms $\mathscr{G}_1$, $\mathscr{G}_2$, and $\mathscr{G}_3$ for a group. We gave them in the order $\mathscr{G}_1\mathscr{G}_2\mathscr{G}_3$. Conceivable other orders to state the axioms are $\mathscr{G}_1\mathscr{G}_3\mathscr{G}_2$, $\mathscr{G}_2\mathscr{G}_1\mathscr{G}_3$, $\mathscr{G}_2\mathscr{G}_3\mathscr{G}_1$, $\mathscr{G}_3\mathscr{G}_1\mathscr{G}_2$, and $\mathscr{G}_3\mathscr{G}_2\mathscr{G}_1$. Of these six possible

The geometric interpretation of multiplication of complex numbers, explained in Section 1, shows at once that as ζ is raised to powers, it works its way counterclockwise around the circle, landing on each of the elements of U_n in turn. Thus U_n under multiplication is a cyclic group, and ζ is a generator. The group U_n is the cyclic subgroup $\langle\zeta\rangle$ of the group U of all complex numbers z, where $|z| = 1$, under multiplication. ▲



5.24 Figure

EXERCISES 5

Computations

In Exercises 1 through 6, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. $\mathbb{R}$ **2.** $\mathbb{Q}^+$ **3.** $7\mathbb{Z}$

4. The set $i\mathbb{R}$ of pure imaginary numbers including 0

5. The set $\pi\mathbb{Q}$ of rational multiples of π **6.** The set $\{\pi^n \mid n \in \mathbb{Z}\}$

7. Which of the sets in Exercises 1 through 6 are subgroups of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication?

In Exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

8. The $n \times n$ matrices with determinant 2

9. The diagonal $n \times n$ matrices with no zeros on the diagonal

10. The upper-triangular $n \times n$ matrices with no zeros on the diagonal

11. The $n \times n$ matrices with determinant -1

12. The $n \times n$ matrices with determinant -1 or 1

13. The set of all $n \times n$ matrices A such that $(A^T)A = I_n$. [These matrices are called **orthogonal.** Recall that A^T, the *transpose* of A, is the matrix whose jth column is the jth row of A for $1 \leq j \leq n$, and that the transpose operation has the property $(AB)^T = (B^T)(A^T)$.]

Let F be the set of all real-valued functions with domain $\mathbb{R}$ and let $\tilde{F}$ be the subset of F consisting of those functions that have a nonzero value at every point in $\mathbb{R}$. In Exercises 14 through 19, determine whether the given subset of F with the induced operation is (a) a subgroup of the group F under addition, (b) a subgroup of the group $\tilde{F}$ under multiplication.

14. The subset $\tilde{F}$

15. The subset of all $f \in F$ such that $f(1) = 0$

16. The subset of all $f \in \tilde{F}$ such that $f(1) = 1$

17. The subset of all $f \in \tilde{F}$ such that $f(0) = 1$

18. The subset of all $f \in \tilde{F}$ such that $f(0) = -1$

19. The subset of all constant functions in F.

20. Nine groups are given below. Give a *complete* list of all subgroup relations, of the form $G_i \leq G_j$, that exist between these given groups $G_1, G_2, \cdots, G_9$.
$G_1 = \mathbb{Z}$ under addition
$G_2 = 12\mathbb{Z}$ under addition
$G_3 = \mathbb{Q}^+$ under multiplication
$G_4 = \mathbb{R}$ under addition
$G_5 = \mathbb{R}^+$ under multiplication
$G_6 = \{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication
$G_7 = 3\mathbb{Z}$ under addition
$G_8 =$ the set of all integral multiples of 6 under addition
$G_9 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication

21. Write at least 5 elements of each of the following cyclic groups.

a. $25\mathbb{Z}$ under addition
b. $\{(\frac{1}{2})^n \mid n \in \mathbb{Z}\}$ under multiplication
c. $\{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication

In Exercises 22 through 25, describe all the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by the given 2×2 matrix.

22. $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ **23.** $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ **24.** $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ **25.** $\begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$

26. Which of the following groups are cyclic? For each cyclic group, list all the generators of the group.

$$G_1 = \langle \mathbb{Z}, + \rangle \quad G_2 = \langle \mathbb{Q}, + \rangle \quad G_3 = \langle \mathbb{Q}^+, \cdot \rangle \quad G_4 = \langle 6\mathbb{Z}, + \rangle$$
$$G_5 = \{6^n \mid n \in \mathbb{Z}\} \text{ under multiplication}$$
$$G_6 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ under addition}$$

In Exercises 27 through 35, find the order of the cyclic subgroup of the given group generated by the indicated element.

