Solutions to Dummit & Foote's Abstract Algebra 3rd Edition

JR

October 27th, 2025

Contents

Preface

This is a collection of solutions to the exercises in Dummit and Foote's *Abstract Algebra*, 3rd edition. These solutions were written by me as I worked through the book, and are intended to serve as a reference for myself and others who are studying abstract algebra. I have made every effort to ensure the correctness of these solutions, but I cannot guarantee that they are free of errors. If you find any mistakes or have suggestions for improvement, please feel free to contact me.

I've attempted to format the solutions in a clear and consistent manner, using LaTeX for typesetting. Each chapter's exercises are included in separate files for better organization if viewing on GitHub. Moreover, solutions to exercises only utilize techniques that are available to an advanced undergraduate student or beginning graduate student, in line with the intended audience of the textbook. As an aside, I've graduated from a bachelor's program in mathematics but have not pursued graduate studies, so my background is primarily at the undergraduate level.

Some suggestions I've been given to improve the guide are citing particularly important exercises that will prove useful in reading subsequent chapters, and providing writeups/discussions for why I choose a particular method of solution (such as functions/homomorphisms that may appear out of nowhere). Most problems are enclosed in the following environment:

Exercise 0.0.1

Example exercise.

However, there are some exercises that I found to be either challenging, interesting, or useful for the development of later material. These exercises are enclosed in a special environment:

(∗) **Exercise 0.0.2**

Example special exercise.

This is to highlight these exercises for future readers who may want to focus on them.

Many thanks to the authors, David S. Dummit and Richard M. Foote, for writing such an excellent textbook that has been a valuable resource for my recreational studies in abstract algebra. I've received requests on Reddit for individuals to assist me in completing this project, but at this time I prefer to work on it independently. However, I welcome feedback and suggestions from anyone who is interested in contributing to the project in the future.

0 Preliminaries

0.1 Basics

For Exercises 1 to 4, let

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

and $\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}$, where $\mathcal{A}$ denotes the set of 2×2 matrices with real entries.

Exercise 0.1.1

Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Solution. Note that the 1st matrix is M itself so that it belongs to $\mathcal{B}$, since $MX = XM = M^2$. Further note that the 3rd, 5th, and 6th matrices are the zero, identity, and exchange matrices respectively. Then the 3rd and 5th belong to $\mathcal{B}$ while the 6th does not. Then only the remaining matrices to check are the 2nd and 4th matrices. For the 2nd matrix:

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 1\cdot 1 & 1\cdot 1 + 1\cdot 1 \\ 0\cdot 1 + 1\cdot 1 & 0\cdot 1 + 1\cdot 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$$

$$XM = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 1\cdot 0 & 1\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 1\cdot 0 & 1\cdot 1 + 1\cdot 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$$

Then $MX \neq XM$ and the 2nd matrix does not belong to $\mathcal{B}$. For the 4th matrix:

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 1\cdot 1 & 1\cdot 1 + 1\cdot 0 \\ 0\cdot 1 + 1\cdot 1 & 0\cdot 1 + 1\cdot 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$XM = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 1\cdot 0 & 1\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 0 & 1\cdot 1 + 0\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

So that $MX \neq XM$. ■

Exercise 0.1.2

Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ where $+$ denotes the usual sum of two matrices.

Solution. We calculate the following:

$$\begin{aligned} M(P+Q) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \\ &= \begin{pmatrix} a+e+c+g & b+f+d+h \\ c+g & d+h \end{pmatrix} \\ &= \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} + \begin{pmatrix} e+g & f+h \\ g & h \end{pmatrix} \\ &= MP + MQ \\ &= PM + QM \\ &= \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} + \begin{pmatrix} e & e+f \\ g & g+h \end{pmatrix} \\ &= \begin{pmatrix} a+e & a+e+b+f \\ c+g & c+g+d+h \end{pmatrix} \\ &= \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= (P+Q)M \end{aligned}$$

■

Exercise 0.1.3

Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ where $\cdot$ denotes the usual product of two matrices.

Solution. Using PQ, proceed as we did above with $M(PQ)$. Rewriting the entries will result in $(MP)Q$. Since $P \in \mathcal{B}$, then we have $(PM)Q$. We rewrite entries again to result in $P(MQ)$. Because $Q \in \mathcal{B}$, we have $P(QM)$, and a final rewrite results in $(PQ)M$. ■

Exercise 0.1.4

Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

Solution. Let X be the matrix described above. Note that

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$
$$XM = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

Because $X \in \mathcal{B}$, then we may compare entries to obtain the following:

$$\begin{cases} p+r = p \\ q+s = p+q \\ r = r \\ s = r+s \end{cases}$$

The first and fourth equations force $r = 0$, and the second equation forces $p = s$. Then $\mathcal{B}$ is classified as

$$\mathcal{B} = \left\{ \begin{pmatrix} p & p+q \\ 0 & p \end{pmatrix} \middle| \; p, q \in \mathbb{R} \right\}$$ ■

Exercise 0.1.5

Determine whether the following functions f are well defined:

(a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.

(b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

Solution.

(a) No, because $1/2 = 2/4$, but $f(1/2) = 1$ and $f(2/4) = 2$.

(b) Yes; suppose $a/b = c/d$. Then $ad = bc$, or that $a^2d^2 = b^2c^2$. Then $a^2/b^2 = c^2/d^2$, or $f(a/b) = f(c/d)$. ■

Exercise 0.1.6

Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

Solution. No. Note that $1 = 1.000\ldots = 0.999\ldots$, but $f(1.000\ldots) = 1$ and $f(0.999\ldots) = 9$. ■

Exercise 0.1.7

Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \iff f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

Solution. Since $=$ is an equivalence relation on B, then $\sim$ is an equivalence relation.

Consider an equivalence class of some $a \in A$, which is the set $\{x \in A \mid x \sim a\}$. By definition of $\sim$, this is the set $\{x \in A \mid f(x) = f(a)\}$, which is precisely the fiber of f over $f(a)$. Since f is surjective, every fiber of f is nonempty, and every fiber corresponds to some equivalence class of $\sim$. ■

0.2 Properties of the Integers

Exercise 0.2.1

For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y.

(a) $a = 20, b = 13$
(b) $a = 69, b = 372$
(c) $a = 792, b = 275$
(d) $a = 11391, b = 5673$
(e) $a = 1761, b = 1567$
(f) $a = 507885, b = 60808$

Solution. For this exercise, we will only do (e) as that has the most steps in calculating both the gcd and the Euclidean Algorithm. The lcm is obtained by dividing the product ab by (a, b).

(a) $(20, 13) = 1, \text{lcm}(20, 13) = 260, 1 = 2(20) - 3(13)$
(b) $(69, 372) = 3, \text{lcm}(69, 372) = 8556, 27(69) - 5(372)$
(c) $(792, 275) = 11, \text{lcm}(792, 275) = 19800, 8(792) - 23(275)$
(d) $(11391, 5673) = 3, \text{lcm}(11391, 5673) = 21540381, 3 = 253(5673) - 126(11391)$
(e) Applying the Euclidean Algorithm to $a = 1761$ and $b = 1567$, we get:

$$\begin{aligned} 1761 &= (1)1567 + 194 \\ 1567 &= (8)194 + 15 \\ 194 &= (12)15 + 14 \\ 15 &= (1)14 + 1 \end{aligned}$$

Then $(1761, 1567) = 1$ so that $\text{lcm}(1761, 1567) = 2759487$. Reversing the Euclidean Algorithm steps to solve for 1, we get:

$$\begin{aligned} 1 &= 15 - 14 \\ &= 15 - (194 - 12(15)) = 13(15) - 194 \\ &= 13(1567 - 8(194)) - 194 = 13(1567) - 105(194) \\ &= 13(1567) - 105(1761 - 1567) = -105(1761) + 118(1567) \end{aligned}$$

(f) $(507885, 60808) = 691, \text{lcm}(507885, 60808) = 44693880, 691 = 142(60808) - 17(507885)$ ■

Exercise 0.2.2

Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t.

Solution. Since $k \mid a$ and $k \mid b$, there exists $x, y \in \mathbb{Z}$ such that $a = kx$ and $b = ky$. Then for any $s, t \in \mathbb{Z}$, we have $as + bt = kxs + kyt = k(xs + yt)$ which is divisible by k. ■

Exercise 0.2.3

Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

Solution. By the Fundamental Theorem of Arithmetic, n has at least two prime factors a, b such that $1 < a, b < n$. Putting $n = ab$, then $n \mid ab$ but $n \nmid a$ and $n \nmid b$. ■

Exercise 0.2.4

Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers

$$x = x_0 + \frac{b}{d}t \text{ and } y = y_0 - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is in fact the general solution).

Solution. We have

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 = N \end{aligned}$$

■

Exercise 0.2.5

Determine the value $\varphi(n)$ each integer $n \leq 30$ where φ denotes the Euler φ-function.

Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\varphi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

■

Exercise 0.2.6

Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

Solution. Let $S \subseteq \mathbb{Z}^+$ be nonempty. We proceed by induction that S has a minimal element. Assume, by way of contradiction, that S has no minimal element, and let S' be the set of elements that are not in S. Since the minimal element of $\mathbb{Z}^+$ is 0, then $0 \notin S$ so that $0 \in S'$. Now for some $k \in \mathbb{Z}^+$, suppose every integer j such that $0 \leq j \leq k$ is in S'. Then $k + 1 \notin S$, since if it were, then it would be the minimal element of S (as every integer less than or equal to k is in S'). Thus, $k + 1 \in S'$. By induction, every integer in $\mathbb{Z}^+$ is in S', contradicting that S is nonempty. Thus, S has a minimal element.

To prove uniqueness of the minimal element, suppose S has two minimal elements x and y. Then by definition of minimality, $x \leq y$ and $y \leq x$, so that $x = y$. ■

Exercise 0.2.7

If p is a prime, prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p}$ is not a rational number).

Solution. Assume, by way of contradiction, that there exist nonzero integers a and b such that $a^2 = pb^2$. Without loss of generality, we may assume that a and b have no common factors (otherwise, we could divide them both by their greatest common divisor). Then $p \mid a^2$, so that $p \mid a$. Then there exists some integer k such that $a = pk$. We then have

$$a^2 = (pk)^2 = p^2k^2 = pb^2$$

so that $b^2 = pk^2$. Then $p \mid b^2$, so that $p \mid b$. However, this contradicts our assumption that a and b have no common factors. Thus, there do not exist nonzero integers a and b such that $a^2 = pb^2$. ■

Exercise 0.2.8

Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\dots 2\cdot 1$ (it involves the greatest integer function).

