MATH 417, HOMEWORK 1

CHARLES ANCEL

Chapter I.4

Exercise 2. 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 $\mathcal{G}1, \mathcal{G}2, \mathcal{G}3$ from Definition 4.1 that does not hold.

Let $*$ be defined on $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ by letting $a * b = a + b$.

Proof. To determine whether the binary operation $*$ gives a group structure on the given set, we need to check the group axioms. Let's enumerate them:

(1) **Associativity ($\mathcal{G}1$):** For all a, b, c in the set, $(a * b) * c = a * (b * c)$.

(2) **Identity ($\mathcal{G}2$):** There exists an identity element e in the set such that for every element a in the set, $e * a = a * e = a$.

(3) **Inverse ($\mathcal{G}3$):** For every element a in the set, there exists an inverse a^{-1} such that $a * a^{-1} = a^{-1} * a = e$.

Given the definitions of $\mathcal{G}1, \mathcal{G}2$, and $\mathcal{G}3$ as provided, let's determine whether the binary operation $*$ gives a group structure on the set $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ with the operation defined as $a * b = a + b$.

For the set $2\mathbb{Z}$:

1. **Associativity ($\mathcal{G}1$):** The operation is just ordinary addition for integers, which is associative. So, for all a, b, c in $2\mathbb{Z}$, the equation $(a * b) * c = a * (b * c)$ holds true.

2. **Identity ($\mathcal{G}2$):** For the binary operation of addition, the identity element is 0. This is because for any integer a, we have $a + 0 = 0 + a = a$. Notably, 0 is also in the set $2\mathbb{Z}$ (since $2 \times 0 = 0$). Thus, the identity element exists in the set.

3. **Inverse ($\mathcal{G}3$):** For any element $a = 2m$ in $2\mathbb{Z}$, its additive inverse is $-a = -2m$, which is also in $2\mathbb{Z}$. Thus, for each element a in $2\mathbb{Z}$, there exists an inverse in $2\mathbb{Z}$ such that the combination of the element and its inverse results in the identity element, 0.

All three axioms $\mathcal{G}1, \mathcal{G}2$, and $\mathcal{G}3$ are satisfied for the set $2\mathbb{Z}$ with the given operation. Therefore, the set $2\mathbb{Z}$ equipped with the binary operation $*$ forms a group.

□

Exercise 5. 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 $\mathcal{G}1, \mathcal{G}2, \mathcal{G}3$ from Definition 4.1 that does not hold.

Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by letting $a * b = a/b$.

Proof. To determine whether the binary operation $*$ gives a group structure on the set $\mathbb{R}^*$, we need to examine each axiom in order:

Set: $\mathbb{R}^*$ (nonzero real numbers)

Operation: $a * b = a/b$

1. Associativity ($\mathcal{G}1$): For all a, b, c in $\mathbb{R}^*$, we need to check if

$$(a * b) * c = a * (b * c)$$

Expanding both sides:

$$\begin{gathered}(a/b) * c = a * (b/c) \\ (a/b)/c = a/(b/c) \\ (a/b) \cdot (1/c) = a \cdot (c/b) \\ a/cb \neq ac/b\end{gathered}$$

The equation does not hold for all a, b, c in $\mathbb{R}^*$. Therefore, associativity ($\mathcal{G}1$) is violated.

Since $\mathcal{G}1$ is not satisfied, we don't need to check $\mathcal{G}2$ and $\mathcal{G}3$. The operation $*$ does not give a group structure on $\mathbb{R}^*$, and the first axiom that does not hold is $\mathcal{G}1$. □

Exercise 10b. Let n be a positive integer and let $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$.

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

Proof. To demonstrate that the groups $\langle n\mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ are isomorphic, we need to find an isomorphism between them, i.e., a bijective function $f : n\mathbb{Z} \to \mathbb{Z}$ that preserves the group operation.

Consider the function:

$$f : n\mathbb{Z} \to \mathbb{Z}$$

defined by:

$$f(nm) = m$$

where $nm \in n\mathbb{Z}$ and $m \in \mathbb{Z}$.

Now, let's verify the properties required for an isomorphism:

1. **Well-defined:** The function f is well-defined as for each element in $n\mathbb{Z}$, it maps to a unique element in $\mathbb{Z}$.

