# Self Study
# Group Theory

Alex Thies

# Contents

Frequently Used Notation iv

Preface v

Chapter 1. Groups 1
1. Introduction to Groups 1
2. Basic Algebra in Groups 2
3. Subgroups 6
4. Homomorphisms 9
5. Groups of Units 12
6. Cyclic Groups 13
7. Permutation Groups 15
8. *Dihedral Groups 17
9. *Symmetric Groups 17
10. *Matrix Groups 17
11. *The Quaternion Group 17

Chapter 2. Quotient Groups 19

Chapter 3. *Group Actions 21

Appendix A. Figures 23

## Frequently Used Notation

| | |
|---|---|
| $f^{-1}(a)$ | the inverse image or preimage of $A$ under $f$. |
| $a\|b$ | $a$ divides $b$. |
| $(a, b)$ | the greatest common divisor of $a, b$. |
| $[a, b]$ | the least common multiple of $a, b$. |
| $\|A\|$ | the number of elements in the set $A$, or the cardinality of $A$. |
| $\mathbb{Z}, \mathbb{Z}^+$ | the integers, the positive integers. |
| $\mathbb{Q}, \mathbb{Q}^+$ | the rational numbers, the positive rational numbers. |
| $\mathbb{R}, \mathbb{R}^+$ | the real numbers, the positive real numbers. |
| $\mathbb{C}, \mathbb{C}^\times$ | the complex numbers, the nonzero complex numbers. |
| $\mathbb{Z}_n$ | the integers modulo $n$. |
| $A \times B$ | the cartesian product of $A$ and $B$. |
| $D_{2n}$ | the dihedral group of order $2n$. |
| $S_n, S_\Omega$ | the symmetric group on $n$ letters, and on the set $\Omega$. |
| $Q_8$ | the quaternion group of order 8. |
| $\mathbb{F}_N$ | the finite field of $N$ elements. |
| $GL_n(F), GL(V)$ | the general linear groups. |
| $SL_n(F)$ | the special linear group. |
| $M_n(F)$ | the set of all $n \times n$ matrices whose entries are elements of the set $F$. |
| $A \cong B$ | $A$ is isomorphic to $B$. |
| $\ker(f)$ | the kernel of the homomorphism $f$. |
| $\mathrm{ord}(a)$ | the order of $a$. |
| $f(A)$ | the image of the homomorphism $f$ over the group $A$. |
| $H \triangleleft G$ | $H$ is a normal subgroup of $G$. |
| $aH, Ha$ | the left coset, and right coset of $H$ with coset representative $a$. |

Matrices will be capital bold letters, e.g., $\mathbf{X}, \mathbf{Y} \in GL(V)$, vectors will be lowercase bold letters, e.g., $\mathbf{u}, \mathbf{v} \in V$.

# Preface

Having utilized Chapters 4-7 from *Essentials of Modern Algebra*, First Edition, by Cheryl Chute Miller in a course on Ring Theory (Math 391), I would like to gain an understanding of the Group Theory covered by Chapters 1-3. Additionally, I have decided to include some Group Theory material from *Abstract Algebra*, Third Edition, by David Dummitt & Richard Foote – the textbook used in Math 444. Sections including material from the Math 444 textbook are preceded by a $\star$.

CHAPTER 1

# Groups

## 1. Introduction to Groups

**Problem 1.17.** Write out the Cayley table for the group $(\mathbb{Z}_6, +_6)$ and identify the inverse of each element.

SOLUTION. Figure 1 is the Cayley table, observe that for $a \in \mathbb{Z}_6$ the inverse under addition modulo 6 is $a^{-1} = 6 - a$. □

**Problem 1.18.** Find the 10 elements of the group $\mathbb{Z}_5 \times \mathbb{Z}_2$, and write out the Cayley table. Recall that its operation uses $+_5$ in the first coordinate and $+_2$ in the second. Identify the inverse of each element.

SOLUTION. Figure 2 is the Cayley table, observe that $\mathbb{Z}_5 \times \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (0,1), (1,1), (2,1), (3,1), (4,1)\}$. The identities are colored in red, thus for $(m,n) \in \mathbb{Z}_5 \times \mathbb{Z}_2$ the inverses are $\big\{(m,n)^{-1} = \big(m^{-1}, n^{-1}\big) : m^{-1} = 5 - m$ and $n^{-1} = 2 - n\big\}$. □

**Problem 1.19.** What does Theorem 1.14 tell us about the entries in the Cayley table of a group?

SOLUTION. Theorem 1.14 states that: Suppose $G$ is a group under the operation $*$.

(i) There is exactly one element in $G$ that has the property of an identity.
(ii) For each element $a \in G$ there is exactly one element of $G$ that satisfies the property of the inverse of $a$.

My guess is that the identity elements $e_G$ are unique in their respective rows and columns of the table, like Sudoku. □

**Problem 1.20.** Prove that a set with exactly one element, $A = \{a\}$, will always form a group since there is only one way to define an operation on the set. Be sure to show that the properties of a group all hold.

PROOF. Let $A$ be as above. Since the operation $*$ must be closed over $A$ the only operation that works is the identity, i.e., the only operation that holds over $A$ is $* : A \to A$ defined by $a \mapsto a$. We must show that $(A, *)$ is a group, i.e., we will show that $*$ is associative, that there exists a unique identity element $e_G \in A$, and that there exists a unique inverse element $a^{-1} \in A$ for each $a \in A$.

Notice that $(a * a) * a = a * a = a$, and that $a * (a * a) = a * a = a$, thus by transitvity we have that $*$ is associative. Additionally, note tha $a \in A$ satisfies the necessary and sufficient properties of both the identity $e_G$, and the inverse (of itself) $a^{-1} = a$. Finally, notice that $*$ is obviously commutative, therefore the group formed from a set containing only one element is always an abelian group. □

**Problem 1.21.** We can even create groups with games! Consider four cups placed in a square pattern on a table. If we have a penny in one of the cups there are four ways we can move it to another cup: Horizontally, Vertically, Diagonally, or Stay where it is. We will label them $H, V, D, S$. To define an operation, consider two movements in a row, i.e., $x * y$ means we first move the penny as $x$ tells us to, then after that move the penny as $y$ instructs. For example, $H * V = D$ since if we first move it horizontally and then vertically altogether we have moved it diagonally. Create the Cayley table for this group, identify the identity, and the inverse of each element.

SOLUTION. Call this group $(G, *)$. Figure 3 is the Cayley table, note that $S$ is the identity and that for each $a \in G$, we have the inverse $a^{-1} = a$. Notice that groups with this property (that each element is its own inverse) have symmetric Cayley tables. □

**Problem 1.22.** Prove that the set $A = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a group under matrix multiplication. Is it abelian?