Solution. Note that there exists some $k \in \mathbb{Z}^+$ such that $n \geq kp$. Then the multiples of p less than or equal to n are $p, 2p, 3p, \dots, kp$, contributing k factors of p. Further, the multiples of p^2 less than or equal to n are $p^2, 2p^2, 3p^2, \dots, lp^2$ where l is the largest integer such that $lp^2 \leq n$. These contribute an additional l factors of p. Continuing this process until we reach p^m where m is the largest integer such that $p^m \leq n$, we find that $m = \log_p n$. Then the largest power of p which divides $n!$ is given by

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^m} \right\rfloor = \sum_{i=1}^{m} \left\lfloor \frac{n}{p^i} \right\rfloor$$

■

Exercise 0.2.9

Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y.

Require: Integers a, b with $a \geq b > 0$
Ensure: Integers g, x, y such that $g = (a, b)$ and $ax + by = g$

```
1:  procedure GCD(a, b)
2:      A, B ← a, b
3:      x_0, y_0 ← 1, 0                          ▷ a = 1·A + 0·B
4:      x_1, y_1 ← 0, 1                          ▷ b = 0·A + 1·B
5:      while a ≠ b do:
6:          if a > b then
7:              a ← a − b
8:              x_0, y_0 ← x_0 − x_1, y_0 − y_1   ▷ Update coefficients for a
9:          else
10:             b ← b − a
11:             x_1, y_1 ← x_1 − x_0, y_1 − y_0   ▷ Update coefficients for b
12:         end if
13:     end while
14:     g ← a
15:     return (g, x_0, y_0)
16: end procedure
```

Exercise 0.2.10

Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ-function. Conclude in particular that φ tends to infinity as n tends to infinity.

Solution. Fix $N \in \mathbb{Z}^+$. Consider $n \in \mathbb{Z}^+$ such that $\varphi(n) = N$. By the Fundamental Theorem of Arithmetic, we may express n as a product of primes $p_1, p_2, \ldots, p_k$ such that $p_1 < p_2 < \cdots < p_k$. Moreover, we have exponents $\alpha_1, \alpha_2, \ldots, \alpha_k$ for each prime. Using the identity that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ for any prime p and integer $\alpha \geq 1$, then

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

Since $\varphi(n) = N$, then N may be expressed as a product of the terms $p_i^{\alpha_i-1}(p_i - 1)$ for $1 \leq i \leq k$. Note that each term is at least 1, so that there are only finitely many ways to express N as a product of such terms. Further, for each term, there are only finitely many choices of p_i and α_i that yield that term. Thus, there are only finitely many integers n such that $\varphi(n) = N$.

To see that φ tends to infinity as n tends to infinity, assume, by way of contradiction, that φ does not tend to infinity as n tends to infinity. Then there exists $M \in \mathbb{Z}^+$ such that $\varphi(n) \leq M$ for infinitely many n. However, there are only finitely many n such that $\varphi(n) \leq K$ for all $K \leq M$ by the first part of this exercise, contradicting our assumption. Thus, φ tends to infinity as n tends to infinity. ■

Exercise 0.2.11

Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ-function.

Solution. By the Fundamental Theorem of Arithmetic, we may express n as a product of primes $p_1, p_2, \ldots, p_k$ such that $p_1 < p_2 < \cdots < p_k$. Moreover, we have exponents $\alpha_1, \alpha_2, \ldots, \alpha_k$ for each prime. Since d is a divisor of n, we may express d as $p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ where $0 \leq \beta_i \leq \alpha_i$ for all $1 \leq i \leq k$. Using the identity that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ for any prime p and integer $\alpha \geq 1$, then

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \quad \text{and} \quad \varphi(d) = \prod_{i=1}^{k} \varphi(p_i^{\beta_i}) = \prod_{i=1}^{k} p_i^{\beta_i - 1}(p_i - 1)$$

It is now clear that $\varphi(d) \mid \varphi(n)$, since $p_i - 1$ divides itself and $p_i^{\beta_i-1}$ divides $p_i^{\alpha_i-1}$ for all $1 \leq i \leq k$. ■

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Exercise 0.3.1

Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

Solution.

$$\begin{aligned}
\bar{0} &= \{0+18k : k \in \mathbb{Z}\} = \{0, 18, -18, 36, -36, \ldots\} \\
\bar{1} &= \{1+18k : k \in \mathbb{Z}\} = \{1, 19, -17, 37, -35, \ldots\} \\
\bar{2} &= \{2+18k : k \in \mathbb{Z}\} = \{2, 20, -16, 38, -34, \ldots\} \\
\bar{3} &= \{3+18k : k \in \mathbb{Z}\} = \{3, 21, -15, 39, -33, \ldots\} \\
\bar{4} &= \{4+18k : k \in \mathbb{Z}\} = \{4, 22, -14, 40, -32, \ldots\} \\
\bar{5} &= \{5+18k : k \in \mathbb{Z}\} = \{5, 23, -13, 41, -31, \ldots\} \\
\bar{6} &= \{6+18k : k \in \mathbb{Z}\} = \{6, 24, -12, 42, -30, \ldots\} \\
\bar{7} &= \{7+18k : k \in \mathbb{Z}\} = \{7, 25, -11, 43, -29, \ldots\} \\
\bar{8} &= \{8+18k : k \in \mathbb{Z}\} = \{8, 26, -10, 44, -28, \ldots\} \\
\bar{9} &= \{9+18k : k \in \mathbb{Z}\} = \{9, 27, -9, 45, -27, \ldots\} \\
\overline{10} &= \{10+18k : k \in \mathbb{Z}\} = \{10, 28, -8, 46, -26, \ldots\} \\
\overline{11} &= \{11+18k : k \in \mathbb{Z}\} = \{11, 29, -7, 47, -25, \ldots\} \\
\overline{12} &= \{12+18k : k \in \mathbb{Z}\} = \{12, 30, -6, 48, -24, \ldots\} \\
\overline{13} &= \{13+18k : k \in \mathbb{Z}\} = \{13, 31, -5, 49, -23, \ldots\} \\
\overline{14} &= \{14+18k : k \in \mathbb{Z}\} = \{14, 32, -4, 50, -22, \ldots\} \\
\overline{15} &= \{15+18k : k \in \mathbb{Z}\} = \{15, 33, -3, 51, -21, \ldots\} \\
\overline{16} &= \{16+18k : k \in \mathbb{Z}\} = \{16, 34, -2, 52, -20, \ldots\} \\
\overline{17} &= \{17+18k : k \in \mathbb{Z}\} = \{17, 35, -1, 53, -19, \ldots\}
\end{aligned}$$

■

Exercise 0.3.2

Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ (use the Division Algorithm).

Solution. Let $a \in \mathbb{Z}$. By the Division Algorithm, there exists unique integers q and r such that $a = nq + r$ where $0 \leq r < n$. Then $a \equiv r \bmod n$, so that $a \in \bar{r}$. Since $0 \leq r < n$, then $\bar{r}$ is one of $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Thus, every equivalence class in $\mathbb{Z}/n\mathbb{Z}$ is one of $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Moreover, these equivalence classes are distinct since if $\bar{i} = \bar{j}$ for some $0 \leq i, j < n$, then $i \equiv j \bmod n$, so that $n \mid (i-j)$. However, since $-n < i - j < n$, then $i - j = 0$, or $i = j$. Thus, the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. ■

Exercise 0.3.3

Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0) \bmod 9$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9—in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9) [note that $10 \equiv 1 \bmod 9$].

Solution. Using the note, then

$$\begin{aligned}
a &\equiv (a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0) \bmod 9 \\
&\equiv (a_n 1^n + a_{n-1}1^{n-1} + \cdots + a_1 1 + a_0) \bmod 9 \\
&= (a_n + a_{n-1} + \cdots + a_1 + a_0) \bmod 9
\end{aligned}$$

■

Exercise 0.3.4

Compute the remainder when 37^{100} is divided by 29.

Solution. Note the following:

$$\begin{aligned}
37^2 &\equiv 6 \bmod 29\\
37^4 &\equiv 6^2 \bmod 29 \equiv 7 \bmod 29\\
37^8 &\equiv 7^2 \bmod 29 \equiv 20 \bmod 29\\
37^{16} &\equiv 20^2 \bmod 29 \equiv 23 \bmod 29 \equiv -6 \bmod 29\\
37^{32} &\equiv (-6)^2 \bmod 29 \equiv 7 \bmod 29\\
37^{64} &\equiv 20 \bmod 29
\end{aligned}$$

Then we have

$$37^{64}37^{32}37^4 \equiv 20 \cdot 7 \cdot 7 \bmod 29 \equiv 20^2 \bmod 29 \equiv 23 \bmod 29$$

Hence the remainder when dividing 37^{100} by 29 is 23. ■

Exercise 0.3.5

Compute the last two digits of 9^{1500}.

Solution. Recall that we take a number mod 100 to find the last two digits. Note that $9^4 \equiv 61 \bmod 100$, and $9^3 \equiv 29 \bmod 100$. Then

$$9^6 = (9^3)^2 \bmod 100 \equiv 29^2 \bmod 100 \equiv 41 \bmod 100.$$

Further,

$$9^{10} = 9^6 \cdot 9^4 \bmod 100 \equiv 41 \cdot 61 \bmod 100 \equiv 1 \bmod 100.$$

Then

$$9^{1500} = (9^{10})^{150} \bmod 100 \equiv 1^{150} \bmod 100 \equiv 1 \bmod 100.$$

Thus, the last two digits of 9^{1500} are 01. ■

Exercise 0.3.6

Prove that the square of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.

Solution.

$$\begin{aligned}
0^2 &= 0 \equiv 0 \bmod 4\\
1^2 &= 1 \equiv 1 \bmod 4\\
2^2 &= 4 \equiv 0 \bmod 4\\
3^2 &= 9 \equiv 1 \bmod 4
\end{aligned}$$

■

Exercise 0.3.7

Prove that for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).