2. **Preserves operation:** For any $nm_1, nm_2 \in n\mathbb{Z}$, where $m_1, m_2 \in \mathbb{Z}$:

$$f(nm_1 + nm_2) = f(n(m_1 + m_2)) = m_1 + m_2 = f(nm_1) + f(nm_2)$$

So, the function f preserves the group operation.

3. **Bijective:**

- **Injective (One-to-one):** Suppose $f(nm_1) = f(nm_2)$, then $m_1 = m_2$. Hence, f is injective.

- **Surjective (Onto):** For every integer m, there's an element nm in $n\mathbb{Z}$ such that $f(nm) = m$. So, f is surjective.

Since f is well-defined, preserves the operation, and is bijective, it is an isomorphism between $\langle n\mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$. Thus, $\langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$. □

Exercise 17. 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 $\det(A) \neq 0$.

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

Proof. To determine if the set of all $n \times n$ upper-triangular matrices with determinant 1 under matrix multiplication forms a group, we'll check the group axioms:

Set: U (set of all $n \times n$ upper-triangular matrices with determinant 1) **Operation:** Matrix multiplication

1. **Closure:** If A, B are two upper-triangular matrices in U, then their product AB is also an upper-triangular matrix. Moreover, using the property of determinants, $\det(AB) = \det(A)\det(B) = 1 \times 1 = 1$, so AB is also in U. Therefore, the set is closed under matrix multiplication.

2. **Associativity:** Matrix multiplication is associative for all matrices, i.e., for all matrices A, B, and C in U, we have:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

3. **Identity element:** The $n \times n$ identity matrix I_n is upper-triangular, and $\det(I_n) = 1$. For any matrix A in U, $A \cdot I_n = I_n \cdot A = A$. Therefore, I_n serves as the identity element in U.

4. **Inverse:** Let A be an upper-triangular matrix in U with determinant 1. Since $\det(A) = 1$ and A is invertible if and only if its determinant is not zero, there exists an inverse matrix A^{-1}. The challenge is showing that A^{-1} is also upper-triangular with determinant 1. Let's demonstrate this:

- We know that $\det(A^{-1}) = 1/\det(A) = 1$.

- Given that A is upper-triangular, its inverse will also be upper-triangular. (This can be shown using the formula for the inverse of a matrix in terms of its adjugate and determinant, or by directly computing the inverse for a generic upper-triangular matrix.)

Therefore, every matrix in U has an inverse in U.

Based on these properties, the set of all $n \times n$ upper-triangular matrices with determinant 1 under matrix multiplication forms a group. □

Exercise 25. Mark each of the following true or false.

(a.) A group may have more than one identity element.

(b.) Any two groups of three elements are isomorphic.

(c.) In a group, each linear equation has a solution.

(d.) The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.

(e.) Any definition a person gives for a group is correct provided that everything that is a group by that person's definition is also a group by the definition in the text.

(f.) Any definition a person gives for a group is correct provided he or she can show that everything that satisfies the definition satisfies the one in the text and conversely.

(g.) Every finite group of at most three elements is abelian.

(h.) An equation of the form $a * x * b = c$ always has a unique solution in a group.

(i.) The empty set can be considered a group.

(j.) Every group is a binary algebraic structure.

Proof. Let's address each of the statements in the given exercise:

(a) **A group may have more than one identity element.**

False. By definition, a group has exactly one identity element. If e_1 and e_2 are both identity elements for a group G, then $e_1 = e_1 \cdot e_2 = e_2$.

(b) **Any two groups of three elements are isomorphic.**

True. If you have two groups of three elements, they both have the structure $\{e, a, a^{-1}\}$ where e is the identity element. The group operations are determined by the properties of the identity and inverses, so these groups are necessarily isomorphic.

(c) **In a group, each linear equation has a solution.**

True. Given an equation $a \cdot x = b$, since a group has inverses for every element, $x = a^{-1} \cdot b$ is a solution.

(d) **The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.**

False. While memorization can be useful, true understanding comes from grasping the underlying concepts and being able to apply, explain, and extrapolate from the definition, not just recite it.

(e) **Any definition a person gives for a group is correct provided that everything that is a group by that person's definition is also a group by the definition in the text.**

False. While this condition ensures that no non-groups are incorrectly identified as groups, it doesn't guarantee that all groups are identified.