PROOF. Recall that matrix multiplication is always associative, it remains to find identities and inverses. Figure 4 is the Cayley table, note that the two-by-two identity matrix contained in $A$ is the identity of $(A, \times)$, i.e., $e_G = \mathbf{I}_2$ and that each element of $A$ is its own inverse under matrix multiplication. Finally, notice that Figure 4 is symmetric, therefore $(A, \times)$ is an abelian group. □

**Problem 1.23.** Verify that $\mathcal{F}(\mathbb{R})$ is a group using the addition of functions as defined in Example 1.13.

SOLUTION. We will show that $(\mathcal{F}(\mathbb{R}), +)$ is a group under normal function addition. We will do this by showing that $+$ is associative, and that an identity and inverses exist under $+$.

Let $f, g, h \in \mathcal{F}(\mathbb{R})$ and compute that $f + (g + h) = f(x) + (g + h)(x) = f(x) + g(x) + h(x) = (f + g)(x) + h(x) = (f + g) + h$, thus $+$ is associative over $\mathcal{F}(\mathbb{R})$. Notice that $0(x) \in \mathcal{F}(\mathbb{R})$ is the identity, thus for each $f \in \mathcal{F}(\mathbb{R})$, we have $-f \in \mathcal{F}(\mathbb{R})$ as an inverse. Hence, $(\mathcal{F}(\mathbb{R}), +)$ is a group. □

## 2. Basic Algebra in Groups

**Problem 1.24.** Prove the Cancellation Law (Theorem 1.20). Do not use any theorems that occur after it in the text.

*Theorem.* (Cancellation Law) Suppose $G$ is a group and $a, b, c \in G$.

(i) If $ab = ac$ then $b = c$.
(ii) If $ba = ca$ then $b = c$.

PROOF. Let $G, a, b, c$ be as above. Recall that since $G$ is a group, there exists a unique inverse $a^{-1} \in G$ such that $aa^{-1} = e_G = a^{-1}a$. Suppose $ab = ac$, we

compute the following:

$$\begin{aligned} ab &= ac, \\ a^{-1}ab &= a^{-1}ac, \\ e_G b &= e_G c, \\ b &= c. \end{aligned}$$

Thus $ab = ac$ implies that $b = c$ as desired. A similar argument shows the second part of the theorem.

$$\begin{aligned} ba &= ca, \\ baa^{-1} &= caa^{-1}, \\ be_G &= ce_G, \\ b &= c. \end{aligned}$$

Thus $ba = ca$ implies that $b = c$, and the theorem is proved. □

**Problem 1.25.** Assume $G$ is a group and $a \in G$. Consider a fixed integer $k$ and use PMI (Theorem 0.3) to prove that for all $n \in \mathbb{N}, a^n a^k = a^{n+k}$. You will need to consider cases here since $k$ can be positive, negative, or 0.

Proof. □

**Problem 1.26.** Prove Theorem 1.23 (ii) for the case of $n > 0$ and $m < 0$.

Proof. □

**Problem 1.27.** Assume $G$ is a group and $a \in G$. Prove by PMI (Theorem 0.3) that for $n \in \mathbb{N}, (a^n)^{-1} = a^{-n}$.

Proof. Let $a, G$ be as above. Notice that for $n = 1$ we have $(a^1)^{-1} = a^{-1}$. Assume that for some natural number $n$ we have $(a^n)^{-1} = a^{-n}$. We compute the following,

$$\begin{aligned} \left(a^{n+1}\right)^{-1} &= (a^n a)^{-1}, \\ &= (a^n)^{-1}a^{-1}, \\ &= a^{-n}a^{-1}, \\ &= a^{-n-1}, \\ &= a^{-(n+1)}. \end{aligned}$$

Thus, for the given proposition $P$ we have shown that $P(n) \Rightarrow P(n+1)$. □

**Problem 1.28.** Suppose $G$ is a group with $a, b \in G$. Prove: If $a^3 = b$, then $b = aba^{-1}$.

PROOF. Let $G, a, b$ be as above and suppose that $a^3 = b$, we compute the following,

$$\begin{aligned} a^3 &= b, \\ a(aaa)a^{-1} &= aba^{-1}, \\ (aaa)\left(aa^{-1}\right) &= aba^{-1}, \\ a^3 e_G &= aba^{-1}, \\ b &= aba^{-1}. \end{aligned}$$

□

**Problem 1.29.** Suppose $G$ is a group and $a, b \in G$. Prove by PMI for all $n \in \mathbb{N}, (aba^{-1})^n = ab^n a^{-1}$. Do not assume $G$ is abelian.

PROOF. Let $G, a, b, n$ be as above. We proceed by mathematical induction over the natural numbers $n \in \mathbb{N}$. Notice the base case $n = 1$ holds since

$$\left(aba^{-1}\right)^1 = ab^1 a^{-1}.$$

Thus, assume that for some $n \in \mathbb{N}$ the following is true

$$(aba^{-1})^n = ab^n a^{-1}.$$

We compute the following,

$$\begin{aligned} \left(aba^{-1}\right)^{n+1} &= \left(aba^{-1}\right)\left(aba^{-1}\right)^n = \left(aba^{-1}\right)^n \left(aba^{-1}\right), \\ &= \left(aba^{-1}\right) ab^n a^{-1} = ab^n a^{-1} \left(aba^{-1}\right), \\ &= ab\left(a^{-1}a\right) b^n a^{-1} = ab^n \left(a^{-1}a\right) ba^{-1}, \\ &= ab(e_G)b^n a^{-1} = ab(e_G)b^n a^{-1}, \\ &= abb^n a^{-1}, \\ &= ab^{n+1}a^{-1}. \end{aligned}$$

Hence, for the given proposition $P$, we have shown that $P(n) \Rightarrow P(n+1)$. □

**Problem 1.30.** Suppose $G$ is a group and $a, b \in G$. Prove: If $n \in \mathbb{N}$ and $\text{ord}(b) = n$, then $\text{ord}(aba^{-1}) = n$. Use the result of the previous exercise to help.

PROOF. Let $G, a, b$ be as above, suppose $n \in \mathbb{N}$ and $\text{ord}(a) = n$. Recall that for all $n \in \mathbb{N}$ we have $(aba^{-1})^n = ab^n a^{-1}$, we compute that

$$\begin{aligned} (aba^{-1})^n &= ab^n a^{-1}, \\ &= ae_G a^{-1}, \\ &= aa^{-1}, \\ &= e_G. \end{aligned}$$

Thus, $\text{ord}(b) = n$ implies that $\text{ord}(aba^{-1}) = n$. □

**Problem 1.31.** Find the order of each element in the group $(\mathbb{Z}_{12}, +_{12})$.

SOLUTION. We compute the following,

| $n$ | ord($n$) | $n$ | ord($n$) | $n$ | ord($n$) |
|---|---|---|---|---|---|
| 0 | 0 | 4 | 2 | 8 | 2 |
| 1 | 11 | 5 | 11 | 9 | 3 |
| 2 | 5 | 6 | 1 | 10 | 5 |
| 3 | 3 | 7 | 11 | 11 | 11 |

□

**Problem 1.32.** Find the order of each element in the group $(\mathbb{Z}_7 +_7)$.

SOLUTION. We compute that for each $a \in \mathbb{Z}_7 / \{0\}$ we have $\text{ord}(a) = 6$ and $\text{ord}(0) = 0$. □

**Problem 1.33.** Find the order of each element in the group $A = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ under matrix multiplication.

