Discrete Structures: Question Bank

Group Theory

1. Which of the following binary operations are closed? In other words, if you perform the indicated operation below over the indicated set below, is the new element going to be in the indicated set?
   (a) subtraction of positive integers
   (b) division of nonzero integers
   (c) function composition of polynomials with real coefficients
   (d) multiplication of 2×2 matrices with integer entries
   (e) exponentiation of integers

2. Which of the following binary operations are associative?
   (a) subtraction of integers
   (b) division of nonzero rationals
   (c) function composition of polynomials with real coefficients
   (d) multiplication of 2×2 matrices with integer entries
   (e) exponentiation of integers

3. Which of the following binary operations are commutative?
   (a) substraction of integers
   (b) division of nonzero real numbers
   (c) function composition of polynomials with real coefficients
   (d) multiplication of 2×2 matrices with real entries
   (e) exponentiation of integers

4. Which of the following sets are closed under the given operation?
   (a) $\{0, 4, 8, 12\}$ addition mod 16
   (b) $\{0, 4, 8, 12\}$ addition mod 15
   (c) $\{1, 4, 7, 13\}$ multiplication mod 15
   (d) $\{1, 4, 5, 7\}$ multiplication mod 9

5. In each case, find the inverse of the element under the given operation.
   (a) 13 in $\mathbb{Z}_{20}$ under $+_{20}$
   (b) 13 in $\mathbb{Z}_{14}^*$ under $\times_{14}$. Recall: $\mathbb{Z}_n^* = \{1 \leq k \leq n \mid (k, n) = 1\}$
   (c) $n - 1$ in $\mathbb{Z}_n^*, n > 2$
   (d) $3-2i$ in $\mathbb{C}^*$, where $i^2 = -1$, the group of non-negative complex numbers under multiplication.

6. Give two reasons why the set of odd integers under addition is not a group.

7. List the elements of $\mathbb{Z}_{20}^*$.

8. Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

9. Let a belong to a group and $a^{12} = e$. Express the inverse of each of the elements a, a^6, a^8, and a^{11} in the form a^k for some positive integer k.

10. In $\mathbb{Z}_9^*$, find the inverse of 2,7 , and 8 .

11. Translate each of the following multiplicative expressions into its additive counterpart. Assume that the operation is commutative. For example $abcb = ab^2c$ (commut.) $= a + b + b + c$.
(a) a^2b^3
(b) $a^{-2}\left(b^{-1}c\right)^2$
(c) $\left(ab^2\right)^{-3}c^2 = e$

12. For group elements a, b, and c, express $(ab)^3$ and $\left(ab^{-2}c\right)^{-2}$ without parentheses.

13. Suppose a and b belong to a group and $a^5 = e$ and $b^7 = e$. Write $a^{-2}b^{-4}$ and $\left(a^2b^4\right)^{-2}$ without using negative exponents.

14. Show that a and b belong to a group and $a^5 = e$ and $b^7 = e$. Write $a^{-2}b^{-4}$ and $\left(a^2b^4\right)^{-2}$ without using negative exponents.

15. Show that the set $5, 15, 25, 35$ is a group under multiplication modulo 40 . What is the identity element of this group? Can you see any relationship between this group and $\mathbb{Z}_8^*$?

16. Let G be a group and let $H = \left\{x^{-1} \mid x \in G\right\}$. Show that $G = H$ as sets.

17. List the members of $K = \left\{x^2 \mid x \in D_4\right\}$ and $L = \left\{x \in D_4 \mid x^2 = e\right\}$.

18. An abstract algebra teacher intended to give a typist a list of nine in tegers 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?

19. Let G be a group with the property that for any x, y, z in the group, $xy = zx$ implies $y = z$. Prove that G is Abelian.

20. Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^{-1} = b^{-1}a^{-1}$. Is this also true for non-Abelian groups? Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$.

21. Show that group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

22. Show that in a group $\left(a^{-1}\right)^{-1} = a$ for all a.

23. For any elements a and b from a group and any integer n, prove that $\left(a^{-1}ba\right)^n = a^{-1}b^n a$.

24. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1a_2a_3 \ldots a_n$?

25. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12 .

26. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

27. Construct a Cayley table for $\mathbb{Z}^*(12)$. Note that Cayley table is a composition table of elements of the group.

28. Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

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

30. Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.

31. 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.

32. 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).