(f) **Any definition a person gives for a group is correct provided he or she can show that everything that satisfies the definition satisfies the one in the text and conversely.**

True. If a definition is equivalent in both its inclusion and exclusion of groups as the definition in the text, then it can be considered correct.

(g) **Every finite group of at most three elements is abelian.**

True. There are only two group structures with three elements: the cyclic group of order 3 and the trivial group (with one element). Both are abelian.

(h) **An equation of the form $a \cdot x \cdot b = c$ always has a unique solution in a group.**

True. By multiplying both sides by a^{-1} on the left and b^{-1} on the right, we get $x = a^{-1} \cdot c \cdot b^{-1}$ as a unique solution.

(i) **The empty set can be considered a group.**

False. By definition, a group must contain at least one element (the identity element).

(j) **Every group is a binary algebraic structure.**

True. A group is defined on a set with a binary operation that combines two elements to produce another element. □

Exercise 31. If $*$ is a binary operation on a set S, an element x of S is an idempotent for $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

Proof. Given that a group G under the operation $*$ has the properties:

(1) An identity element e such that for every $a \in G$, $e * a = a * e = a$.

(2) Every element has an inverse. That is, for every $a \in G$, there exists a^{-1} such that $a * a^{-1} = a^{-1} * a = e$.

Let's prove that a group has exactly one idempotent element:

Let x be an idempotent element of G. That is, $x * x = x$.

To show that x must be the identity element e:

Starting with the idempotent property $x * x = x$:

Multiply both sides by the inverse of x, denoted x^{-1}: $x^{-1} * (x * x) = x^{-1} * x$

Using associativity, we can rearrange the parentheses: $(x^{-1} * x) * x = x^{-1} * x$

Now, $x^{-1} * x$ is the identity e, so: $e * x = e$

This implies that $x = e$ since the identity e is the only element in the group that satisfies this property.

Thus, x, the idempotent element, must be the identity element e.

Now, let's prove that no other element in G can be idempotent:

Suppose, for contradiction, that there exists some element $y \neq e$ in G such that $y*y = y$. Then: $y^{-1} * (y * y) = y^{-1} * y$

Using associativity: $(y^{-1} * y) * y = y^{-1} * y$

Which gives: $e * y = e$

This is a contradiction because we assumed y is not the identity. Thus, our assumption is false, and no other element apart from e can be idempotent.

In conclusion, a group G has exactly one idempotent element, which is its identity element e. □

Exercise 33. Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

Proof. **Base Step:** For $n = 1$:

$(a * b)^1 = a * b$ and $a^1 * b^1 = a * b$. Clearly, $(a * b)^1 = a^1 * b^1$.

Inductive Step: Assume the property holds for some arbitrary positive integer k, i.e.,

$$(a * b)^k = a^k * b^k \qquad \text{(Inductive Hypothesis)}$$

We want to prove that the property also holds for $k + 1$, i.e.,

$$(a * b)^{k+1} = a^{k+1} * b^{k+1}$$

Starting with the left-hand side:

$$(a * b)^{k+1} = (a * b)^k * (a * b)$$

Using our Inductive Hypothesis:

$$= a^k * b^k * a * b$$

Since G is an abelian group, the operation (in this case, $*$) is commutative. Using this property:

$$= a^k * a * b^k * b$$
$$= a^{k+1} * b^{k+1}$$

Which is our desired right-hand side.

Thus, by the principle of mathematical induction, the property $(a * b)^n = a^n * b^n$ holds for all $n \in \mathbb{Z}^+$ and for all $a, b \in G$.

Proof. Let G be an abelian group. To prove $(a * b)^n = a^n * b^n$ for all $a, b \in G$ and $n \in \mathbb{Z}^+$, we use mathematical induction on n.

For the base case, when $n = 1$, we have:

$$(a * b)^1 = a * b$$

and

$$a^1 * b^1 = a * b$$

So, $(a * b)^1 = a^1 * b^1$.