SOLUTION. Note that $e_A = \mathbf{I}_2$, we compute that $\text{ord}(e_A) = 0$, and that for each other $a \in A$ we have $\text{ord}(a) = 1$. □

**Problem 1.34.** Find the order of each element in the group $G = \{Horizontally, Vertically, Diagonally, Stay\}$ from exercise 21 above (use the operation defined in that exercise).

SOLUTION. Recall that $e_G = S$, we compute that $\text{ord}(e_A) = 0$, and that for each other $a \in A$ we have $\text{ord}(a) = 1$. □

**Problem 1.35.** Complete the proof of Theorem 1.26.

*Theorem.* Suppose $G$ is a group and $a \in G$ with $\text{ord}(a) = n$ for some $n \in \mathbb{N}$. For any $t \in \mathbb{Z}$, $a^t = e_G$ if and only if $n$ divides $t$, i.e., $t = nq$ for some unique integer $q$.

PROOF. $\Rightarrow$) was done in the book.
$\Leftarrow$) Let $G, a, n$ be as above. Let $t \in \mathbb{Z}$ such that $n|t$. We will show that $a^t = e_G$ for all $t$ such that $n|t$.

$$\begin{aligned} a^t &= a^{nq}, \\ &= (a^n)^q, \\ &= e_G^n, \\ &= e_G. \end{aligned}$$

□

**Problem 1.36.** Suppose $G$ is a group and $a \in G$. Prove: if $\text{ord}(a) = 6$ then $\text{ord}(a^5) = 6$. Do any other elements $a^2, a^3, a^4$ have have order 6? Explain.

PROOF. □

**Problem 1.37.** Suppose $G$ is a group and $a \in G$. Assume $a^{50} = e_G$ but $a^{75} \neq e_G$ and $a^{10} \neq e_G$. Find the order of $a$, and prove that your answer is correct.

SOLUTION. Let $G, a$ be as above. We claim that $\text{ord}(a) = 50$, but suppose that there exists a different $m \in \mathbb{Z}$ such that $m \leq 50$ and $a^m = e_G$. We will show that $m$ must be 50.

We know by a theorem that if there exist $t \in \mathbb{Z}$ such that $a^t = e_G$, and $\text{ord}(a) = n$, then $n|t$. Thus, since $a^{50} = e_G$ we know that $m|50$; therefore we can claim that $m \in \{1, 2, 5, 10, 25, 50\}$. We also know that $a^{75} \neq e_G$, thus the divisors of 75 cannot be candidates for $m$, thus we can narrow down the set of possible $m$ to $\{2, 10, 50\}$. Finally, we know that $a^{10} \neq e_G$, by the above argument we know that $m$ can neither be 2 nor 10, thus $m = 50$ and $\text{ord}(a) = 50$ as we aimed to show. □

**Problem 1.38.** Suppose $G$ is a group and $a \in G$ with $a \neq e_G$. **Prove**: If $a^p = e_G$ for some prime number $p$, then $\text{ord}(a) = p$.

PROOF. Let $G, a$ be as above. Suppose $a^p = e_G$ for some prime number $p$. Further, suppose that there exists $n \in \mathbb{Z}$, $n \leq p$ such that $a^n = e_G$; we will show that $n = p$.

Since $a^p = e_G$, $a^n = e_G$, and $n \leq p$ we know that $n|p$. But since $p$ is prime, that means that $n = 1$, or $n = p$.

**Case 1**: Let $n = p$, we're done.
**Case 2**: Let $n = 1$, so we have $a^1 = e_G$, but we assumed $a \neq a_G$, so this case fails.
Thus, $\text{ord}(a) = p$. □

**Problem 1.39.** Suppose $G$ is a group and $a \in G$. Prove: If $\text{ord}(a)$ is an even integer then for any odd $k \in \mathbb{Z}$, $a^k \neq e_G$. Would the statement still be true if the words even and odd changed places, i.e., if $\text{ord}(a)$ is odd then for any even $k \in \mathbb{Z}, a^k \neq e_G$? Give a brief justification of your answer.

PROOF. Let $a, G$ be as above. Suppose that $\text{ord}(a) = 2n$ for some $n \in \mathbb{Z}$, and $k \in \mathbb{Z}$ such that $k = 2m + 1$ for some $m \in \mathbb{Z}$. Then we can compute $a^{2n} = e_G \iff a^{2n+1} = a$. Thus if $a$ has even order, $a$ raised to an odd power can never equal the identity. A similar argument shows the same for $a$ with odd order and even powers. □

## 3. Subgroups

**Problem 1.40.** Prove or disprove that $H = \{0, 3, 6, 9\}$ is a subgroup of $(\mathbb{Z}_{12}, +_{12})$.

PROOF. Its obvious that $H$ is nonempty, observe Figure 5 to see that $H$ is closed under $+_{12}$, has an identity, and each element of $H$ has an inverse under $+_{12}$, thus $H$ is a subgroup of $(\mathbb{Z}_{12}, +_{12})$. □

**Problem 1.41.** Prove or disprove that $H = \{0, 3, 6, 9\}$ is a subgroup of $(\mathbb{Z}_{10}, +_{10})$.

PROOF. Notice that $3 +_{10} 9 = 2$ and $2 \notin H$ thus $H$ is not closed under $+_{10}$ and not a subgroup of $\mathbb{Z}_{10}$ □

**Problem 1.42.** Prove that $H = \{0, 2, 4, 8, 16\}$ is a subgroup of $(\mathbb{Z}_{18}, +_{18})$.

PROOF. Observe rows 3,4 and columns 3,4 from Figure 6 indicate that there does not exist $8^{-1} \in H$ under $+_{18}$, thus $H$ is not a subgroup of $\mathbb{Z}_{18}$. □

**Problem 1.43.** Prove or disprove that $H = \{(0,0),(0,2),(1,0),(1,2)\}$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4$ under the operation using $+_2$ in the first coordinate and $+_4$ in the second coordinate.