33. Find an element X in D_4 such that $R_{90}VXH = D'$.

34. Suppose F_1 and F_2 are distinct reflections in a dihaderal group D_n. Prove that $F_1F_2 \neq R_0$.

35. Prove that the set of 3×3 matrices

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

under ordinary matrix multiplication is a group. This group is called Heisenberg group. It is related to Heisenberg uncertainty principle of quantum mechanics.

36. Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian.

Subgroups

1. For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_{10}^*, \quad \mathbb{Z}_{12}^*, \quad \mathbb{Z}_{20}^*, \text{ and } \quad D_4.$$

   Here and in the following, $\mathbb{Z}_n^* = U(n) = \{1 \leq m \leq n-1 \mid \gcd(m,n) = 1\}$.

2. Let $\mathbb{Q}$ be the set of rational numbers under addition, and let $\mathbb{Q}^*$ be the set of rational numbers under multiplication. In $\mathbb{Q}$, list the elements in $\left\langle \frac{1}{2} \right\rangle$. In $\mathbb{Q}^*$, list the elements in $\left\langle \frac{1}{2} \right\rangle$.

3. Let $\mathbb{Q}$ and $\mathbb{Q}^*$ be as above. Find the order of each element in $\mathbb{Q}$ and $\mathbb{Q}^*$.

4. Prove that in any group, an element and its inverse have the same order.

5. Without actually computing the orders, explain why the two elements in each of the following pairs of elements from $\mathbb{Z}_{30}$ must have the same order: $\{2, 28\}, \{8, 22\}$. Do the same for the following pairs of elements from $\mathbb{Z}_{15}^*$: $\{2, 8\}, \{7, 13\}$.

6. In the group $\mathbb{Z}_{12}$, find $|a|, |b|$, and $|a+b|$ for each case.

   (a) $a = 6, b = 2$

   (b) $a = 3, b = 8$

   (c) $a = 5, b = 4$

   Do you see any relationship between $|a|, |b|$, and $|a+b|$?

7. If a, b, and c are group elements and $|a| = 6$ and $|b| = 7$, express $\left(a^4 c^{-2} b^4\right)^{-1}$ without using negative exponents.

8. How many subgroups of order 4 does D_4 have?

9. Determine all elements of finite order in $\mathbb{R}^*$, the group of non-zero real numbers.

10. Complete the statement: "A group element x is its own inverse if and only if $|x| =$ "

11. For any group elements a and x, prove that $\left|xax^{-1}\right| = |a|$.

12. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group. Recall that center of the group denoted by $Z(G)$ is defined as follows:

$$Z(G) = \{g \in G \mid gx = xg, \quad \forall x \in G\}$$

13. Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

14. If a is a group element and a has an infinite order, prove that $a^m \neq a^n$ when $m \neq n$.

15. For any group element a and b, prove that $|ab| = |ba|$.

16. Show that if a is an element of a group G, then $|a| \leq |G|$.

17. Show that $\mathbb{Z}_{14}^* = \langle 3 \rangle = \langle 5 \rangle$. Is $\mathbb{Z}_{14}^* = \langle 11 \rangle$?

18. Show that $\mathbb{Z}_{20}^* \neq \langle k \rangle$, for any $k \in \mathbb{Z}_{20}^*$.

19. Suppose n is an even positive integer and H is a subgroup of Z_n. Prove that either every member of H is even or exactly half of the members of H are even.

20. Let n be a positive even integer and let H be a subgroup of Z_n of odd order. Prove that every member of H is an even integer.

21. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

22. Suppose that H is a subgroup of $\mathbb{Z}$ under addition and that H contains 2^{50} and 3^{50}. What are the possibilities for H ?

23. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G.

24. Let G be an Abelian group and $H = \{x \in G || x \mid \text{is odd } \}$. Prove that H is a subgroup of G.

25. If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

26. Prove that a group of even order must have an odd number of elements of order 2.

27. Give an example of elements a and b from a group such that a has finite order, b has infinite order and ab has finite order.

28. In the group $\mathbb{R}^*$, find the elements a and b such that $|a| = \infty, |b| = \infty$, and $|ab| = 2$.

29. Prove that the subset of elements of finite order in an Abelian group forms a subgroup. (This subgroup is called the torsion subgroup.)