Assume the statement holds for some positive integer k, that is,

$$(a * b)^k = a^k * b^k$$

Now, for $n = k + 1$:

$$(a * b)^{k+1} = (a * b)^k * (a * b)$$

Using the inductive hypothesis, this becomes:

$$= a^k * b^k * a * b$$

Using the commutative property of the operation in G, we get:

$$= a^k * a * b^k * b$$

$$= a^{k+1} * b^{k+1}$$

Thus, by induction, $(a * b)^n = a^n * b^n$ holds for all $n \in \mathbb{Z}^+$ and for all $a, b \in G$. □

□

Chapter I.5

Exercise 5. 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.

The set $\pi\mathbb{Q}$ of rational multiples of π.

Proof. To verify if $\pi\mathbb{Q}$ is a subgroup of $\mathbb{C}$ under addition, we'll check:

(1) **Closure:** For any $a, b \in \pi\mathbb{Q}$, their sum $a + b$ remains in $\pi\mathbb{Q}$.

(2) **Identity:** 0 is in $\pi\mathbb{Q}$.

(3) **Inverse:** For each $a \in \pi\mathbb{Q}$, its inverse $-a$ is in $\pi\mathbb{Q}$.

Proof:

(1) Let $a = p\pi$ and $b = q\pi$ with p, q rational. Their sum $a + b = (p + q)\pi$ is still in $\pi\mathbb{Q}$.

(2) $0 = 0\pi$ is a member of $\pi\mathbb{Q}$.

(3) The additive inverse of $a = p\pi$ is $-a = -p\pi$, which belongs to $\pi\mathbb{Q}$.

Thus, $\pi\mathbb{Q}$ is a subgroup of $\mathbb{C}$ under addition. □

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

The $n \times n$ with determinant 2

Proof. To determine whether a set of matrices forms a subgroup of $GL(n, \mathbb{R})$, we must verify:

(1) **Closure:** If A, B are both in the set, then their product AB must also be in the set.

(2) **Identity:** The identity matrix I_n must be in the set.

(3) **Inverses:** For each matrix A in the set, its inverse A^{-1} must also be in the set.

Given set: The $n \times n$ matrices with determinant 2.

Proof:

(1) Closure: If A, B are both matrices in our set, then $\det(A) = 2$ and $\det(B) = 2$. Using the property of determinants, $\det(AB) = \det(A)\det(B) = 2 \times 2 = 4$. Hence, the product AB does not have a determinant of 2, and our set is not closed under matrix multiplication.

Given that closure fails, there's no need to verify the other conditions. The set of $n \times n$ matrices with determinant 2 is not a subgroup of $GL(n, \mathbb{R})$. □

Exercise 11. In Exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

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

Proof. To determine whether a set of matrices forms a subgroup of $GL(n, \mathbb{R})$, we must verify:

(1) **Closure:** If A, B are both in the set, then their product AB must also be in the set.

(2) **Identity:** The identity matrix I_n must be in the set.

(3) **Inverses:** For each matrix A in the set, its inverse A^{-1} must also be in the set.

Given set: The $n \times n$ matrices with determinant -1.

Proof:

(1) **Closure:** If A, B are matrices in our set, then $\det(A) = -1$ and $\det(B) = -1$. Using the property of determinants, $\det(AB) = \det(A)\det(B) = (-1) \times (-1) = 1$. Hence, the product AB does not have a determinant of -1, and our set is not closed under matrix multiplication.

Given that closure fails, there's no need to verify the other conditions. The set of $n \times n$ matrices with determinant -1 is not a subgroup of $GL(n, \mathbb{R})$. □

Exercise 17. 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.

The subset of all $f \in \tilde{F}$ such that $f(0) = 1$ To determine if the subset is a subgroup, we must verify a few properties. Let's denote this subset as S.

For the set S to be a subgroup under the given operations, the following must hold:

(1) **Identity:** The identity element of the group must be in the subset S.

(2) **Closure:** For all elements in the subset S, the result of the operation must also be in the subset S.

(3) **Inverses:** For each element in the subset S, its inverse must also be in S.

Let's evaluate:

Part (a). a subgroup of the group F under addition:

(1) **Identity:** The identity for addition in the group F is the zero function $f(x) = 0$. However, this function doesn't satisfy $f(0) = 1$, so the identity is not in S. Hence, S is **not** a subgroup of F under addition.