Solution. Since a^2 and b^2 is either 0 mod 4 or 1 mod 4, then we have 4 potential sums:

$$\begin{aligned}
0 + 0 &\equiv 0 \bmod 4\\
0 + 1 &\equiv 1 \bmod 4\\
1 + 0 &\equiv 1 \bmod 4\\
1 + 1 &\equiv 2 \bmod 4
\end{aligned}$$

In any of the sums, there is no remainder of 3 when dividing by 4. ■

Exercise 0.3.8

Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b and c. [Consider the equation mod 4 as in the previous two exercises and show that a, b and c would all have to be divisible by 2. Then each of a^2, b^2 and c^2 has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

Solution. We consider the equation in mod 4. By Exercise 0.3.7, the left side of the equation can only be 0, 1, or 2 mod 4. However, the right side is $3c^2$, which is either 0 mod 4 or 3 mod 4 since c^2 is either 0 mod 4 or 1 mod 4 by Exercise 0.3.6. Thus, both sides must be 0 mod 4, so that $4 \mid a^2 + b^2$ and $4 \mid 3c^2$.

It is easy to see that if $4 \mid c^2$, then $2 \mid c$. We now consider the fact that $4 \mid a^2 + b^2$. If both a and b are odd, then $a^2 + b^2 \equiv 2 \bmod 4$, which is false. If one of a or b is odd and the other is even, then $a^2 + b^2 \equiv 1 \bmod 4$, which is false. Thus, both a and b are even, so that $2 \mid a$ and $2 \mid b$. Then there exist integers a_0, b_0, c_0 such that $a = 2a_0, b = 2b_0$, and $c = 2c_0$. Substituting these into the original equation, we have

$$4a_0^2 + 4b_0^2 = 12c_0^2 \implies a_0^2 + b_0^2 = 3c_0^2.$$

However, this contradicts our assumption that a, b, and c are nonzero integers, since we have found a smaller set of integers a_0, b_0, and c_0 that satisfy the same equation. Iterating this process leads to a contradiction, so there are no nonzero integers a, b, and c such that $a^2 + b^2 = 3c^2$. ■

Exercise 0.3.9

Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Solution. Let a be an odd integer. Then there exists some integer k such that $a = 2k + 1$. Then

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Since one of k or $k + 1$ is even, then $2 \mid k(k + 1)$, hence $8 \mid 4k(k + 1)$. Thus, $a^2 \equiv 1 \bmod 8$. ■

(∗) Exercise 0.3.10

Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ-function.

Solution. Recall that $\varphi(n)$ is defined as the number of integers a such that $1 \le a \le n$, and $(a, n) = 1$. Hence, to prove that the number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$, it suffices to prove that $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $(a, n) = 1$.

- ($\Rightarrow$) Suppose $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then there exists some $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\overline{a} \cdot \overline{b} = \overline{1}$, or $ab \equiv 1 \bmod n$. Then there exists some integer k such that $ab - 1 = kn$, or $ab - kn = 1$. Thus, $(a, n) = 1$.
- ($\Leftarrow$) Suppose $(a, n) = 1$. Then there exist integers x and y such that $ax + ny = 1$. Then $ax \equiv 1 \bmod n$, so that $\overline{a} \cdot \overline{x} = \overline{1}$. Thus, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

Exercise 0.3.11

Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution. Since $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then there exist $\overline{c}, \overline{d} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\overline{a} \cdot \overline{c} = \overline{1}$ and $\overline{b} \cdot \overline{d} = \overline{1}$. Then

$$(\overline{a} \cdot \overline{b})(\overline{c} \cdot \overline{d}) = \overline{a}(\overline{b} \cdot \overline{d}) \cdot \overline{c} = \overline{a} \cdot \overline{1} \cdot \overline{c} = \overline{a} \cdot \overline{c} = \overline{1},$$

so that $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

Exercise 0.3.12

Let $n \in \mathbb{Z}, n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \bmod n$ and deduce that there cannot be an integer c such that $ac \equiv 1 \bmod n$.

Solution. Since $(a, n) = d > 1$, then there exist integers x and y such that $ax + ny = d$. Let $b = n/d$. Then

$$ab = a(n/d) = n(a/d) \equiv 0 \bmod n,$$

so that such a b exists, since $a/d, n/d \in \mathbb{Z}$. Moreover, if there existed some integer c such that $ac \equiv 1 \bmod n$, then we would have $(ac)b = (ab)c \equiv b \bmod n$. This contradicts that $ab \equiv 0 \bmod n$, so such a c cannot exist. ■

Exercise 0.3.13

Let $n \in \mathbb{Z}, n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \bmod n$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers].

Solution. Since $(a, n) = 1$, there exists $c, x \in \mathbb{Z}$ such that $ac + nx = 1$. Then $ac \equiv 1 \bmod n$. ■

Exercise 0.3.14

Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.

Solution. The previous two exercises show that a and n are relatively prime if and only if there exists b such that $ab \equiv 1 \bmod n$, which is exactly the proposition. For $n = 12$, the elements $1, 5, 7, 11$ are relatively prime to 12, so that $(\mathbb{Z}/11\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ whose inverses are $\overline{1}, \overline{7}, \overline{5}, \overline{11}$ respectively. ■

Exercise 0.3.15

For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

(a) $a = 13, n = 20$

(b) $a = 69, n = 89$

(c) $a = 1891, n = 3797$

(d) $a = 6003722857, n = 77695236973$

Solution. To proceed with these exercises, we will need to use the Euclidean Algorithm to find (a, n), then use the series of quotients and remainders to express 1 as a $\mathbb{Z}$-linear combination of a and n in order to find the inverse. In particular, we will obtain a combination in the form of $ax + ny = 1$. Then $ax \equiv 1 \bmod n$ so that the inverse of a is x. Refer to Exercise 0.2.1 to see how we applied the Euclidean Algorithm.

(a) $-3(13) + 2(20) = 1 \implies -3 \cdot 13 \equiv 1 \bmod 20$, so the inverse is $\overline{-3} = \overline{17}$.

(b) $40(69) - 31(89) = 1 \implies 40 \cdot 69 \equiv 1 \bmod 89$, so the inverse is $\overline{40}$.

(c) $253(1891) - 126(3797) = 1 \implies 253 \cdot 1891 \equiv 1 \bmod 3797$, so the inverse is $\overline{253}$.

(d) $17n - 220a = 1 \implies -220a \equiv 1 \bmod n \implies 77695237193a \equiv 1 \bmod n$, so the inverse is $\overline{77695237193}$.

■

Exercise 0.3.16

Write a computer program to add and multiply mod n, for any n given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if $(a, n) = 1$, an integer c between 1 and $n - 1$ such that $\bar{a} \cdot \bar{c} = \bar{1}$ may be printed on request. (Your program should not, of course, simply quote "mod" functions already built into many systems).

Solution. Using the function GCD from Exercise 0.2.9, we have the following algorithm:

Require: Integers a, b, n with $n > 1$
Ensure: $\bar{a} + \bar{b}$ and $\bar{a} \cdot \bar{b}$, reduced modulo n, and if $(a, n) = 1$, the multiplicative inverse of $\bar{a}$ mod n

```
1:  procedure AddMod(a, b, n)
2:      s ← a + b
3:      while s < 0 do:
4:          s ← s + n
5:      end while
6:      while s ≥ 0 do:
7:          s ← s − n
8:      end while
9:      return s
10: end procedure
11: procedure MultiplyMod(a, b, n)
12:     p ← a · b
13:     while p < 0 do:
14:         p ← p + n
15:     end while
16:     while p ≥ 0 do:
17:         p ← p − n
18:     end while
19:     return p
20: end procedure
21: procedure InverseMod(a, n)
22:     (g, x, y) ← GCD(a, n)
23:     if g ≠ 1 then
24:         return "No inverse exists"
25:     else
26:         while x < 0 do:
27:             x ← x + n
28:         end while
29:         while x ≥ 0 do:
30:             x ← x − n
31:         end while
32:         return x
33:     end if
34: end procedure
```

1 Introduction to Groups

1.1 Basic Axioms and Examples

Let G be a group.

Exercise 1.1.1

Determine which of the following binary operations are associative:

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by

$$(a, b) \star (c, d) = (ad + bc,\ bd)$$

(e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$

Solution.

(a) Not associative: $(1 \star 0) \star 1 = 0 \neq 2 = 1 \star (0 \star 1)$.

(b) Associative:

$$\begin{aligned}(a \star b) \star c &= (a + b + ab) \star c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a + b + c + bc + ab + ac + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a \star (b + c + bc) \\ &= a \star (b \star c)\end{aligned}$$

(c) Not associative: $(1 \star 0) \star 2 = 11/25 \neq 7/25 = 1 \star (0 \star 2)$.

(d) Associative:

$$\begin{aligned}[(a, b) \star (c, d)] \star (e, f) &= (ad + bc, bd) \star (e, f) \\ &= ((ad + bc)f + bde, bdf) \\ &= (adf + bcf + bde, bdf) \\ &= (adf + b(cf + de), bdf) \\ &= (a, b) \star (cf + de, df) \\ &= (a, b) \star [(c, d) \star (e, f)]\end{aligned}$$

(e) Not associative: $(1 \star 2) \star 3 = 1/6 \neq 3/2 = 1 \star (2 \star 3)$. ■

Exercise 1.1.2

Decide which of the binary operations in the preceding exercise are commutative.

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc,\ bd)$

(e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$

Solution.

(a) Not commutative: $1 - 0 \neq 0 - 1$.

(b) Commutative: $a \star b = a + b + ab = b + a + ba = b \star a$.

(c) Commutative: $a \star b = (a + b)/5 = (b + a)/5 = b \star a$.

(d) Commutative: $(a, b) \star (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) \star (a, b)$.

(e) Not commutative: $1/2 \neq 2/1$. ■

Exercise 1.1.3

Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Solution. Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\begin{aligned}(\bar{a} + \bar{b}) + \bar{c} &= \overline{a + b} + \bar{c} \\ &= \overline{(a + b) + c} \\ &= \overline{a + (b + c)} \\ &= \bar{a} + \overline{b + c} \\ &= \bar{a} + (\bar{b} + \bar{c})\end{aligned}$$

■

Exercise 1.1.4

Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Solution. Since $\cdot$ is associative over $\mathbb{Z}$, we may use the same argument as in the previous exercise. ■

Exercise 1.1.5

Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Solution. Note that $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$, but there is no $\bar{a}$ such that $\bar{0} \cdot \bar{a} = \bar{1}$. Hence, $\mathbb{Z}/n\mathbb{Z}$ does not have an identity under multiplication, so it is not a group. ■

Exercise 1.1.6

Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even

(c) the set of rational numbers of absolute value < 1

(d) the set of rational numbers of absolute value ≥ 1 together with 0

(e) the set of rational numbers with denominators equal to 1 or 2

(f) the set of rational numbers with denominators equal to 1, 2, or 3

Solution. Let S denote the set in each part.