PROOF. As in Problem 1.40 it is obvious to see that $H$ is nonempty, observe Figure 7 to see that $H$ has all of the properties of a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_4$ under the operation using $+_2$ in the first coordinate and $+_4$ in the second coordinate. □

**Problem 1.44.** Prove or disprove that $H = \{0,2,4,6\}$ is a subgroup of $(\mathbb{Z}_7 +_7)$.

PROOF. Notice that $2 +_7 6 = 1$ and that $1 \notin H$, thus $H$ is not closed under $+_7$ and not a subgroup of $\mathbb{Z}_7$. □

**Problem 1.45.** Determine if the set $G = \{\frac{n}{3} : n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Q}, +)$. Either prove that it is or give a specific example of how it fails.

PROOF. It is obvious to see that $G$ is nonempty, it remains to show that $G$ is closed under addition, has an inverse, and that each element of $G$ has an inverse under addition.

Since integer addition is closed, we know that $G$ is closed under addition. As before, since integer addition has an identity and inverse, we know that $G$ has the same properties, thus $G$ satisfies all of the necessary and sufficient conditions required of a subgroup. □

**Problem 1.46.** Determine if the set $\left\{\frac{1}{n} : n \in \mathbb{Z}, n \neq 0\right\}$ is a subgroup of $(\mathbb{Q}^*, \cdot)$ (nonzero rational numbers). Either prove that it is or give a specific example of how it fails.

PROOF. Notice that there do not exist inverses under $\cdot$ in $G$ since the numerator is fixed and $n \in \mathbb{Z}/\{0\}$, thus $G$ is not a subgroup of $(\mathbb{Q}^*, \cdot)$. □

**Problem 1.47.** Determine if $K = \{3n : n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. Either prove that it is or give a specific example of how it fails.

PROOF. Notice that $K$ is nonempty, we will now show that $K$ is closed under addition, and contains inverses under addition.

Let $a, b \in K$, then

$$\begin{aligned} a + b &= 3n + 3m, \\ &= 3(n+m), \\ &= 3\ell \quad \text{for some integer } \ell = n + m. \end{aligned}$$

Thus $K$ is closed under addition. Since $-n \in \mathbb{Z}$ we have $a^{-1} = 3(-n) \in K$, so for each $a \in K$ there exists a unique $a^{-1} \in K$. Hence, $K$ is a subgroup. □

**Problem 1.48.** Determine if $K = \{3 + n : n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. Either prove that it is or give a specific example of how it fails.

PROOF. □

**Problem 1.49.** Consider the set $H = \left\{ \begin{pmatrix} a & b \\ -b & -a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. Determine if $H$ is a subgroup of $M_2(\mathbb{R})$ under usual addition of matrices.

PROOF. Let $H$ be as above, notice that $H \neq \emptyset$ is obvious. We will show that $H$ is closed under matrix addition. Let $\mathbf{X}, \mathbf{Y} \in H$, then

$$\begin{aligned} \mathbf{X} + \mathbf{Y} &= \begin{pmatrix} a & b \\ -b & -a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & -c \end{pmatrix}, \\ &= \begin{pmatrix} a+c & b+d \\ -(b+d) & -(a+c) \end{pmatrix}. \end{aligned}$$

Since $\mathbb{R}$ is closed under addition we know that $\mathbf{X} + \mathbf{Y} \in H$, thus $H$ is closed under matrix addition. It remains to show that $H$ has inverses for each of its elements. Notice that for $\mathbf{X} \in H$ we have $\mathbf{X}^{-1} = \begin{pmatrix} -a & -b \\ b & a \end{pmatrix}$ such that $a \neq b$. Hence, $H$ is a subgroup of $M_2(\mathbb{R})$. □

**Problem 1.50.** Determine if the set $K = \{x^2 : x \in \mathbb{R}\}$ is a subgroup of $(\mathbb{R}, +)$. (Note that $x^2$ means usual multiplication.)

PROOF. Notice that $x^2 + y^2 \neq (x+y)^2$ therefore $K$ is not closed under addition and not a subgroup. □

**Problem 1.51.** Determine if the set $K = \{x^2 : x \in \mathbb{R}^+\}$ is a subgroup of $(\mathbb{R}^+, \cdot)$. (Note that $x^2$ means usual multiplication, and $\mathbb{R}^+$ is the set of positive real numbers.)

PROOF. Let $K$ be as above, notice that $K \neq \emptyset$ is obvious. We will show that $K$ is closed under $\cdot$ and has inverses for each of its elements under $\cdot$. Let $a, b \in K$, then there exist $x, y \in \mathbb{R}$ such that $a = x^2, b = y^2$. So we have

$$ab = x^2 y^2 = (xy)^2$$

and since $xy \in \mathbb{R}$ we have that $K$ is closed. It remains to show that $K$ has inverses for each of its elements under $\cdot$. Notice that $a^{-1} = x^{-2} = 1/x^2$ and that $1/x^2 \in \mathbb{R}^+$. Hence, $K$ is a subgroup of $(\mathbb{R}^+, \cdot)$. □

**Problem 1.52.** Let $G$ be a group, and define the set $H = \{a \in G : a^2 = e_G\}$. Prove: If $G$ is abelian then $H$ is a subgroup of $G$. Where does your proof break down if we do not know $G$ is abelian?

PROOF. Let $G, H$ be as above and suppose $G$ is an abelian group. Consider $a \in G$, since $G$ is abelian we know that $a^2 \in G$ so $H$ is nonempty. We will now show that $H$ is closed under $*$. Let $\alpha, \beta \in H$, then for $a, b \in G$ we have $\alpha = a^2, \beta = b^2$, thus,

$$\begin{aligned} \alpha * \beta &= a^2 * b^2, \\ &= a(ab)b, \\ &= a(ba)b, \quad \text{this is where we need that } G \text{ is abelian;} \\ &= (ab)^2. \end{aligned}$$

Thus, $\alpha\beta \in H$, it remains to show that for each $\alpha \in H$ we have $\alpha^{-1} \in H$ such that $\alpha\alpha^{-1} = e_H$. We can see that $\alpha^{-1} = a^{-2}$ fairly easily. Thus, we have shown that the subset of squares of a group is a subgroup. □

**Problem 1.53.** Prove Theorem 1.33.
*Lemma*: Let $G$ be a group, the identity of $G$ is also the identity for $H$, any subgroup of $G$ i.e., $e_G = e_H$.

PROOF. □

*Corollary*: Any pair of subgroups of $G$ are not disjoint because they have their shared identity element in common.

*Theorem.* Let $G$ be a group. If $H_1$ and $H_1$ are both subgroups of $G$ then $H_1 \cap H_2$ is also a subgroup of $G$.

PROOF. Let $G, H_1, H_2$ be as above. We must show that $H_1 \cap H_2$ is nonempty, closed under $*$ and has an inverse for each of its elements under $*$, where $*$ is from $(G, *)$. Since $H_i$ are subgroups they're nonempty, but we must show that their intersection is also nonempty, i.e., we must show that any pair of subgroups of $G$ are not disjoint, which we did in the Lemma. Thus, since $H_1, H_2$ are not disjoint, $H_1 \cap H_2$ is nonempty; it remains to show that $H_1 \cap H_2$ is closed under $*$ and has inverses for each of its elements under $*$.