Part (b). a subgroup of the group $\tilde{F}$ under multiplication:

(1) **Identity:** The identity for multiplication in the group $\tilde{F}$ is the function $f(x) = 1$. This function satisfies $f(0) = 1$ and hence the identity is in S.

(2) **Closure:** Suppose f, g are in S. Then, by definition, $f(0) = g(0) = 1$. So, for the function $f \cdot g$ (defined by pointwise multiplication), we have:

$$(f \cdot g)(0) = f(0) \cdot g(0) = 1 \cdot 1 = 1$$

This means $f \cdot g$ is also in S. Hence, S is closed under multiplication.

(3) **Inverses:** For any function f in S, the inverse function $1/f$ must also be in S. Since $f(0) = 1$, we have $(1/f)(0) = 1/f(0) = 1$. Also, because f is nonzero at all points, $1/f$ is defined at all points and is nonzero. Hence, $1/f$ is in S.

From the above, S is a subgroup of $\tilde{F}$ under multiplication.

Proof. For part (a), S is not a subgroup of F under addition as the identity element of F is not in S. For part (b), S is a subgroup of $\tilde{F}$ under multiplication because it contains the identity of $\tilde{F}$, is closed under multiplication, and has inverses for all its elements in $\tilde{F}$. □

Exercise 20(G_7). Give a complete list of all subgroup relations, of the form $G_i \leq G_j$, that exist between these given groups $G_1, G_2, \cdots, G_9$.

$$G_7 = 3\mathbb{Z} \text{ under addition}$$

Proof. Let's break down the relationships between each of the groups:

$G_1 = \mathbb{Z}$ (under addition): This is the set of all integers.

$G_2 = 12\mathbb{Z}$ (under addition): This is the set of all integer multiples of 12.

$G_3 = Q^+$ (under multiplication): This is the set of all positive rational numbers.

$G_4 = \mathbb{R}$ (under addition): This is the set of all real numbers.

$G_5 = \mathbb{R}^+$ (under multiplication): This is the set of all positive real numbers.

$G_6 = \{\pi n | n \in \mathbb{Z}\}$ (under multiplication): This is the set of all integer multiples of π.

$G_7 = 3\mathbb{Z}$ (under addition): This is the set of all integer multiples of 3.

G_8: This is the set of all integer multiples of 6 (i.e., $6\mathbb{Z}$) under addition.

$G_9 = \{6n | n \in \mathbb{Z}\}$ (under multiplication): This is the same as G_8, but under multiplication.

From the above:

1. $G_2 \leq G_1$: Every multiple of 12 is an integer.
2. $G_7 \leq G_1$: Every multiple of 3 is an integer.
3. $G_8 \leq G_1$: Every multiple of 6 is an integer.
4. $G_2 \leq G_7$: Every multiple of 12 is also a multiple of 3.
5. $G_8 \leq G_7$: Every multiple of 6 is also a multiple of 3.
6. $G_1 \leq G_4$: Every integer is a real number.
7. $G_2 \leq G_4$: Every multiple of 12 is a real number.
8. $G_7 \leq G_4$: Every multiple of 3 is a real number.
9. $G_8 \leq G_4$: Every multiple of 6 is a real number.
10. $G_3 \leq G_5$: Every positive rational number is a positive real number.

The groups G_6 and G_9 don't seem to be subgroups of the others due to their specific definitions related to π and 6, respectively, under multiplication.

Therefore, the subgroup relations are: $G_2 \leq G_1$, $G_7 \leq G_1$, $G_8 \leq G_1$, $G_2 \leq G_7$, $G_8 \leq G_7$, $G_1 \leq G_4$, $G_2 \leq G_4$, $G_7 \leq G_4$, $G_8 \leq G_4$, and $G_3 \leq G_5$. □

Exercise 29. In Exercises 27 through 35, find the order of the cyclic subgroup of the given group generated by the indicated element.

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

Proof. Consider the element $z = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ in the group U_6.

To find the order of the cyclic subgroup generated by z, we need to find the smallest positive integer n such that $z^n = 1$.

Computing the powers of z: $z^1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ $z^2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$ $z^3 = \cos 2\pi + i\sin 2\pi = 1$

Therefore, the order of the cyclic subgroup generated by z is 3. □

Exercise 34. In Exercises 27 through 35, find the order of the cyclic subgroup of the given group generated by the indicated element.