(a) Clearly, $0 \in S$. Moreover, for any $s \in S$, then $-s \in S$. Since $\mathbb{Q}$ is associative under addition, then so is S. To show closure, let $a/b, c/d \in S$, where b and d are odd, and $(a, b) = (c, d) = 1$. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

where bd is odd. Note that a number is even when at least one of its factors is even. It follows that any common factor of $ad + bc$ and bd must also be odd, hence the fraction in its lowest terms will still have an odd denominator. Thus, S is closed under addition and is a group.

(b) S is not a group, since $1/2 \in S$, but $1/2 + 1/2 = 2/2 = 1/1 \notin S$.

(c) Same as previous.

(d) S is not a group, since $3/2, 1 \in S$, but $3/2 - 1 = 1/2 \notin S$.

(e) Since $0 = 0/1$, then $0 \in S$. Moreover, for any $s \in S$, then $-s \in S$. Since $\mathbb{Q}$ is associative under addition, then so is S. To show closure, we first note that $s \in S$ has the form

$$s = a \quad \text{or} \quad s = a + \frac{1}{2}$$

for some $a \in \mathbb{Z}$. If any two $s_1, s_2 \in S$ have the same form, then $s_1 + s_2 \in S$. Otherwise, suppose without loss of generality that s_1 has the first form and s_2 has the second form. Then

$$s_1 + s_2 = a + \left(b + \frac{1}{2}\right) = (a + b) + \frac{1}{2} \in S$$

so that S is closed under addition and is a group.

(f) S is not a group, since $1/2, 1/3 \in S$, but $1/2 + 1/3 = 5/6 \notin S$. ■

Exercise 1.1.7

Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x+y$ (i.e., $x \star y = x+y-[x+y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well defined binary operation on G and that G is an abelian group under $\star$ (called the *real numbers mod 1*).

Solution. Suppose $x, y \in G$. To show closure, there are two cases:

- Suppose $0 \leq x + y < 1$. Then $[x + y] = 0$ so that $x \star y = x + y - 0 = x + y \in G$.
- Suppose $1 \leq x + y < 2$. Then $[x + y] = 1$ so that $x \star y = x + y - 1 \in G$.

To show associativity, let $x, y, z \in G$. Recall that $[a \pm b] = [a] \pm b$ for all $a \in \mathbb{R}$ and $b \in \mathbb{Z}$. Then

$$\begin{aligned}
(x \star y) \star z &= (x + y - [x + y]) \star z \\
&= (x + y - [x + y]) + z - [(x + y - [x + y]) + z] \\
&= x + y + z - [x + y] - [x + y + z - [x + y]] \\
&= x + y + z - [x + y] - [x + y + z] + [x + y] \\
&= x + y + z - [x + y + z] \\
&= x + y + z - [y + z] - [x + y + z] + [y + z] \\
&= x + y + z - [y + z] - [x + y + z - [y + z]] \\
&= x + (y + z - [y + z]) - [x + (y + z - [y + z])] \\
&= x \star (y + z - [y + z]) \\
&= x \star (y \star z)
\end{aligned}$$

Moreover, $0 \in G$ is the identity since for any $x \in G$, then $x \star 0 = x + 0 - [x + 0] = x$. Additionally, for any $x \in G$, its inverse is $1 - x$ if $x \neq 0$ and 0 if $x = 0$, since

$$x \star (1 - x) = x + (1 - x) - [x + (1 - x)] = 1 - 1 = 0$$

Finally, $\star$ is commutative since $x \star y = x + y - [x + y] = y + x - [y + x] = y \star x$. Hence, G is abelian under $\star$. ■

Exercise 1.1.8

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).

(b) Prove that G is not a group under addition.

Solution.

(a) Since $1^1 = 1$, then $1 \in G$. Moreover, for any $z \in G$ such that $z^n = 1$, then its inverse z^{-1} satisfies $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$ so that $z^{-1} \in G$. Since multiplication in $\mathbb{C}$ is associative, then so is G. Finally, let $z, w \in G$ such that $z^n = 1$ and $w^m = 1$ for some $n, m \in \mathbb{Z}^+$. Then

$$(zw)^{nm} = z^{nm} w^{nm} = (z^n)^m (w^m)^n = 1 \cdot 1 = 1$$

so that $zw \in G$. Hence, G is a group under multiplication.

(b) Not a group, since $1 \in G$ and $-1 \in G$, but $1 + (-1) = 0 \notin G$ since $0^n \neq 1$ for all $n \in \mathbb{Z}^+$. ■

(∗) Exercise 1.1.9

Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses.]

Solution.

(a) Since $0 + 0\sqrt{2} \in G$, then G has an identity. Moreover, for any $a + b\sqrt{2} \in G$, its inverse is $-a - b\sqrt{2} \in G$. Since addition in $\mathbb{R}$ is associative, then so is G. Finally, let $a + b\sqrt{2}, c + d\sqrt{2} \in G$ for some $a, b, c, d \in \mathbb{Q}$. Then

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$$

since $a + c, b + d \in \mathbb{Q}$. Hence, G is a group under addition.

(b) Since $1 + 0\sqrt{2} \in G$, then G has an identity. Moreover, for any nonzero $a + b\sqrt{2} \in G$, its inverse is

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

where $a^2 - 2b^2 \neq 0$ since $a + b\sqrt{2} \neq 0$. Since multiplication in $\mathbb{R}$ is associative, then so is G. Finally, let $a + b\sqrt{2}, c + d\sqrt{2} \in G$ for some nonzero $a, b, c, d \in \mathbb{Q}$. Then

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in G$$

since $ac + 2bd, ad + bc \in \mathbb{Q}$. Hence, the nonzero elements of G are a group under multiplication. ■

Exercise 1.1.10

Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

Solution. Let G be a finite group, and let $G = \{g_1, g_2, \ldots, g_n\}$ for some $n \in \mathbb{Z}^+$ with $g_1 = 1$. Note that $g_i g_j$ is the (i, j)-th entry of the group table, and a symmetric matrix implies that the (i, j)-th entry is equal to the (j, i)-th entry for all $1 \leq i, j \leq n$.

We have that G is abelian if and only if $g_i g_j = g_j g_i$ for all $1 \leq i, j \leq n$, which holds if and only if the (i, j)-th entry is equal to the (j, i)-th entry for all $1 \leq i, j \leq n$. This is true if and only if the group table is a symmetric matrix. ■

Exercise 1.1.11

Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Solution. For each $\bar{x} \in \mathbb{Z}/12\mathbb{Z}$, add it to itself until we arrive at $\bar{0}$. $|\bar{0}| = 1$, and $\bar{1} = 12$ since $12 \cdot \bar{1} = \overline{12} = \bar{0}$. In particular, we have:

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\lvert\bar{x}\rvert$	1	12	6	4	3	12	2	12	3	4	6	12

■

Exercise 1.1.12

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\bar{1}, \overline{-1}, \bar{5}, \bar{7}, \overline{-7}, \overline{13}$.

Solution.

$\bar{x}$	$\bar{1}$	$\overline{-1}$	$\bar{5}$	$\bar{7}$	$\overline{-7}$	$\overline{13}$
$\lvert\bar{x}\rvert$	1	2	2	2	2	1

■

Exercise 1.1.13

Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Solution.

$\overline{x}$	$\overline{1}$	$\overline{2}$	$\overline{6}$	$\overline{9}$	$\overline{10}$	$\overline{12}$	$\overline{-1}$	$\overline{-10}$	$\overline{-18}$
$\lvert\overline{x}\rvert$	36	18	6	4	18	3	36	18	2

■

Exercise 1.1.14

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Solution.

$\overline{x}$	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{13}$	$\overline{-13}$	$\overline{17}$
$\lvert\overline{x}\rvert$	1	2	6	3	6	2

■

Exercise 1.1.15

Prove that $(a_1a_2\dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

Solution. We proceed by induction. For $n = 1$, the result is clear. Suppose it is true for some $n \in \mathbb{Z}^+$. Then for $n+1$, we have

$$\begin{aligned}(a_1a_2\dots a_na_{n+1})^{-1} &= ((a_1a_2\dots a_n)a_{n+1})^{-1}\\ &= a_{n+1}^{-1}(a_1a_2\dots a_n)^{-1}\\ &= a_{n+1}^{-1}(a_n^{-1}a_{n-1}^{-1}\dots a_1^{-1})\\ &= a_{n+1}^{-1}a_n^{-1}a_{n-1}^{-1}\dots a_1^{-1}\end{aligned}$$

The result follows by induction. ■

Exercise 1.1.16

Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Solution.

- ($\Rightarrow$) Suppose $x^2 = 1$. Then $|x| \leq 2$. Since $|x| \in \mathbb{Z}^+$, then $|x|$ is either 1 or 2.
- ($\Leftarrow$) Suppose $|x|$ is either 1 or 2. If $|x| = 1$, then $x = 1$ so that $x^2 = 1$. If $|x| = 2$, then $x^2 = 1$. ■

Exercise 1.1.17

Let x be an element of G. Prove that if $|x| = n$ for some positive integer n, then $x^{-1} = x^{n-1}$.

Solution. Note that $x^n = x^{n-1}x = 1$. Then $x^{n-1} = x^{-1}$. ■

Exercise 1.1.18

Let x, y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Solution. We prove $xy = yx$ if and only if $y^{-1}xy = x$ first.
- ($\Rightarrow$) Suppose $xy = yx$. Then multiplying both sides on the left by y^{-1} gives $y^{-1}xy = y^{-1}yx = 1x = x$.
- ($\Leftarrow$) Suppose $y^{-1}xy = x$. Then multiplying both sides on the left by y gives $xy = yy^{-1}xy = yx$.

Next, we prove $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.
- ($\Rightarrow$) Suppose $y^{-1}xy = x$. Then multiplying both sides on the left by x^{-1} gives $x^{-1}y^{-1}xy = x^{-1}x = 1$.
- ($\Leftarrow$) Suppose $x^{-1}y^{-1}xy = 1$. Then multiplying both sides on the left by x gives $y^{-1}xy = xx^{-1} = 1x = x$.

The result follows. ■

(∗) **Exercise 1.1.19**

Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.

(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.