Let $a, b \in H_1 \cap H_2$, thus $a, b \in H_1, H_2, G$ as well. Notice that $ab \in H_1, H_2$ as well since $H_1, H_2$ are subgroups of $G$, hence $ab \in H_1 \cap H_2$ and thus $H_1 \cap H_2$ is closed under $*$.

Since $G, H_1, H_2$ are groups, for each $a$ in these groups we have $a^{-1}$, thus $a_{-1} \in H_1 \cap H_2$. Hence, $H_1 \cap H_2$ is a subgroup of $G$. □

## 4. Homomorphisms

**Problem 1.54.** Determine if the function $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ defined by $f(x) = 2x \pmod 4$ is a homomorphism between groups $(\mathbb{Z}_8, +_8)$ and $(\mathbb{Z}_4, +_4)$ In this definition $2x$ means usual integer multiplication.

PROOF. Recall that since $\mathbb{Z}_8$ and $\mathbb{Z}_4$ are groups, they are closed. Notice from Figure 9 that the only ouputs of $f$ over $\mathbb{Z}_8$ are 0 and 2. Additionally, observe from Figure 8 that the only outputs of $+_4$ given inputs 0 and 2 are again 0 and 2, thus $f$ is a homomorphism. Thus, for each $a, b \in \mathbb{Z}_8$ we have $f(a)f(b) = f(ab)$. □

**Problem 1.55.** Prove that for any $n \in \mathbb{N}$ with $n > 1$, the function $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = x \pmod n$ is a homomorphism between groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +_n)$.

PROOF. Let $a, b \in \mathbb{Z}$. Observe that $f(a) = a \pmod n$ and $f(b) = b \pmod n$, thus their sum is $f(a)+f(b) = a+b \pmod n$. Also, we have $f(a+b) = a+b \pmod n$, so $f(a + b) = f(a) + f(b)$ as desired. □

**Problem 1.56.** Prove that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 4x$ is a homomorphism of $(\mathbb{Z}, +)$. (Note that $4x$ means usual integer multiplication.)

PROOF. Let $a, b \in \mathbb{Z}$ and $f$ be as above. Then $f(a) = 4a$, $f(b) = 4b$, and $f(a + b) = 4(a + b)$. Additionally, we have $f(a) + f(b) = 4(a + b)$. Hence, $f$ is a homomorphism. □

**Problem 1.57.** Determine if the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2 + 1$ is a homomorphism of$(\mathbb{R}, +)$.

PROOF. Let $g$ be as above, suppose $a, b \in \mathbb{R}$, then $g(a + b) = (a + b)^2 + 1 = a^2 + 2ab + b^2 + 1$. Additionally, we have $g(a) + g(b) = a^2 + b^2 + 2$. Notice that $g(a) + g(b) \neq g(a + b)$, hence $g$ is not a homomorphism. □

**Problem 1.58.** Determine if the function $h : \mathbb{Z} \to \mathbb{Z}$ defined by $h(x) = x^3$ is a homomorphism of $(\mathbb{Z}, +)$.

PROOF. □

**Problem 1.59.** Determine if the function $g : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $g(x) = 1/x$ is a homomorphism of $(\mathbb{R}^+, \cdot)$. Recall that $\mathbb{R}^+$ is the set of positive real numbers.

PROOF. □

**Problem 1.60.** Determine if the function $f : M_2(\mathbb{R}) \to \mathbb{R}$ defined by $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + b$ is a homomorphism. Recall that both $M_2(\mathbb{R})$ and $\mathbb{R}$ use an operation of addition.

PROOF. □

**Problem 1.61.** Use PMI to prove (iii) of Theorem 1.37.

*Theorem.* Let $G$ and $K$ be groups and suppose $f : G \to K$ is a homomorphism. Then the following must hold:

(i) $f(e_G) = e_K$
(ii) $f\left(a^{-1}\right) = (f(a))^{-1}$ for each $a \in G$.
(iii) For every $n \in \mathbb{Z}$ and $a \in G$, $(f(a))^n = f\left(a^n\right)$.
(iv) For every $a \in G$, if $a$ has finite order then $\text{ord}(f(a))$ evenly divides $\text{ord}(a)$.

PROOF. Let $G, K, a, n, f$ be as above. Notice that for $n = 1$ we have $f(a)^1 = f(a^1)$. Assume that for some $n \in \mathbb{N}$ that $(f(a))^n = f\left(a^n\right)$. We compute that,

$$\begin{aligned} (f(a))^{n+1} &= (f(a))^n f(a), \\ &= f\left(a^n\right) f\left(a\right), \\ &= f\left(a^n a\right), \\ &= f\left(a^{n+1}\right). \end{aligned}$$

Thus we have shown that for the given proposition $P$, that $P(n) \Rightarrow P(n + 1)$. □

**Problem 1.62.** Prove (iv) of Theorem 1.37.

PROOF. Let $G, a, f$ be as in the previous problem. Since $a$ has finite order, there exists an $n \in \mathbb{N}$ such that $a^n = e_G$, and $n$ is the least integer with this property. Consider $f(a^n) = f(e_G) = e_K$. From the previous problem we also know that $(f(a))^n = f\left(a^n\right)$, thus $(f(a))^n = e_K$, therefore $n$ is either the order of $f(a)$, or the order of $f(a) = m$ such that $m|n$. Thus, $\text{ord}(f(a))|\,\text{ord}(a)$. □

**Problem 1.63.** Prove (i) of Theorem 1.40.

*Theorem.* Suppose $G$ and $K$ are groups and $f : G \to K$ is an isomorphism.

(i) $G$ is abelian if and only if $K$ is abelian.
(ii) For every $a \in G$, if $a$ has finite order then $\text{ord}(a) = \text{ord}(f(a))$.

PROOF. Let $G, K, f$ be as above. $\Rightarrow$) Suppose $G$ is Abelian, we'll show $K$ is Abelian as well, i.e., that for $a, b \in G$ and the values to which they are mapped $f(a), f(b) \in K$ we have $f(a)f(b) = f(b)f(a)$. Since $G$ is Abelian we know that for $a, b \in G$ we have $ab = ba$, and since $f$ is an isomorphism we have

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a),$$

as we aimed to do.