The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Proof. To determine the order of the cyclic subgroup generated by M, we need to find the smallest positive integer n such that M^n is the identity matrix.

$$M = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

First, let's compute M^2:

$$M^2 = M \times M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Computing M^3:

$$M^3 = M^2 \times M = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Finally, computing M^4:

$$M^4 = M^3 \times M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Which is the identity matrix for 4×4 matrices.

Therefore, the smallest positive integer n for which M^n is the identity matrix is $n = 4$.

Proof. Consider the matrix M in the group of invertible 4×4 matrices. To determine the order of the cyclic subgroup generated by M, we computed the powers of M and found that M^4 is the identity matrix. Therefore, the order of the cyclic subgroup generated by M is 4. □

□

Exercise 47. Prove that if G is an abelian group, written multiplicatively, with identity element e, then all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G. To show that the set H of all elements x of G satisfying the equation $x^2 = e$ is a subgroup of G, we must verify the subgroup criteria:

(1) **Identity:** The identity element e of G is in H since $e^2 = e$.

(2) **Closure:** For any two elements a, b in H, their product ab must also be in H.

(3) **Inverses:** For every element a in H, its inverse a^{-1} should also be in H.

Proof.

(1) We have already seen that e is in H.

(2) Let a, b be any two elements in H. Thus, we have:

$$a^2 = e$$

$$b^2 = e$$

Now, considering the element ab in G (because G is a group and is closed under multiplication):

$$(ab)^2 = a^2 \cdot b^2 = e \cdot e = e$$

Since G is abelian, $ab = ba$. Thus, the square of ab is e. This implies that ab is also in H, establishing the closure of H under the group operation.

(3) Let a be any element in H. By definition of H, we have:

$$a^2 = e$$

Taking the inverse of both sides, we get:

$$(a^2)^{-1} = e^{-1}$$

Given that the inverse of the identity is the identity itself, and using properties of inverses, we get:

$$a^{-2} = e$$

Since G is abelian, the inverse of a is also its reciprocal, so $(a^{-1})^2 = e$, implying that a^{-1} is in H.

Hence, all the criteria for H to be a subgroup of G are satisfied. Therefore, H is a subgroup of G. □

Exercise 57. Show that a group with no proper nontrivial subgroups is cyclic.

Let G be a group with no proper nontrivial subgroups. We wish to show that G is cyclic.

Case 1: If G has only the identity element e, then G is trivially cyclic as it can be generated by e.

Case 2: If G has more than one element, let a be any element in G such that $a \neq e$.

Consider the subgroup $\langle a \rangle$ generated by a. This subgroup contains all powers of a: $a, a^2, a^3, \ldots$ as well as $a^{-1}, a^{-2}, \ldots$.

(1) We claim that $\langle a \rangle$ cannot be a proper nontrivial subgroup of G. This is because by our hypothesis, G has no proper nontrivial subgroups other than $\{e\}$. So, if $\langle a \rangle$ were proper and nontrivial, it would contradict our assumption.

(2) Since $\langle a \rangle$ is not a proper subgroup of G and a is in G, we must have $\langle a \rangle = G$.

Thus, every element in G can be expressed as a power of a, which implies that G is cyclic and generated by a.

Proof. Given a group G with no proper nontrivial subgroups, either G is trivial (consists of only the identity), or there exists some $a \in G$ such that $a \neq e$.

For the trivial case, G is cyclic.

For the non-trivial case, considering the subgroup generated by a, $\langle a \rangle$, we note that it cannot be proper and nontrivial as per the given conditions. Therefore, $\langle a \rangle$ must equal G, and all elements of G can be expressed as powers of a. This makes G a cyclic group generated by a. □

Chapter I.6

Exercise 17. In exercises 17 through 21, find the number of elements in the indicted cyclic group.

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

Proof. To find the number of elements in the cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25, we are essentially trying to find the order of the element 25 in $\mathbb{Z}_{30}$. This order is the smallest positive integer n such that $25n \equiv 0 \mod 30$.