(b) Prove that $(x^a)^{-1} = x^{-a}$.

(c) Establish part (a) for arbitrary integers a and b (positive, negative, or zero).

Solution.

(a) Since x^a has a amount of x and x^b has b amount of x, then $x^a x^b$ has $a + b$ amount of x, or x^{a+b}. Similarly, $(x^a)^b$ has ab amount of x, or x^{ab}.

(b) Recall that $x^{-a} = (x^{-1})^a$. We proceed by induction. For $a = 1$, we have $x^{-1} = (x^{-1})^1$. Suppose $(x^a)^{-1} = (x^{-1})^a$ for some $a \in \mathbb{Z}^+$. Then for $a + 1$, we have

$$(x^{a+1})^{-1} = (x^a x)^{-1} = x^{-1}(x^a)^{-1} = x^{-1}(x^{-1})^a = (x^{-1})^{a+1}$$

hence the result follows by induction.

(c) There are three cases to consider:
- If both $a, b \in \mathbb{Z}^+$, then we proceed as in part (a).
- If one of a or b is 0, we may assume without loss of generality that $b = 0$. Then $x^{a+0} = x^a x^0 = x^a$. Moreover, we have $(x^a)^0 = 1$ by definition, so $x^{a\cdot 0} = x^0 = 1$.
- If one of a or b is negative, we may assume without loss of generality that $b < 0$, hence $-b \in \mathbb{Z}^+$. For the first part of (a), we have
$$x^a = x^{a+b-b} = x^{a+b}x^{-b} = x^{a+b}(x^b)^{-1}$$
so that $x^a x^b = x^{a+b}$. For the second part of (a), we have
$$(x^a)^b = ((x^a)^{-b})^{-1} = (x^{-ab})^{-1} = x^{ab}.$$
Hence, the result follows. ■

Exercise 1.1.20

For x an element in G, show that x and x^{-1} have the same order.

Solution. Suppose $|x| = n \in \mathbb{Z}^+$. Then

$$(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$$

so that $|x^{-1}| \leq n$ and has finite order. Similarly, suppose $|x^{-1}| = m \in \mathbb{Z}^+$. Then

$$x^m = ((x^{-1})^m)^{-1} = 1^{-1} = 1$$

so that $|x| \leq m$ and has finite order. Hence, $|x| = |x^{-1}|$. Moreover, the above shows that if either x or x^{-1} has finite order, then so does the other. Hence, they both have finite or infinite order. ■

Exercise 1.1.21

Let G be a finite group and let x be an element of order n. Prove that if n is odd, then $x = (x^2)^k$ for some $k \geq 1$.

Solution. Since n is odd, then $n = 2m - 1$ for some $m \in \mathbb{Z}^+$. Since $|x| = n$, then

$$1 = x^n = x^{2m-1} = (x^2)^m x^{-1}$$

so that $x = (x^2)^m$. ■

(∗) Exercise 1.1.22

If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Solution. We first show that $(g^{-1}xg)^n = g^{-1}x^n g$ for all $n \in \mathbb{Z}^+$ by induction. For $n = 1$, the result is clear. Suppose it holds for some $n \in \mathbb{Z}^+$. Then for $n + 1$, we have

$$(g^{-1}xg)^{n+1} = (g^{-1}xg)^n(g^{-1}xg) = (g^{-1}x^n g)(g^{-1}xg) = g^{-1}x^{n+1}g$$

so the result follows by induction.

Let $|x| = n \in \mathbb{Z}^+$. Then

$$(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}1g = 1$$

so that $|g^{-1}xg| \leq n$. Similarly, let $|g^{-1}xg| = m \in \mathbb{Z}^+$. Then

$$x^m = (gg^{-1})x^m(gg^{-1}) = g(g^{-1}xg)^m g^{-1} = g1g^{-1} = 1$$

so that $|x| \leq m$. Hence, $|x| = |g^{-1}xg|$. We may use similar reasoning to show that if either x or $g^{-1}xg$ has finite order, then so does the other. Hence, they both have finite or infinite order.

To deduce that $|ab| = |ba|$ for all $a, b \in G$, let $x = ba$ and $g = b$. Using the fact that $|x| = |g^{-1}xg|$, we have

$$|ba| = |b^{-1}(ba)b| = |ab|$$

Hence, the result follows. ■

Exercise 1.1.23

Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.

Solution. Let $|x^s| = r \in \mathbb{Z}^+$. Then

$$1 = (x^s)^r = x^{sr}$$

so that $r \leq t$. Moreover,

$$(x^s)^r = x^{sr} = 1$$

implies that $|x| = st \leq sr$, hence $t \leq r$. Thus, $|x^s| = r = t$. ■

Exercise 1.1.24

If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

Solution. We proceed by induction. For $n = 1$, the result is clear. Suppose it holds for some $n \in \mathbb{Z}^+$. Then for $n + 1$, we have

$$(ab)^{n+1} = (ab)^n(ab) = (a^n b^n)(ab) = a^{n+1}b^{n+1}$$

so the result follows by induction for all positive n. For $n = 0$, we have $(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0$. Finally, for negative n, we have

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

since a and b commute. Hence, the result holds for all $n \in \mathbb{Z}$. ■

Exercise 1.1.25

Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian.

Solution. Since $x^2 = 1$, then $x = x^{-1}$ for all $x \in G$. Let $a, b \in G$. Then

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

so that G is abelian. ■

(∗) Exercise 1.1.26

Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all $h, k \in H$, $hk,\ h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

Solution. Let H be a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses. Since H is nonempty, there exists some $h \in H$. Since H is closed under inverses, then $h^{-1} \in H$. Since H is closed under the binary operation on G, then $hh^{-1} = 1 \in H$ so that H has an identity. Moreover, for any $k \in H$, its inverse $k^{-1} \in H$ since H is closed under inverses. Since $\star$ is associative on G, then it is also associative on H. Hence, H is a group under the operation $\star$ restricted to H. ■

(∗) Exercise 1.1.27

Prove that if x is an element of the group G, then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup. (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

Solution. Let $H = \{x^n \mid n \in \mathbb{Z}\}$. Since $x^0 = 1 \in H$, then H is nonempty. Moreover, for any $x^a, x^b \in H$ where $a, b \in \mathbb{Z}$, we have

$$x^a x^b = x^{a+b} \in H$$

by Exercise 1.1.19 so that H is closed under the binary operation on G. Additionally, we have

$$(x^a)^{-1} = x^{-a} \in H$$

so that H is closed under inverses. Hence, by the preceding exercise, H is a subgroup of G. ■

Exercise 1.1.28

Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:

(a) Prove that the associative law holds:

$$\text{for all } (a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B, [(a_1, b_1)(a_2, b_2)](a_3, b_3) = (a_1, b_1)[(a_2, b_2)(a_3, b_3)]$$

(a) Prove that $(1, 1)$ is the identity of $A \times B$, and

(b) Prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Solution.

(a) Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$. Then

$$\begin{aligned}[(a_1, b_1)(a_2, b_2)](a_3, b_3) &= (a_1a_2, b_1b_2)(a_3, b_3)\\ &= ((a_1a_2)a_3, (b_1b_2)b_3)\\ &= (a_1(a_2a_3), b_1(b_2b_3))\\ &= (a_1, b_1)(a_2a_3, b_2b_3)\\ &= (a_1, b_1)[(a_2, b_2)(a_3, b_3)]\end{aligned}$$

(b) For $a \in A, b \in B$, we have $(a, b)(1, 1) = (a \star 1, b \diamond 1) = a, b)$.

(c) We have $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1)$. ■

Exercise 1.1.29

Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Solution. Let $a, a' \in A$ and $b, b' \in B$. Suppose $A \times B$ is abelian. Then

$$(aa', bb') = (a, b)(a', b') = (a', b')(a, b) = (a'a, b'b)$$

so that A and B are abelian. If A and B are both abelian, then

$$(a, b)(a', b) = (aa', bb') = (a'a, b'b) = (a', b')(a, b)$$

hence $A \times B$ is abelian. ■

Exercise 1.1.30

Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Solution. Let $a \in A$ and $b \in B$. Then

$$(a, 1)(1, b) = (a \cdot 1, 1 \cdot b) = (a, b) = (1 \cdot a, b \cdot 1) = (1, b)(a, 1)$$

so that $(a, 1)$ and $(1, b)$ commute. Let $\ell = \text{lcm}(|a|, |b|)$. Then

$$(a, b)^\ell = (a^\ell, b^\ell) = (1, 1)$$

so that $|(a, b)| \leq \ell$. Moreover, if $(a, b)^k = (1, 1)$ for some $k \in \mathbb{Z}^+$, then $a^k = 1$ and $b^k = 1$ so that both $|a|$ and $|b|$ divide k. Hence, ℓ divides k so that $\ell \leq k$. Thus, $|(a, b)| = \ell$. ■

Exercise 1.1.31

Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

Solution. Let $g \in G$. If $g \neq g^{-1}$, then $g \in t(G)$. Moreover, $g^{-1} \neq (g^{-1})^{-1} = g$ so that $g^{-1} \in t(G)$ as well. It follows that the elements of $t(G)$ may be paired off as (g, g^{-1}) where $g \neq g^{-1}$, hence $t(G)$ has an even number of elements. Since G has even order, then $G - t(G)$ also has an even number of elements. Note that $1 \notin t(G)$ since $1 = 1^{-1}$. Thus, $G - t(G)$ contains at least one nonidentity element x. Since $x \notin t(G)$, then $x = x^{-1}$ so that $x^2 = 1$ and $|x| = 2$. ■

Exercise 1.1.32

If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Solution. Let $a, b \in \mathbb{Z}^+$ be such that $0 \leq a < b < n$. Suppose $x^a = x^b$. Then

$$1 = x^b x^{-a} = x^{b-a}$$

so that $|x| \leq b - a < n$, which is a contradiction. Hence, the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Since these elements are all in G, then $|x| = n \leq |G|$. ■

Exercise 1.1.33

Let x be an element of finite order n in G.

(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.

(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

Solution.

(a) Assume, by way of contradiction, that $x^i = x^{-i}$ for some i where $1 \leq i < n$. Then

$$1 = x^i x^i = x^{2i}$$

Note that $2i$ is even, so $2i \neq n$ since n is odd. Noting that $2i < n$, then the only possibility for $x^{2i} = 1$ is if $2i = 0$, which is impossible since $i \geq 1$. This is a contradiction, hence $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.