30. Compute the orders of the following groups.

    (a) $\mathbb{Z}_3^*, \mathbb{Z}_4^*, \mathbb{Z}_{12}^*$
    (b) $\mathbb{Z}_5^*, \mathbb{Z}_7^*, \mathbb{Z}_{35}^*$
    (c) $\mathbb{Z}_4^*, \mathbb{Z}_5^*, \mathbb{Z}_{20}^*$

(d) $\mathbb{Z}_3^*, \mathbb{Z}_5^*, \mathbb{Z}_{15}^*$

On the basis of your answer, make a conjecture about the relationship among $|\mathbb{Z}_r^*|, |\mathbb{Z}_s^*|$ and $\left|\mathbb{Z}_{(rs)}^*\right|$.

31. Let $\mathbb{R}^*$ be a group of non-zeros real numbers under multiplication anf let $H = \{x \in \mathbb{R}^* \mid x^2 \text{ is rational }\}$. Prove that H is a subgroup of $\mathbb{R}^*$. Can the exponent 2 be replaced by any positive integer and still have H be a subgroup?

32. Find a noncyclic group of order 4 in $\mathbb{Z}_{40}^*$.

33. Prove that a group of even order must have an element of order 2.

34. Let

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z} \right\}$$

under addition. Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \middle| \, a + b + c + d = 0 \right\}$$

Prove that H is a subgroup of G. What if 0 is replaced by 1 above?

Cyclic Group

1. Find all generators of $\mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{20}$.

2. Suppose that $\langle a \rangle, \langle b \rangle, \langle c \rangle$ are cyclic groups of orders 6, 8, and 20, respectively. Find all the generators of $\langle a \rangle, \langle b \rangle$, and $\langle c \rangle$.

3. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$. Let a be a group element of order 18. List the elements of the subgroup $\langle a^3 \rangle$ and $\langle a^{10} \rangle$.

4. Find an example of a cyclic group, all of whose proper subgroups are cyclic.

5. How many subgroups does $\mathbb{Z}_{20}$ have?

6. In $\mathbb{Z}_{24}$, list all the generators for subgroup order 8.

7. In $\mathbb{Z}$, find all the generators of the subgroup $\langle 3 \rangle$.

8. In $\mathbb{Z}_{24}$, find a generator for $\langle 21 \rangle \cap \langle 10 \rangle$.

9. Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is prime?

10. Let G be an Abelian group and let $H = \{g \in G || g \mid \text{divided } 12\}$. Prove that H is a subgroup of G. Is there anything special about 12 here?

11. Complete the statement: $|a| = \left|a^2\right|$ if and only if $|a| =$

12. If a cyclic group has an element of infinite order, how many elements of finite order it has?

13. Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation $x^{35} = e$. Prove that G is cyclic. Does your argument work if 35 is replaced with 33 ?

14. Prove that a group of order 3 must be cyclic.

15. List all the elements of order 8 in $\mathbb{Z}_{8000000}$. How do you know your list is complete?

16. Let G be a finite group. Show that there exists a fixed positive integer n such that $a^n = e$ for all a in G.

17. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

18. Let m and m be two elements of $\mathbb{Z}$. Find a generator for $\langle m \rangle \cap \langle n \rangle$.

Isomorphism

1. Find an isomorphism from the group of integers under addition to group of even integers under addition.

2. Show that $\mathbb{Z}_8^*$ is not isomorphic to $\mathbb{Z}_{10}^*$.

3. Show that $\mathbb{Z}_8^*$ is isomorphic to $\mathbb{Z}_{12}^*$.

4. Show that the map $a \to \log_{10} a$ is a nisomorphism from $\mathbb{R}^+$under multiplication to $\mathbb{R}$ under addition.

5. Let G be a group under addition and $\bar{G}$ be a group under addition and ϕ be an isomorphism from G to $\bar{G}$. If $\phi(a) = \bar{a}$ and $\phi(b) = \bar{b}$, find an expression for $\phi\left(a^3 b^{-2}\right)$ in terms of $\bar{a}$ and $\bar{b}$.

6. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g \in G$ is an automorphism (automorphism is an isomorphism from the group to itself) if and only if G is Abelian.