27. The subgroup of $\mathbb{Z}_4$ generated by 3

28. The subgroup of V generated by c (see Table 5.11)

29. The subgroup of U_6 generated by $\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$

30. The subgroup of U_5 generated by $\cos \frac{4\pi}{5} + i \sin \frac{4\pi}{5}$

31. The subgroup of U_8 generated by $\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}$

EXERCISES 6

Computations

In Exercises 1 through 4, find the quotient and remainder, according to the division algorithm, when n is divided by m.

1. $n = 42, m = 9$

2. $n = -42, m = 9$

3. $n = -50, m = 8$

4. $n = 50, m = 8$

In Exercises 5 through 7, find the greatest common divisor of the two integers.

5. 32 and 24 **6.** 48 and 88 **7.** 360 and 420

In Exercises 8 through 11, find the number of generators of a cyclic group having the given order.

8. 5 **9.** 8 **10.** 12 **11.** 60

An isomorphism of a group with itself is an **automorphism of the group.** In Exercises 12 through 16, find the number of automorphisms of the given group.
[*Hint:* Make use of Exercise 44. What must be the image of a generator under an automorphism?]

12. $\mathbb{Z}_2$ **13.** $\mathbb{Z}_6$ **14.** $\mathbb{Z}_8$ **15.** $\mathbb{Z}$ **16.** $\mathbb{Z}_{12}$

In Exercises 17 through 21, find the number of elements in the indicated cyclic group.

17. The cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25

18. The cyclic subgroup of $\mathbb{Z}_{42}$ generated by 30

19. The cyclic subgroup $\langle i \rangle$ of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication

20. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $(1 + i)/\sqrt{2}$

21. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $1 + i$

In Exercises 22 through 24, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

22. $\mathbb{Z}_{12}$ **23.** $\mathbb{Z}_{36}$ **24.** $\mathbb{Z}_8$

In Exercises 25 through 29, find all orders of subgroups of the given group.

25. $\mathbb{Z}_6$ **26.** $\mathbb{Z}_8$ **27.** $\mathbb{Z}_{12}$ **28.** $\mathbb{Z}_{20}$ **29.** $\mathbb{Z}_{17}$

Concepts

In Exercises 30 and 31, 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.

30. An element a of a group G has *order* $n \in \mathbb{Z}^+$ if and only if $a^n = e$.

31. The *greatest common divisor* of two positive integers is the largest positive integer that divides both of them.

32. Mark each of the following true or false.

_______ **a.** Every cyclic group is abelian.
_______ **b.** Every abelian group is cyclic.
_______ **c.** $\mathbb{Q}$ under addition is a cyclic group.
_______ **d.** Every element of every cyclic group generates the group.
_______ **e.** There is at least one abelian group of every finite order >0.
_______ **f.** Every group of order ≤ 4 is cyclic.

_______ **g.** All generators of $\mathbb{Z}_{20}$ are prime numbers.
_______ **h.** If G and G' are groups, then $G \cap G'$ is a group.
_______ **i.** If H and K are subgroups of a group G, then $H \cap K$ is a group.
_______ **j.** Every cyclic group of order >2 has at least two distinct generators.

In Exercises 33 through 37, either give an example of a group with the property described, or explain why no example exists.

33. A finite group that is not cyclic

34. An infinite group that is not cyclic

35. A cyclic group having only one generator

36. An infinite cyclic group having four generators

37. A finite cyclic group having four generators

The generators of the cyclic multiplicative group U_n of all nth roots of unity in $\mathbb{C}$ are the **primitive** nth **roots of unity**. In Exercises 38 through 41, find the primitive nth roots of unity for the given value of n.

38. $n = 4$

39. $n = 6$

40. $n = 8$

41. $n = 12$

Proof Synopsis

42. Give a one-sentence synopsis of the proof of Theorem 6.1.

43. Give at most a three-sentence synopsis of the proof of Theorem 6.6.

Theory

44. Let G be a cyclic group with generator a, and let G' be a group isomorphic to G. If $\phi : G \to G'$ is an isomorphism, show that, for every $x \in G$, $\phi(x)$ is completely determined by the value $\phi(a)$. That is, if $\phi : G \to G'$ and $\psi : G \to G'$ are two isomophisms such that $\phi(a) = \psi(a)$, then $\phi(x) = \psi(x)$ for all $x \in G$.

45. Let r and s be positive integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

46. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

47. Let r and s be positive integers.

a. Define the **least common multiple** of r and s as a generator of a certain cyclic group.

b. Under what condition is the least common multiple of r and s their product, rs?

c. Generalizing part (b), show that the product of the greatest common divisor and of the least common multiple of r and s is rs.

48. Show that a group that has only a finite number of subgroups must be a finite group.

49. Show by a counterexample that the following "converse" of Theorem 6.6 is not a theorem: "If a group G is such that every proper subgroup is cyclic, then G is cyclic."

50. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Show that $ax = xa$ for all $x \in G$. [*Hint:* Consider $(xax^{-1})^2$.]

51. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.