(b)
- ($\Rightarrow$) Suppose $x^i = x^{-i}$ for some i where $1 \leq i < n$. Then

$$1 = x^i x^i = x^{2i}$$

Since $x^n = x^{2k} = 1$, then the only i such that $1 \leq i < 2k$ and $x^{2i} = 1$ is $i = k$.
- ($\Leftarrow$) Suppose $i = k$. Then

$$x^i = x^k = x^{2k-k} = x^{n-k} = x^{-k} = x^{-i}$$

■

Exercise 1.1.34

If x is an element of infinite order in G, prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.

Solution. Assume, by way of contradiction, that $x^a = x^b$ for some $a, b \in \mathbb{Z}$ where $a < b$. Then

$$1 = x^b x^{-a} = x^{b-a}$$

so that $|x| \leq b - a$, contradicting that x has infinite order. Hence, the elements $x^n, n \in \mathbb{Z}$ are all distinct. ■

Exercise 1.1.35

If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 1.1.27) of G generated by x).

Solution. Let $|x| = n \in \mathbb{Z}^+$ and let $m \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers q and r such that

$$m = qn + r$$

where $0 \leq r < n$. Then

$$x^m = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = x^r$$

so that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$. ■

(∗) Exercise 1.1.36

Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 1.1.32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Solution. Since G has even order, it has an element of order 2 by Exercise 1.1.31. Without loss of generality, let a be that element so that $a^2 = 1$. Since there are no elements of order 4, then the remaining elements b and c may have order 2 or 3.

We now observe that $ab \neq 1$ since that would imply that $b = a^{-1} = a$ contradicting that a and b are distinct elements. Similarly, $ab \neq a$ since that would imply that $b = 1$, and $ab \neq b$ since that would imply that $a = 1$. Thus, $ab = ba = c$. Similarly, $ac \neq 1, a, c$ so that $ac = ca = b$, hence $b^2 = (ca)(ac) = c^2$.

We now consider the possible orders of b and c. If $b^2 \neq 1$, then $|b| = 3$. But then $b^3 = bb^2 = bc = a$, contradicting that $|b| = 3$. Thus, $b^2 = 1$. Similarly, $c^2 = 1$. The group table for G is therefore as follows:

$\star$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

from which we may deduce that G is abelian. ■

1.2 Dihedral Groups

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.

Exercise 1.2.1

Compute the order of each of the elements in the following groups:

(a) D_6 (b) D_8 (c) D_{10}

Solution. For any reflection $sr^k \in D_{2n}$, it is clear that $sr^k \neq 1$. Moreover, $(sr^k)^2 = s(r^k s)r^k = s(sr^{-k})r^k = r^{-k}r^k = 1$ so that every reflection has order 2. We now compute the orders of the rotations in each group.

(a) $D_6 = \{1, r, r^2, s, sr, sr^2\}$. Then $|1| = 1$ and $|r| = |r^2| = 2$.

(b) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Then $|1| = 1$, $|r^2| = 2$ and $|r| = |r^3| = 4$.

(c) $D_{10} = \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$. Then $|1| = 1$ and $|r| = |r^2| = |r^3| = |r^4| = 5$. ■

Exercise 1.2.2

Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Solution. If x is not a power of r, then x is a reflection, i.e., $x = sr^k$ for some $0 \leq k < n$. Then

$$rx = r(sr^k) = (rs)r^k = (sr^{-1})r^k = s(r^{-1}r^k) = sr^{k-1} = (sr^k)r^{-1} = xr^{-1}$$

■

Exercise 1.2.3

Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2. [cf. Exercise 1.1.33.]

Solution. Every element of D_{2n} which is not a power of r is a reflection. For this solution, see Exercise 1.2.1.

To see that s and sr generate D_{2n}, note that for any rotation $r^k \in D_{2n}$ and any reflection $sr^k \in D_{2n}$ where $0 \leq k < n$, then

$$r^k = (s(sr))^k \quad \text{and} \quad sr^k = s(s(sr))^k.$$

Hence, D_{2n} is generated by s and sr. ■

Exercise 1.2.4

If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 1.1.33.]

Solution. Since $k < n$, then $r^k \neq 1$. Moreover, $(r^k)^2 = r^{2k} = r^n = 1$ so that $|r^k| = 2$. To see that r^k commutes with all elements of D_{2n}, note that every element of D_{2n} is of the form $s^i r^j$ where $i \in \{0, 1\}$ and $0 \leq j < n$. Then

$$r^k(s^i r^j) = s^i r^{-k} r^j = s^i r^k r^j = (s^i r^j) r^k.$$

Now suppose $w \in D_{2n}$ commutes with all elements of D_{2n}. If w is a rotation, then $w = r^m$ for some $0 \leq m < n$. Since w commutes with s, then $sw = ws$. But $sw = w^{-1}s$ as well, so that $w = w^{-1}$. By Exercise 1.1.33, then $m = k$ since n is even.

Suppose w is a reflection, so that $w = sr^m$ for some $0 \leq m < n$. Since w commutes with r, then $rw = wr$. But $rw = wr^{-1}$ as well, so that $r = r^{-1}$. Then $r^2 = 1$, contradicting that $|r| = n \geq 4$. Hence, w must be a rotation, and we have shown that $w = r^k$. ■

Exercise 1.2.5

If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 1.1.33]

Solution. We use a similar argument as the previous exercise. If there was such a nonidentity $w \in D_{2n}$, we may use the odd case in Exercise 1.1.33 if we assume w is a rotation. We would get $r^k = r^{-k}$, which is never true since n is odd. If w is a reflection, then we would have the same contradiction as before. Hence, the identity is the only element of D_{2n} which commutes with all elements of D_{2n}. ■

Exercise 1.2.6

Let x and y be elements of order 2 in any group G. Prove that if $t = xy$, then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, y satisfy the same relations in G as s, r do in D_{2n}).

Solution. Since $|x| = |y| = 2$, then $x = x^{-1}$ and $y = y^{-1}$. Then

$$tx = (xy)x = x(yx) = x(xy)^{-1} = xt^{-1}$$

■

Exercise 1.2.7

Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators a and b of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and conversely, the relations for a and b follow from those for r and s.]

Solution. Suppose $a^2 = b^2 = (ab)^n = 1$. The natural choices for r and s are $r = ab$ and $s = a$. Then

$$r^n = (ab)^n = 1, \quad s^2 = a^2 = 1, \quad rs = (ab)a = a(ba) = a(b^{-1}a^{-1}) = a(ab)^{-1} = sr^{-1}$$

Conversely, suppose $r^n = s^2 = 1$ and $rs = sr^{-1}$. The natural choices for a and b are $a = s$ and $b = sr$. Then

$$a^2 = s^2 = 1, \quad b^2 = (sr)(sr) = s(rs)r = s(sr^{-1})r = (ss)r^{-1}r = 1, \quad (ab)^n = (s(sr))^n = r^n = 1$$

■

Exercise 1.2.8

Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 1.1.27).

Solution. Let $H = \langle r\rangle$ be the cyclic subgroup of D_{2n} generated by r. Since $|r| = n$, then by Exercise 1.1.35, the distinct elements of H are $1, r, r^2, \ldots, r^{n-1}$. It follows that $|H| = n$. ■

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

Exercise 1.2.9

Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Solution. Label the vertices of a tetrahedron 1 through 4 so that vertex 1 has 4 choices. Then vertex 2 has 3 remaining choices, and vertex 3 and 4 are determined after. It follows that $4(3) = 12$ symmetries. ■

Exercise 1.2.10

Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Solution. 8 choices for vertex 1 and 3 adjacent vertices for vertex 2; $8(3) = 24$ symmetries. ■

Exercise 1.2.11

Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.

Solution. 6 choices for vertex 1 and 4 adjacent vertices for vertex 2; $6(4) = 24$ symmetries. ■

Exercise 1.2.12

Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Solution. 20 choices for vertex 1 and 3 adjacent vertices for vertex 2; $20(3) = 60$ symmetries. ■

Exercise 1.2.13

Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.

Solution. 12 choices for vertex 1 and 5 adjacent vertices for vertex 2; $12(5) = 60$ symmetries. ■

Exercise 1.2.14

Find a set of generators for $\mathbb{Z}$.

Solution. Any integer is of the form $n1$, so $\mathbb{Z} = \langle 1 \rangle$. ■

Exercise 1.2.15

Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

Solution. Each element of $\mathbb{Z}/n\mathbb{Z}$ is of the form $k\bar{1}$ for $0 \leq k < n$. Then $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \mid n\bar{1} = \bar{0} \rangle$. ■

Exercise 1.2.16

Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). (Show that the last relation is the same as $x_1 y_1 = y_1 x_1^{-1}$.)

Solution. Let D_4 have the usual presentation $\langle r, s \mid r^2 = s^2 = 1, rs = sr^{-1} \rangle$. Since $r^2 = 1$, then $r = r^{-1}$, hence $rs = sr^{-1}$ is equivalent to $rs = sr$. Let $x_1 = r$ and $y_1 = s$. Then $x_1^2 = r^2 = 1$ and $y_1^2 = s^2 = 1$. Suppose $rs = sr$. Then

$$1 = rssr = (rs)^2 = x_1 y_1 x_1 y_1 = (x_1 y_1)^2$$

Conversely, suppose $(x_1 y_1)^2 = 1$. Then

$$rs = x_1 y_1 = (x_1 y_1)^{-1} = y_1^{-1} x_1^{-1} = y_1 x_1 = sr$$

Thus, the two presentations are equivalent. ■

Exercise 1.2.17

Let X_{2n} be the group whose presentation is displayed in (1.2).

$$X_{2n} = \langle x, y \mid x^n = y^2 = 1, xy = yx^2 \rangle$$

(a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.

(b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [use the facts that $x^n = 1$ and $x^3 = 1$.]

Solution.

(a) If $n = 3k$, then

$$X_{2n} = X_{6k} = \langle x, y \mid x^{3k} = y^2 = 1, xy = yx^2 \rangle$$

As shown in the text,

$$x = xy^2 = yx^2y = yxyx^2 = y^2x^4 = x^4$$

so that $x^3 = 1$. To show that X_{6k} has the same generators and relations as D_6, assume the relations of X_{6k} hold. Set $r = x$ and $s = y$. We then have $r^3 = x^3 = 1$, $s^2 = y^2 = 1$, and

$$rs = xy = yx^2 = sr^2 = sr^{-1}$$

Now suppose the relations of D_6 hold. Then

$$x^n = r^{3k} = (r^3)^k = 1^k = 1, \quad y^2 = s^2 = 1$$

and

$$xy = rs = sr^{-1} = sr^2 = yx^2$$

Thus, the two presentations are equivalent, and $|X_{6k}| = |D_6| = 6$.