7. Show that $\mathbb{Z}$ has infinitely many subgroups isomorphic to $\mathbb{Z}$.

8. Identify a group G that has subgroups isomorphic to $\mathbb{Z}_n$ for all positive integer n.

9. Prove or disprove that $\mathbb{Z}_{20}^*$ and $\mathbb{Z}_{24}^*$ are isomorphic.

10. Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

11. Prove that $\mathbb{Q}$, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

12. Prove that Q^+, the group of positive rational numbers under multiplication, is isomorphic to a proper subgroup of itself.

Cosets, Lagrange's theorem

1. Let $H = \{0, \pm 1, \pm 3, \pm 6, \ldots\}$. Find all the left cosets of H in $\mathbb{Z}$.

2. Are the following cosets same?

    1. $11 + H = 17 + H$
    2. $-1 + H = 5 + H$

3. Find all the left cosets of $\{1, 11\}$ in $\mathbb{Z}_{30}^*$

4. Suppose that a has order 15. Find all the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

5. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there?

6. Let a and b be elements of a group G and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.

7. If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.

8. Let a and b be non identity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

9. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H ?

10. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

11. Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.

12. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5 , prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.

13. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?

14. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.

15. Suppose that a group contains elements of orders 1 through 10 . What is the minimum possible order of the group?

16. Prove that a group of order 63 must have an element of order 3.

Rings

1. Give an example of a finite noncommutative ring. Give an example of an infinite noncommutative ring that does not have a unity.

2. The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. Find it.

3. Give an example of a subset of a ring that is a subgroup under addition but not a subring.

4. Find an integer n that shows that the rings $\mathbb{Z}_n$ need not have the following properties that the ring of integers has.

   (a) $a^2 = a$ implies $a = 0$ or $a = 1$

   (b) $ab = 0$ implies $a = 0$ or $b = 0$

   (c) $ab = ac$ and $a \neq 0$ implies $b = c$

   Is the n you found prime?

5. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$.

6. Prove that the intersection of any collection of subrings of a ring R is a subring of R.

7. Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that b divides c if and only if ab divides c.

8. Describe all the subrings of the ring of integers.

9. Let a and b belong to a ring R and let m be an integer. Prove that $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$.

10. Show that if m and n are integers and a and b are elements from a ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

11. Show that a ring that is cyclic under addition is commutative.

12. Show that a unit of a ring divides every element of the ring.

13. Suppose that a and b belong to a commutative ring R with unity. If a is a unit of R and $b^2 = 0$, show that $a + b$ is a unit of R.

14. Give an example of a ring with a property that $ab = 0$ but $ba \neq 0$.

15. Let n be an integer greater than 1 . In a ring in which $x^n = x$ for all x, show that $ab = 0$ implies $ba = 0$.

16. Suppose that R is a ring such that $x^3 = x$ for all $x \in R$. Prove that $6x = 0$ for all $x \in R$.

17. Let R be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$ if and only if R is commutative.

18. Suppose that R is a ring and $a^2 = a$ for all $a \in R$. Show that R is commutative.

19. Let R be a commutative ring with more than one element. Prove that if for every nonzero element a of R we have $aR = R$, then R has a unity and every nonzero element has an inverse.

20. Suppose that R is a ring with no zero-divisors and that R contains a nonzero element b such that $b^2 = b$. Show that b is the unity for R.

Integral Domains and Fields

1. Show that a commutative ring with the cancellation property (under multiplication) has no zerodivisors.

2. List all zero-divisors in Z_{20}. Can you see a relationship between the zero-divisors of Z_{20} and the units of Z_{20} ?

3. Show that every nonzero element of Z_n is a unit or a zero-divisor.

4. Find a nonzero element in a ring that is neither a zero-divisor nor a unit.

5. Let R be a finite commutative ring with unity. Prove that every non- zero element of R is either a zero-divisor or a unit. What happens if we drop the "finite" condition on R ?

6. Let $a \neq 0$ belong to a commutative ring. Prove that a is a zero- divisor if and only if $a^2 b = 0$ for some $b \neq 0$.

7. Give an example of a commutative ring without zero-divisors that is not an integral domain.

8. Find two elements a and b in a ring such that both a and b are zero-divisors, $a + b \neq 0$, and $a + b$ is not a zero-divisor.

9. A ring element a is called an idempotent if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

10. Let a and b be idempotents in a commutative ring. Show that each of the following is also an idempotent: $ab, a - ab, a + b - ab, a + b - 2ab$.

11. Let $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field.

12. Prove that there is no integral domain with exactly six elements.