$\Leftarrow$) Suppose $K$ is Abelian, we'll show that $G$ is Abelian as well. Since $K$ is Abelian we know that for $f(a), f(b) \in K$, we have $f(a)f(b) = f(b)f(a)$. Recall that since $f$ is an isomorphism there exists a unique $f^{-1}$ such that $f^{-1}(f(ab)) = ab$, thus

$$f(a)f(b) = f(ab) = f^{-1}(f(ab)) = ab = ba = f^{-1}(f(ba)) = f(ba) = f(b)f(a).$$

Hence, since $K$ is Abelian and $f$ is an isomorphism, $G$ is also Abelian, as we aimed to show. □

**Problem 1.64.** Prove (ii) of Theorem 1.40.

PROOF. Let $G, K, f$ be as in the previous problem. Suppose $a \in G$ has finite order, $n = \text{ord}(a)$. Then,

$$\begin{aligned} a^n &= e_G, \\ f(a^n) &= f(e_G), \\ (f(a))^n &= e_K. \end{aligned}$$

Thus, $\text{ord}(a) = \text{ord}(f(a))$ as we aimed to show.

□

**Problem 1.65.** Suppose $G$ and $K$ are groups and $f : G \to K$ is a homomorphism. Define the set $f(G) = \{y \in K : \text{there is some } a \in G \text{ with } f(a) = y\}$. Prove that if $f(G)$ is a subgroup of $K$.

PROOF. We proceed directly. Notice that $f(G)$ is the empty set if and only if $G$ is the trivial ring, thus for nontrivial $G$, $f(G)$ is nonempty. Let $x, y \in f(G)$, then there exist $a, b \in G$ such that $f(a) = x, f(b) = y$. We compute the following

$$\begin{aligned} x \star y &= f(a) \star f(b), \\ &= f(a \star b), \\ &= f(c), \quad \text{for } c = a \star b, c \in G. \end{aligned}$$

Since $c \in G$ we know they $f(c) \in f(G)$, thus $f(G)$ is closed under the operation of $(K, \star)$. Since $G, K$ are groups, their elements have inverses, therefore $y^{-1} \in K$ such that $y^{-1} = f(a)$ for some $a \in G$. Then $y^{-1} \in f(G)$. Thus, $f(G)$ is a subgroup of $K$. □

**Problem 1.66.** Suppose that $f : G \to K$ and $g : K \to H$ are homomorphisms of the groups $G$, $K$, and $H$. Prove that the function $g \circ f$ is a homomorphism from $G$ to $H$.

PROOF. Let $f, g, G, K, H$ be as above. Suppose $a \in G, b = f(a) \in K, c = g(b) \in H$. We compute that,

$$\begin{aligned}(g \circ f)(ab) &= (g \circ f)(a) \circ (g \circ f)(b),\\ &= g\left(f(a)f(b)\right),\\ &= g(f(a))g(f(b)),\\ &= (g \circ f)(a) \cdot (g \circ f)(b).\end{aligned}$$

Thus the composition of $f$ and $g$ is also a homomorphism. □

## 5. Groups of Units

**Problem 2.1.** Find the elements of $(U(20), \cdot_{20})$ and show its Cayley table.

PROOF. □

**Problem 2.2.** Find the elements of $(U(12), \cdot_{12})$ and show its Cayley table.

PROOF. □

**Problem 2.3.** Find the elements of $(U(14), \cdot_{14})$ and show its Cayley table.

PROOF. □

**Problem 2.5.** Find the elements of $(U(16), \cdot_{16})$ and show its Cayley table.

PROOF. □

**Problem 2.8.** Find the elements of $(U(11), \cdot_{11})$ and show its Cayley table.

PROOF. □

**Problem 2.11.** In the group $(U(21), \cdot_{21})$ find the order of each element.

PROOF. □

**Problem 2.12.** In the group $(U(20), \cdot_{20})$ find the order of each element.

PROOF. □

**Problem 2.14.** In the group $(U(12), \cdot_{12})$ find the order of each element.

PROOF. □

**Problem 2.16.** In the group $(U(15), \cdot_{15})$ find the order of each element.

PROOF. □

**Problem 2.17.** If we have positive integers $n < m$, is $U(n) \subseteq U(m)$? Give a proof or counterexample.

PROOF. □

**Problem 2.18.** Determine if the set $\{1, 3, 5, 7, 9\}$ is a group under the operation $\cdot_{10}$.

PROOF. □

**Problem 2.19.** Use Euler's function to determine the size of the set $U(p)$ for an arbitrary prime $p$.

PROOF. □

**Problem 2.20.** Prove or disprove: $U(p) = \mathbb{Z}_p - \{0\}$ for $p$ prime.

PROOF. □

**Problem 2.21.** Suppose we have $n = p^2$ when $p$ is prime. Is it true that $U(n) = \mathbb{Z}_n - \{0\}$? Be sure to explain why or why not.

PROOF. □

**Problem 2.22.** Using Euler's function, explain how to find the cardinality of $U(pq)$ when $p$ and $q$ are distinct primes.

PROOF. □

**Problem 2.23.** Using Euler's function, what is the cardinality of $U(35)$?

PROOF. □

**Problem 2.24.** Using Euler's function, what is the cardinality of $U(50)$?

PROOF. □

**Problem 2.25.** Using Euler's function, what is the cardinality of $U(105)$?

PROOF. □

## 6. Cyclic Groups

**Problem 2.26.** Find all of the cyclic subgroups in $(U(20), \cdot_{20})$. Is $U(20)$ a cyclic group?

PROOF. □

**Problem 2.27.** Find all of the cyclic subgroups in $(U(15), \cdot_{15})$. Is $U(15)$ a cyclic group?

PROOF. □

**Problem 2.28.** Find all of the cyclic subgroups in $(U(7), \cdot_7)$. Is $U(7)$ a cyclic group?

PROOF. □

**Problem 2.29.** Find all of the cyclic subgroups in $(U(12), \cdot_{12})$. Is $U(12)$ a cyclic group?

PROOF. □

**Problem 2.30.** Find all of the cyclic subgroups in $(U(30), \cdot_{30})$. Is $U(30)$ a cyclic group?

PROOF. □

**Problem 2.31.** Find all of the cyclic subgroups in $(U(10), \cdot_{10})$. Is $U(lO)$ a cyclic group?

PROOF. □

**Problem 2.32.** Find all of the cyclic subgroups in $(U(9), \cdot_9)$. Is $U(9)$ a cyclic group?

PROOF. □

**Problem 2.33.** Let $G$ denote an arbitrary group with $a, b \in G$. Prove: If $a = b^k$ for some integer $k$, *and* $\text{ord}(a) = \text{ord}(b) = n$ for some $n \in \mathbb{N}$, then $\langle a \rangle = \langle b \rangle$.

PROOF. □

**Problem 2.34.** We needed **finite order** elements in the previous exercise since infinite order elements can make it fail! In the group $\mathbb{Z}$ under usual addition, find nonzero integers $a$ and $b$ with $a = b^k$ for some nonzero integer $k$, both $a$ and $b$ of infinite order, but $\langle a \rangle \neq \langle b \rangle$.