(b) Since $(3, n) = 1$, there exist integers a and b such that $3a + nb = 1$. From the relations of X_{2n}, we have $x^3 = 1$ and $x^n = 1$. Then

$$x = x^{3a+nb} = (x^3)^a(x^n)^b = 1^a1^b = 1$$

so that $X_{2n} = 1, y$ where $y^2 = 1$. It follows that $|X_{2n}| = 2$. ■

Exercise 1.2.18

Let Y be the group whose presentation is displayed in (1.3).

(a) Show that $v^2 = v^{-1}$. [Use the relation $v^3 = 1$.]

(b) Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left-hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right-hand side. Then use part (a).]

(c) Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]

(d) Show that $uv = 1$. [Use part (c) and the last relation.]

(e) Show that $u = 1$. Deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $u^4v^3 = 1$.]

Solution.

(a) $v^3 = 1 \implies v^2 = v^{-1}$.

(b) From $uv = v^2u^2$, we have $vuv = u^2$ so that $vu = u^2v^{-1} = u^2v^2$. It follows that $v^2u^3v = (v^2u^2)(uv) = (uv)(uv) = u(vu)v = u(u^2v^2)v = u^3$.

(c) It follows that $u^9 = (u^4)^2u = u$. Then $uv = (u^3)^3v = v(u^3)^3 = vu$.

(d) $uv = v^2u^2 = u^2v^2$. Then $1 = uv$.

(e) $u^4v^3 = u(uv)^3 = u1^3 = 1$. Then $1v = 1$, and $u = v = 1$, so $Y = 1$. ■

1.3 Symmetric Groups

Exercise 1.3.1

Let σ be the permutation

$$1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 5, \quad 4 \mapsto 2, \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5, \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 4, \quad 5 \mapsto 1$$

Find the cycle decompositions of each of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

Solution.

$$\sigma = (1\ 3\ 5)(2\ 4) \qquad \tau = (1\ 5)(2\ 3)$$
$$\sigma^2 = (1\ 5\ 3) \qquad \sigma\tau = (2\ 5\ 3\ 4)$$
$$\tau\sigma = (1\ 2\ 4\ 3) \qquad \tau^2\sigma = (1\ 3\ 5)(2\ 4)$$ ■

Exercise 1.3.2

Let σ be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 7$	$7 \mapsto 12$	$8 \mapsto 9$	$9 \mapsto 3$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13$

Find the cycle decompositions of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

Solution.

$$\sigma = (1\ 13\ 5\ 1)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) \qquad \tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$$
$$\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13) \qquad \sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(8\ 10\ 14)$$
$$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14) \qquad \tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$$ ■

Exercise 1.3.3

For each of the permutations whose cycle decompositions were computed in the preceding two exercises, compute its order.

Solution. Note that the order of a cycle decomposition is the lcm of the orders of each of the cycles, and that the order of an m-cycle is m. Then the orders are the following (the first number will be for Exercise 1, and the second for Exercise 2):

$$|\sigma| = 6, 12 \qquad |\tau| = 2, 30$$
$$|\sigma^2| = 3, 6 \qquad |\sigma\tau| = 4, 6$$
$$|\tau\sigma| = 4, 6 \qquad |\tau^2\sigma| = 6, 13$$ ■

Exercise 1.3.4

Compute the order of each of the elements in the following groups:

(a) S_3

(b) S_4

Solution.

(a)

Permutation	Order
1	1
(12)	2
(13)	2
(23)	2
(123)	3
(132)	3

(b)

Permutation	Order	Permutation	Order	Permutation	Order	Permutation	Order
1	1	(34)	2	(143)	3	(1342)	4
(12)	2	(123)	3	(234)	3	(1423)	4
(13)	2	(124)	3	(243)	3	(1432)	4
(14)	2	(132)	3	(1234)	4	(12)(34)	2
(23)	2	(134)	3	(1243)	4	(13)(24)	2
(24)	2	(142)	3	(1324)	4	(14)(23)	2

■

Exercise 1.3.5

Find the order of $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.

Solution. There are cycles of lengths 5, 2, 3, and 2. Then the order is $\operatorname{lcm}(5,2,3,2) = 30$. ■

Exercise 1.3.6

Write out the cycle decomposition of each element of order 4 in S_4.

Solution. See Exercise 1.3.4. ■

Exercise 1.3.7

Write out the cycle decomposition of each element of order 2 in S_4.

Solution. See Exercise 1.3.4. ■

Exercise 1.3.8

Prove that if $\Omega = \{1, 2, 3, \dots\}$, then S_Ω is an infinite group (do not say $\infty! = \infty$).

Solution. For each $n \in \mathbb{Z}^+$, consider the permutation σ_n defined by

$$\sigma_n = (2n-1\ 2n)$$

Note that $\sigma_n \in S_\Omega$. Moreover, for $m, n \in \mathbb{Z}^+$ with $m \neq n$, then $\sigma_m \neq \sigma_n$, since σ_m moves $2m-1$ while σ_n does not, hence each σ_n is distinct. Then the set

$$A = \{\sigma_n \mid n \in \mathbb{Z}^+\} \subseteq S_\Omega$$

is infinite, so S_Ω is infinite as well. ■

Exercise 1.3.9

(a) Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12-cycle?
(b) Let τ be the 8-cycle (1 2 3 4 5 6 7 8). For which positive integers i is τ^i also an 8-cycle?
(c) Let ω be the 14-cycle (1 2 3 4 5 6 7 8 9 10 11 12 13 14). For which positive integers i is ω^i also a 14-cycle?

Solution. We will compute the explicit powers for the first problem, notice a pattern with the integers that produce a 12-cycle, and apply that pattern to the other problems.

(a) For each integer between 1 and 11, we compute the cycle:

$$\sigma^1 = \sigma \qquad \sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$$
$$\sigma^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12) \qquad \sigma^4 = (1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(4\ 8\ 12)$$
$$\sigma^5 = \sigma \qquad \sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)$$
$$\sigma^7 = \sigma \qquad \sigma^8 = \sigma^4$$
$$\sigma^9 = \sigma^3 \qquad \sigma^{10} = \sigma^2$$
$$\sigma^{11} = \sigma$$

From direct calculations, it seems that the integers i such that $(12, i) = 1$ produce a 12-cycle, while i such that $(12, i) = k$ produces k $12/k$-cycles. In this particular case, the set of integers that produce a 12-cycle is the set $\{x + 12k \mid x \in \{1, 5, 7, 11\}, k \in \mathbb{Z}\}$.

(b) $\{x + 8k \mid x \in \{1, 3, 5, 7\}, k \in \mathbb{Z}\}$.

(c) $\{x + 14k \mid x \in \{1, 3, 5, 9, 11, 13\}, k \in \mathbb{Z}\}$. ■

Exercise 1.3.10

Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.

Solution. We proceed by induction on the first part. For $i = 1$, then $\sigma^1(a_k) = \sigma(a_k) = a_{k+1}$, where $k + 1$ is replaced by its least residue mod m when $k + 1 > m$. Suppose the statement is true for some i. Then

$$\sigma^{i+1}(a_k) = \sigma(\sigma^i(a_k)) = \sigma(a_{k+i}) = a_{k+i+1},$$

where $k + i + 1$ is replaced by its least residue mod m when $k + i + 1 > m$. By induction, the statement is true for all $i \in \mathbb{Z}^+$.

To determine the order of σ, note that there are m distinct elements $a_1, a_2, \ldots, a_m$ in the cycle. Then for any i where $1 \leq i < m$, then $\sigma^i(a_1) = a_{1+i} \neq a_1$. For σ^m, then $\sigma^m(a_1) = a_{1+m} = a_1$. In particular, this holds for all a_k. Then $\sigma^m = \mathrm{id}$, and $|\sigma| = m$. ■

(∗) Exercise 1.3.11

Let σ be the m-cycle $(1\ 2\ \dots\ m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Solution.

- ($\Rightarrow$) Suppose σ^i is an m-cycle, and assume, by way of contradiction, that $(m,i) = d > 1$. Then there exist $a, b \in \mathbb{Z}^+$ such that $ad = i$ and $bd = m$. Since $|\sigma^i| = m$ because it is an m-cycle, then

$$(\sigma^i)^b = (\sigma^{ad})^b = (\sigma^{bd})^a = (\sigma^m)^a = \mathrm{id}^a = \mathrm{id}\,.$$

  However, $bd = m$ with $d > 1$ implies that $b < m$, so $|\sigma^i| \leq b < m$, contradicting that $|\sigma^i| = m$. It follows that $(m,i) = 1$.
- ($\Leftarrow$) Suppose that $(m,i) = 1$. Denote $x' \equiv x \bmod m$. We claim that the integers

$$(1+i)', (1+2i)', \dots, (1+(m-1)i)'$$

  are all distinct. Suppose $(1+xi)' = (1+yi)'$ for some $0 \leq x, y \leq m-1$ with $x \neq y$. Then $i(x-y) \equiv 0 \bmod m$. Since $(m,i) = 1$, then $m \mid (x-y)$. However, since $1 - m \leq x - y \leq m - 1$, then the only choice for $x - y$ is 0, or that $x = y$. Then we have exactly m distinct integers so that

$$\sigma^i = (1\ (1+i)'\ (1+2i)'\ \dots\ (1+(m-1)i)').$$

  Thus, σ^i is an m-cycle. ■

Exercise 1.3.12

(a) If $\tau = (1\,2)(3\,4)(5\,6)(7\,8)(9\,10)$, determine whether there is an n-cycle ($n \geq 10$) with $\tau = \sigma^k$ for some integer k.

(b) If $\tau = (1\,2)(3\,4\,5)$, determine whether there is an n-cycle ($n \geq 5$) with $\tau = \sigma^k$ for some integer k.

Solution.