In the group $\mathbb{Z}_{30}$, addition is performed modulo 30. To find the order of 25, we start by repeatedly adding 25 to itself until we obtain a result that's congruent to 0 modulo 30.

$$
\begin{aligned}
&1 \times 25 \equiv 25 \mod 30 \\
&2 \times 25 \equiv 50 \mod 30 \equiv 20 \mod 30 \\
&3 \times 25 \equiv 75 \mod 30 \equiv 15 \mod 30 \\
&4 \times 25 \equiv 100 \mod 30 \equiv 10 \mod 30 \\
&5 \times 25 \equiv 125 \mod 30 \equiv 5 \mod 30 \\
&6 \times 25 \equiv 150 \mod 30 \equiv 0 \mod 30
\end{aligned}
$$

From the calculations above, we see that $25 \times 6 \equiv 0 \mod 30$. Therefore, the order of 25 in $\mathbb{Z}_{30}$ is 6.

Thus, the cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25 has 6 elements. □

Exercise 20. In exercises 17 through 21, find the number of elements in the indicted cyclic group.

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

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

Proof. We start by repeatedly multiplying $(\frac{(1+i)}{\sqrt{2}})$ by itself:

(1) $(\frac{(1+i)}{\sqrt{2}})^1 = \frac{(1+i)}{\sqrt{2}}$

(2) $(\frac{(1+i)}{\sqrt{2}})^2 = (1+i)\frac{(1+i)}{\sqrt{2}} = \frac{(1+2i+i^2)}{2} = 1+i-1 = i$

(3) $(\frac{(1+i)}{\sqrt{2}})^3 = i(\frac{(1+i)}{\sqrt{2}}) = \frac{-1+i}{\sqrt{2}}$

(4) $(\frac{(1+i)}{\sqrt{2}})^4 = (-1+i)\frac{(1+i)}{\sqrt{2}} = -1$

(5) $(\frac{(1+i)}{\sqrt{2}})^5 = -1 * (\frac{(1+i)}{\sqrt{2}}) = -\frac{(1+i)}{\sqrt{2}}$

(6) $(\frac{(1+i)}{\sqrt{2}})^6 = (\frac{(1+i)}{\sqrt{2}})^2(\frac{(1+i)}{\sqrt{2}})^2(\frac{(1+i)}{\sqrt{2}})^2 = i^3 = -i$

(7) $(\frac{(1+i)}{\sqrt{2}})^7 = (\frac{(1+i)}{\sqrt{2}})^6(\frac{(1+i)}{\sqrt{2}}) = -i(\frac{(1+i)}{\sqrt{2}}) = \frac{(1-i)}{\sqrt{2}}$

(8) $(\frac{(1+i)}{\sqrt{2}})^8 = (\frac{(1+i)}{\sqrt{2}})^4(\frac{(1+i)}{\sqrt{2}})^4 = (-1)^2 = 1$

In this case, $(\frac{(1+i)}{\sqrt{2}})$ represents a $45°$ or $\pi/4$ radian rotation, and to complete a full rotation and return to 1, the identity element, it must be raised to the power of 8. That is:

$(\frac{(1+i)}{\sqrt{2}})^8 = 1$

Thus, the order of $|\langle\frac{(1+i)}{\sqrt{2}}\rangle|$ in $\mathbb{C}^*$ is 8, and the cyclic subgroup generated by $(\frac{(1+i)}{\sqrt{2}})$ has 8 elements. □

Exercise 27. In Exercises 25 through 29, find all orders of subgroups of the given group.

Given: $\mathbb{Z}_{12}$

Proof. To find the orders of subgroups of $\mathbb{Z}_{12}$, we first recognize that the order of a subgroup must divide the order of the group. In the case of $\mathbb{Z}_{12}$, the group order is 12. The divisors of 12 are 1, 2, 3, 4, 6, and 12.

The possible orders of subgroups of $\mathbb{Z}_{12}$ are these divisors, and for each possible order, there exists a subgroup:

(1) Order 1: The trivial subgroup 0.

(2) Order 2: The subgroup generated by 6, $0, 6$.

(3) Order 3: The subgroup generated by 4, $0, 4, 8$.

(4) Order 4: The subgroup generated by 3, $0, 3, 6, 9$.

(5) Order 6: The subgroup generated by 2, $0, 2, 4, 6, 8, 10$.

(6) Order 12: The entire group $\mathbb{Z}_{12}$.