PROOF. □

**Problem 2.35.** Find two integers $1 \leq a \leq 5, 1 \leq b \leq 5$ for which $\langle a \rangle = \langle b \rangle$ is true in one of the groups $(U(7), \cdot_7)$ or $(\mathbb{Z}_6, +_6)$ but is false in the other group.

PROOF. □

**Problem 2.36.** Prove: If $G$ is a cyclic group then $G$ is abelian.

PROOF. □

**Problem 2.37.** Let $G$ and $K$ be groups and $f : G \to K$ an isomorphism. Prove: $G$ is cyclic if and only if $K$ is cyclic.

PROOF. □

**Problem 2.38.** Let $G$ and $K$ be groups and $f : G \to K$ a homomorphism. Prove or disprove: If $G$ is cyclic then $K$ is cyclic.

PROOF. □

**Problem 2.39.** Let $G$ and $K$ be groups. Prove: If $G \times K$ is cyclic then both $G$ and $K$ must be cyclic.

PROOF. □

**Problem 2.40.** Prove (ii) of Theorem 2.16.

PROOF. □

**Problem 2.41.** Prove (i) of Theorem 2.18.

PROOF. □

**Problem 2.42.** Consider the group of functions $\mathcal{F}\mathbb{R}$ under addition of functions. Determine the elements of the cyclic subgroup $\langle f \rangle$ where $f(x) = x - 1$.

PROOF. □

## 7. Permutation Groups

**Problem 2.43.** Prove: If $f : A \to B, g : B \to C$, and $h : C \to D$ are functions, then $h \circ (g \circ f) = (h \circ g) \circ f$.

PROOF. □

**Problem 2.44.** Let $A = \{x \in R : x \neq 0, 1\}$. Determine if $f : A \to A$ defined by $f(x) = 1 - \frac{1}{x}$ is a permutation of $A$.

PROOF. □

**Problem 2.45.** Let $A = \{x \in \mathbb{R} : x \neq 0, 1\}$. Determine if $f : A \to A$ defined by $f(x) = \frac{x}{x-1}$ is a permutation of $A$.

PROOF. □

**Problem 2.46.** Determine if $f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ defined by $f(x) = x^3 \pmod 5$, where $x^3$ denotes usual integer multiplication, is a permutation of $\{0, 1, 2, 3, 4\}$.

PROOF. □

**Problem 2.47.** Determine if $g : \{0, 1, 2, 3, 4, 5\} \to \{0, 1, 2, 3, 4, 5\}$ defined by $g(x) = (x+2) \pmod 6$, where $x+2$ denotes usual integer addition, is a permutation of $\{0, 1, 2, 3, 4, 5\}$.

PROOF. □

**Problem 2.48.** Determine if $h : \{0, 1, 2, 3, 4, 5, 6\} \to \{0, 1, 2, 3, 4, 5, 6\}$ defined by $h(x) = x^2 \pmod 7$, where $x^2$ denotes usual integer multiplication, is a permutation of $\{0, 1, 2, 3, 4, 5, 6\}$.

PROOF. □

**Problem 2.49.** Write $\alpha \circ \alpha$, $\beta \circ \beta$, $\alpha \circ \beta$, and $\beta \circ \alpha$ as products of disjoint cycles for the $\alpha, \beta \in S_7$ defined in Example 2.33.

PROOF. □

**Problem 2.50.** For the permutations $\alpha = (127)(38)(456)$ and $\beta = (23568)(147)$ in $S_8$, write $\alpha \circ \alpha$, $\beta \circ \beta$, $\alpha \circ \beta$, and $\beta \circ \alpha$ as products of disjoint cycles.

PROOF. □

**Problem 2.51.** For the permutations $\alpha = (1254)(36)$ and $\beta = (14678)$ in $S_8$, write $\alpha \circ \alpha$, $\beta \circ \beta$, $\alpha \circ \beta$, and $\beta \circ \alpha$ as products of disjoint cycles.

PROOF. □

**Problem 2.52.** For the permutations $\alpha = (234)(567)$ and $\beta = (2358)(147)$ in $S_8$, write $\alpha^2$, $\alpha^{-1}$, $\alpha \circ \beta$, and $\beta \circ \alpha^{-1}$ as products of disjoint cycles.

PROOF. □

**Problem 2.53.** For the permutations $\alpha = (1356)$ and $\beta = (124)(35)$ in $S_6$, write $\alpha^2$, $\beta^{-1}$, $\alpha \circ \beta$, and $\beta^{-1} \circ \alpha$ as products of disjoint cycles.

PROOF. □

**Problem 2.54.** For the permutations $\alpha = (15)(278)(34)$ and $\beta = (12)(368)$ in $S_8$, write $\alpha^2 \circ \beta$, $\beta^{-1} \circ \alpha$, $\alpha^{-2} \circ \beta$, and $\beta^{-3}$ as products of disjoint cycles.

PROOF. □

**Problem 2.55.** For the permutations $\alpha = (468)$ and $\beta = (1234)(58)$ in $S_8$, write $\alpha^2 \circ \beta$, $\beta^{-1} \circ \alpha$, $\alpha^{-2} \circ \beta$, and $\beta^{-3}$ as products of disjoint cycles.

PROOF. □

**Problem 2.56.** For the permutations $\alpha = (15)(278)(34)$ and $\beta = (12)(368)$ in $S_8$, write $\alpha^3$, $\beta \circ \alpha^2$, $\alpha^{-1} \circ \beta^2$, and $\beta \circ \alpha$ products of disjoint cycles.

PROOF. □

**Problem 2.57.** Show that in $S_k (k < 1)$ two disjoint cycles will commute. That is, if $\alpha = (a_1 a_2 \cdots a_n)$ and $\beta = (b_1 b_2 \cdots b_m)$ are cycles with $\{a_1, a_2, \ldots, a_n\} \cap \{b_1, b_2, \ldots, b_m\} \neq \emptyset$, then $a \circ b = b \circ a$.

PROOF. □

In exercises 58-64, write $\omega$ as a product of transpositions to determine if $\omega$ is even or odd.

**Problem 2.58.** $\omega = (1234)(5678) \in S_8$.

PROOF. □

**Problem 2.59.** $\omega = (23456)(17) \in S_8$.

PROOF. □

**Problem 2.60.** $\omega = (135)(2678) \in S_8$.

PROOF. □

**Problem 2.61.** $\omega = (123)(456)(789) \in S_9$.

PROOF. □

**Problem 2.62.** $\omega = (2345678) \in S_8$.

PROOF. □

**Problem 2.63.** $\omega = (13)(2468) \in S_8$.

PROOF. □

**Problem 2.64.** $\omega = (14)(356) \in S_7$.

PROOF. □

**Problem 2.65.** Find an odd permutation of $S_8$ which (when written as a product of disjoint cycles) includes a cycle of length 5. What is its order?