Thus, the possible orders of subgroups of $\mathbb{Z}_{12}$ are 1, 2, 3, 4, 6, and 12. □

Exercise 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 the group G, then $H \cap K$ is a group.

(j.) Every cyclic group of order > 2 has at least two distinct generators.

Proof. □

Exercise 39.

(a.) Every cyclic group is abelian.

True. By definition, a cyclic group is generated by a single element. Therefore, for any two elements a and b in the group, they can be expressed as $a = g^m$ and $b = g^n$ for some integers m and n. Their product is $g^m \cdot g^n = g^{m+n}$, which is commutative.

(b.) Every abelian group is cyclic.

False. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein 4-group) which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. It's abelian, but not cyclic since no single element can generate the entire group.

(c.) $\mathbb{Q}$ under addition is a cyclic group.

False. There's no single rational number that can generate all rational numbers through repeated addition.

(d.) Every element of every cyclic group generates the group.

False. Consider the group $\mathbb{Z}_{10}$. The element 2 generates $\{0, 2, 4, 6, 8\}$, not the entire group.

(e.) There is at least one abelian group of every finite order > 0.

True. For every positive integer n, the group $\mathbb{Z}_n$ is an abelian group of order n.

(f.) Every group of order ≤ 4 is cyclic.

False. The Klein 4-group, as mentioned in part (b.) is a non-cyclic group of order 4.

(g.) All generators of $\mathbb{Z}_{20}$ are prime numbers.

False. 3 is a generator, but so is 7, and 7 is not prime in $\mathbb{Z}_{20}$ (since $7 \times 3 = 21 \equiv 1 \mod 20$).

(h.) If G and G' are groups, then $G \cap G'$ is a group.

False. $G \cap G'$ is not necessarily a group unless both G and G' are subgroups of some bigger group and their intersection is non-empty.

(i.) If H and K are subgroups of the group G, then $H \cap K$ is a group.

True. The intersection of two subgroups is always a subgroup.

(j.) Every cyclic group of order > 2 has at least two distinct generators.

True. If a cyclic group is generated by a, then it's also generated by a^{-1} (the inverse of a), and these are distinct unless the group is of order 2.

Proof. □

Exercise 52. Let p be a prime number. Find the number of generators of the cyclic group $\mathbb{Z}_{p^r}$, where r is an integer ≥ 1.

Proof. In a cyclic group, an element a is a generator if and only if the order of a is p^r.

Recall that the order of an element a in $\mathbb{Z}_{p^r}$ is the smallest positive integer k such that $a^k \equiv 1 \mod p^r$. From the theory of cyclic groups, a will be a generator if and only if a is relatively prime to p^r.

The number of elements that are relatively prime to p^r is given by Euler's totient function, $\phi(p^r)$.

For p a prime number, the function $\phi(p^r)$ is calculated as:

$$\phi(p^r) = p^r - p^{r-1}$$

This is because there are p^r total numbers from 0 to $p^r - 1$, and p^{r-1} of them are multiples of p and thus are not relatively prime to p^r.

The number of generators of the cyclic group $\mathbb{Z}_{p^r}$ is given by Euler's totient function $\phi(p^r)$. Using the formula for $\phi(p^r)$ when p is prime, we find:

$$\phi(p^r) = p^r - p^{r-1}$$

Thus, the cyclic group $\mathbb{Z}_{p^r}$ has $p^r - p^{r-1}$ generators. □

Exercise 55. Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if p is a prime number.

Proof. Let H be a nontrivial subgroup of $\mathbb{Z}_p$ and let a be a non-zero element of H. Given that p is prime, every integer from 1 to $p-1$ is relatively prime to p. Thus, for our chosen a, the $\gcd(a, p) = 1$.

By Bezout's identity, since a and p are relatively prime, there exist integers x and y such that $ax + py = 1$. In the context of our group, this means $ax \equiv 1 \pmod{p}$. As a result, a has an inverse in $\mathbb{Z}_p$, which means a can generate all the elements in $\mathbb{Z}_p$.

This implies that H contains all elements of $\mathbb{Z}_p$, making H equivalent to $\mathbb{Z}_p$. Thus, $\mathbb{Z}_p$ has no proper nontrivial subgroups. $\square$