PROOF. □

**Problem 2.66.** Write the permutation $\omega = (1234)(678) \in S_8$ as a product of transpositions two different ways. Be sure to check that the product of the transpositions really does give you the same permutation.

PROOF. □

**Problem 2.67.** Write the permutation $\omega = (127)(348)(56) \in S_8$ as a product of transpositions two different ways. Be sure to check that the product of the transpositions really does give you the same permutation.

PROOF. □

**Problem 2.68.** Write the permutation $\omega = (13)(456)(27) \in S_8$ as a product of transpositions two different ways. Be sure to check that the product of the transpositions really does give you the same permutation.

PROOF. □

**Problem 2.69.** Prove: For any $k > 1$, a cycle in $S_k$ of length $m > 1$ is even (as a permutation) if and only if $m$ is odd (as an integer).

PROOF. □

**Problem 2.70.** Prove: For any $k > 1$ and any permutation $\alpha \in S_k$, $\alpha^2$ must be an even permutation.

PROOF. □

**Problem 2.71.** Prove: If $k \geq 3$ and $\alpha \in S_k$ is a cycle of length 3, $\alpha = (a_1 a_2 a_3)$, then $\text{ord}(a) = 3$.

PROOF. □

**Problem 2.72.** Let $k > 1$ and $a \in S_k$ a cycle of length $m > 1$. Prove: $a^2$ is a cycle if and only if $m$ is odd.

PROOF. □

## 8. ⋆Dihedral Groups

## 9. ⋆Symmetric Groups

## 10. ⋆Matrix Groups

## 11. ⋆The Quaternion Group

CHAPTER 2

# Quotient Groups

**0.1. Cosets.**

**0.2. Normal Subgroups.**

**0.3. Quotient Groups.**

**0.4. *The Isomorphism Theorems.**

**0.5. Homomorphic Images of a Group.**

**0.6. Theorems of Cauchy and Sylow.**

CHAPTER 3

# *Group Actions

**0.1. *Introduction to Group Actions.**

**0.2. *Group Actions and Permutation Representations.**

**0.3. *Groups Acting on Themselves by Left Multiplication – Cayley's Theorem.**

**0.4. *Groups Acting on Themselves by Conjugation – The Class Equation.**

**0.5. *Automorphisms.**

**0.6. *The Sylow Theorems.**

**0.7. *The Simplicity of $A_n$.**

APPENDIX A

# Figures

**0.1. Cayley Tables.** These are the Cayley tables required for several of the problems involving showing a set and binary operation form a group or subgroup.

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

FIGURE 1. Cayley Table for $(\mathbb{Z}_6, +_6)$ from Problem 1.3.17

| $*_{5\times2}$ | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) | (4,0) | (4,1) |
|---|---|---|---|---|---|---|---|---|---|---|
| (0,0) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) | (4,0) | (4,1) |
| (0,1) | (0,1) | (0,0) | (1,1) | (1,0) | (2,1) | (2,0) | (3,1) | (3,0) | (4,1) | (4,0) |
| (1,0) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) | (4,0) | (4,1) | (0,0) | (0,1) |
| (1,1) | (1,1) | (1,0) | (2,1) | (2,0) | (3,1) | (3,0) | (4,1) | (4,0) | (0,1) | (0,0) |
| (2,0) | (2,0) | (2,1) | (3,0) | (3,1) | (4,0) | (4,1) | (0,0) | (0,1) | (1,0) | (0,1) |
| (2,1) | (2,1) | (2,0) | (3,1) | (3,0) | (4,1) | (4,0) | (0,1) | (0,0) | (1,1) | (1,0) |
| (3,0) | (3,0) | (3,1) | (4,0) | (4,1) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) |
| (3,1) | (3,1) | (3,0) | (4,1) | (4,0) | (0,1) | (0,0) | (1,1) | (1,0) | (2,1) | (2,0) |
| (4,0) | (4,0) | (4,1) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) |
| (4,1) | (4,1) | (4,0) | (0,1) | (0,0) | (1,1) | (1,0) | (2,1) | (2,0) | (3,1) | (3,0) |

FIGURE 2. Cayley Table for $(\mathbb{Z}_5 \times \mathbb{Z}_2, *_{5\times2})$ from Problem 1.3.18

| $*$ | S | H | V | D |
|---|---|---|---|---|
| S | S | H | V | D |
| H | H | S | D | V |
| V | V | D | S | H |
| D | D | V | H | S |

FIGURE 3. Cayley Table for $(G, *)$ from Problem 1.21

**0.2. Tables for Functions on Finite Sets.** These are the tables that define some functions over finite sets for certain problems.

| $\times$ | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ |
|---|---|---|---|---|
| $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ |
| $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ |
| $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ |
| $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ | $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ | $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ |

FIGURE 4. Cayley Table for $(A, \times)$ from Problem 1.22

| $+_{12}$ | 0 | 3 | 6 | 9 |
|---|---|---|---|---|
| 0 | 0 | 3 | 6 | 9 |
| 3 | 3 | 6 | 9 | 0 |
| 6 | 6 | 9 | 0 | 3 |
| 9 | 9 | 0 | 3 | 6 |

FIGURE 5. Cayley Table for Problem 1.40

| $+_{18}$ | 0 | 2 | 4 | 8 | 16 |
|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 8 | 16 |
| 2 | 2 | 4 | 6 | 10 | 0 |
| 4 | 4 | 6 | 8 | 12 | 2 |
| 8 | 8 | 10 | 12 | 16 | 6 |
| 16 | 16 | 0 | 2 | 6 | 4 |

FIGURE 6. Cayley Table for Problem 1.42

| $*$ | (0,0) | (0,2) | (1,0) | (1,2) |
|---|---|---|---|---|
| (0,0) | (0,0) | (0,2) | (1,0) | (1,2) |
| (0,2) | (0,2) | (0,0) | (1,2) | (1,0) |
| (1,0) | (1,0) | (1,2) | (0,0) | (0,2) |
| (1,2) | (1,2) | (1,0) | (0,2) | (0,0) |

FIGURE 7. Cayley Table for Problem 1.43

| $+_4$ | $f(a) = 0$ | $f(b) = 2$ |
|---|---|---|
| $f(a) = 0$ | 0 | 2 |
| $f(b) = 2$ | 2 | 0 |

FIGURE 8. Cayley Table for part of Problem 1.54 where $f(a), f(b) \in \mathbb{Z}_4$, and $a, b \in \mathbb{Z}_8$

| $a$ | $2a \pmod 4$ |
|---|---|
| 0 | 0 |
| 1 | 2 |
| 2 | 0 |
| 3 | 2 |
| 4 | 0 |
| 5 | 2 |
| 6 | 0 |
| 7 | 2 |

FIGURE 9. Function table for $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ mapped by $a \mapsto 2a \pmod 4$ from Problem 1.54.