(a) We first observe that for any n-cycle σ, then σ^k sends any element a_i to a_{i+k}, where $i + k$ is replaced by its least residue mod n when $i + k > n$. In this specific problem, τ consists of 2-cycles, which means that σ^k must send each element to itself after two applications. Then $2k \equiv 0 \bmod n$, but $k \not\equiv 0 \bmod n$ since $\sigma^k \neq 1$. It follows that $n \mid 2k$ but $n \nmid k$, so it must be that $n = 2k$. We see that σ^k will be a product of k 2-cycles. However, τ is a product of 5 2-cycles, so $k = 5$ and $n = 10$. Thus, there exists an n-cycle σ such that $\sigma^5 = \tau$ when $n = 10$, and $\sigma = (1\,6\,2\,7\,3\,8\,4\,9\,5\,10)$.

(b) We first prove that $(ac, bc) = c(a,b)$. Let $d = (a,b)$ and $d' = (ac,bc)$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. Then $acx + bcy = dc$. Since d' is the smallest integer that is written of the form $acx' + bcy'$ for $x', y' \in \mathbb{Z}$ (if there were any greater, then $d' \neq (ac,bc)$), then $d' \leq dc$. Moreover, $d \mid a$ and $d \mid b$ implies $cd \mid ac$ and $cd \mid bc$. Then $cd \mid d'$, or $cd \leq d'$. Then $dc = d'$, or $c(a,b) = (ac,dc)$.

Suppose there existed some n-cycle σ and k such that $\sigma^k = \tau$. Then $\sigma^{2k}(1) = 1$, or $2k \equiv 0 \bmod n$. Moreover, $\sigma^{3k}(3) = 3$, or that $3k \equiv 0 \bmod n$. Then $n \mid 2k$ and $n \mid 3k$ so that $n \mid (2k, 3k)$. By the above, then $(2k, 3k) = k(2,3) = k$, and $n \mid k$. But then $\sigma^k = (\sigma^n)^q = 1$, contradicting that $\sigma^k = \tau$. ■

Exercise 1.3.13

Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Solution.

- ($\Rightarrow$) Let $\sigma \in S_n$ such that $|\sigma| = 2$. Perform cycle decomposition on σ to obtain a product of disjoint cycles. Let $(a_1\ a_2\ \dots\ a_m)$ be one of the cycles. Since $\sigma \neq 1$, then $\sigma(a_1) = a_2$ and $\sigma^2(a_1) = a_3$. However, $\sigma^2 = 1$, so $\sigma^2(a_1) = a_1$ so that $a_1 = a_3$. Then $m \leq 2$, and the cycle is $(a_1\ a_2)$ so that any cycle in the cycle decomposition of σ is of length 2.
- ($\Leftarrow$) Suppose σ's cycle decomposition is a product of commuting 2-cycles $(a_1\ b_1)(a_2\ b_2)\dots(a_k\ b_k)$. Since $(a_1\ b_1)^2 = 1$, and the 2-cycles commute, then $\sigma^2 = 1$. Moreover, because $\sigma \neq 1$, then $|\sigma| = 2$. ■

Exercise 1.3.14

Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Solution.

- ($\Rightarrow$) Let $\sigma \in S_n$ such that $|\sigma| = p$. Perform cycle decomposition on σ to obtain a product of disjoint cycles. Let $(a_1\ a_2\ \dots\ a_m)$ be one of the cycles. Recall from Exercise 1.3.12 (a) that for any i, $\sigma^i(a_1) = a_{1+i}$, where $1+i$ is replaced by its least residue mod m when $1 + i > m$. Since $\sigma^p = 1$, then $\sigma^p(a_1) = a_1$, so that $a_{1+p} = a_1$. It follows that $m \mid p$. Since p is prime, then $m = 1$ or $m = p$. However, if $m = 1$, then the cycle is trivial and can be removed from the cycle decomposition. Then every cycle in the cycle decomposition of σ has length p.
- ($\Leftarrow$) Suppose σ's cycle decomposition is a product of commuting p-cycles $\pi_1, \pi_2, \dots, \pi_k$. For any $1 \leq t < p$, then $\pi_i^t \neq 1$ for all i. Then $\sigma^t = \pi_1^t\pi_2^t\dots\pi_k^t \neq 1$. However, $\sigma^p = (\pi_1^p)(\pi_2^p)\dots(\pi_k^p) = 1$. Then $|\sigma| = p$.

For a counterexample when p is not prime, consider $\sigma = (1\ 2\ 3)(4\ 5)$ in S_5. Then $|\sigma| = 6$, but the cycle decomposition consists of a 3-cycle and a 2-cycle. ■

Exercise 1.3.15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Solution. Let $\sigma \in S_n$ have the cycle decomposition

$$\sigma = \pi_1\pi_2\dots\pi_k$$

where each π_i is a disjoint cycle of length m_i. Note that since the cycles are disjoint, they commute. Then

$$\sigma^t = \pi_1^t\pi_2^t\dots\pi_k^t$$

Suppose $|\sigma| = m$. Then $\sigma^m = \mathrm{id}$. Let x be in some cycle π_i. Note that for all other π_j where $j \neq i$, then π_j fixes x. Then

$$\sigma^m(x) = \pi_i^m(x) = x$$

so that $\pi_i^m = \mathrm{id}$. It follows that $m_i \mid m$ for all i, so $\mathrm{lcm}(m_1, m_2, \dots, m_k) \mid m$. Morover, let $l = \mathrm{lcm}(m_1, m_2, \dots, m_k)$. Then

$$\sigma^l = \pi_1^l\pi_2^l\dots\pi_k^l = \mathrm{id}$$

so that $m \mid l$. It follows that $m = l$. ■

(∗) Exercise 1.3.16

Show that if $n \geq m$ then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}.$$

[Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle.]

Solution. Note that in an m-cycle, there are m integers to write. The first integer has n choices, the second $n-1$ choices. Continuing on, then the m-th integer has $n-m+1$ choices. However, each choice of m integers has m equivalent representations (such as $(1\ 2\ 3\ 4)$ being equivalent to $(2\ 3\ 4\ 1)$ by shifting each integer to the left one place). Then take the product $n(n-1)(n-2)\dots(n-m+1)$ and divide by m. ■

Exercise 1.3.17

Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.

Solution. The first 2-cycle has $n(n-1)/2$ choices, and the second 2-cycle has $(n-2)(n-3)/2$ choices. Moreover, there are 2 representations for the same set of 2-cycles, so multiply the above quantities and divide by 2 to obtain $n(n-1)(n-2)(n-3)/8$. ■

Exercise 1.3.18

Find all numbers n such that S_5 contains an element of order n.

Solution. S_5 contains elements of order 1 through 5. Moreover, we can have a 2 and 3-cycle together whose lcm is 6. Then $n = 1, 2, 3, 4, 5, 6$. ■

Exercise 1.3.19

Find all numbers n such that S_7 contains a number an element of order n.

Solution. We have n from 1 to 7. We can have 2 and 5-cycles and 3 and 4-cycles. Then $n = 10$ and 12. ■

Exercise 1.3.20

Find a set of generators and relations for S_3.

Solution. Recall that $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Moreover, no element in S_3 has order 6 so that no element generates S_3. It must be that there are at least 2 generators. Put $\alpha = (1\ 2)$ and $\beta = (1\ 3)$. Then $\alpha^2 = \beta^2 = 1$. Then $|\alpha| = |\beta| = 2$, and $\alpha\beta = (1\ 3\ 2), \beta\alpha = (1\ 2\ 3)$, and $\alpha\beta\alpha = (2\ 3)$. Since $\alpha^2 = \beta^2 = 1$ is not enough to determine the order of $\alpha\beta$ (because $\alpha\beta \neq \beta\alpha$), then we must add $(\alpha\beta)^2 = 1$. Then we have the presentation $S_3 = \langle \alpha, \beta \mid \alpha^2 = \beta^2 = (\alpha\beta)^3 = 1 \rangle$. ■

1.4 Matrix Groups

Let F be a field and let $n \in \mathbb{Z}^+$.

Exercise 1.4.1

Prove that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$.

Solution. Recall that $\mathbb{F}_2 = \{0, 1\}$. Moreover, consider

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

where $a, b, c, d \in \mathbb{F}_2$. The determinant is $ad - bc$, which is never 0 whenever a, d are nonzero or when b, c are nonzero, but not both. Then

$$\mathrm{GL}_2(\mathbb{F}_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

■

Exercise 1.4.2

Write out all the elements of $\mathrm{GL}_2(\mathbb{F}_2)$ and compute the order of each element.

Solution. By direct calcuation, we obtain the following:

A	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$\lvert A \rvert$	1	2	2	2	3	3

■

Exercise 1.4.3

Show that $\mathrm{GL}_2(\mathbb{F}_2)$ is non-abelian.

Solution. Consider the matrices of $\mathrm{GL}_2(\mathbb{F}_2)$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Then we have the following products:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Since the two products are not equal, then $\mathrm{GL}_2(\mathbb{F}_2)$ is non-abelian. ■

Exercise 1.4.4

Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Solution. Since n is not prime, it must be composite. Then there exist $a, b \in \mathbb{Z}^+$ such that $1 < a, b < n$ and $n = ab$. Moreover, $(a, n) \neq 1$ since $a \mid n$. Then a has no multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z}$ is not a field. ■

Exercise 1.4.5

Show that $\mathrm{GL}_n(F)$ is a finite group if and only if F has a finite number of elements.

Solution.

- ($\Rightarrow$) We proceed by contrapositive. Suppose F has an infinite number of elements. Consider the set of matrices

$$S = \{\alpha I \mid \alpha \in F^\times\}$$

where I is the identity matrix. It is clear that $S \subseteq \mathrm{GL}_n(F)$ since $\det(\alpha I) = \alpha^n \neq 0$ for all $\alpha \in F^\times$. Moreover, for $\alpha, \beta \in F^\times$ with $\alpha \neq \beta$, then $\alpha I \neq \beta I$, so that S is infinite. It follows that $\mathrm{GL}_n(F)$ is infinite.
- ($\Leftarrow$) Suppose F has a finite number of elements, say q. Then each entry of a matrix in $\mathrm{GL}_n(F)$ has q choices, and there are n^2 entries in total. Then the total number of matrices with entries from F is q^{n^2}. Since $\mathrm{GL}_n(F)$ is a subset of these matrices, then $\mathrm{GL}_n(F)$ is finite. ■

Exercise 1.4.6

If $|F| = q$ is finite prove that $|\mathrm{GL}_n(F)| < q^{n^2}$.

Solution. See the right-to-left implication in the previous exercise. ■

Exercise 1.4.7

Let p be a prime. Prove that the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section). [Subtract the number of 2×2 matrices which are *not* invertible from the total number of 2×2 matrices over $\mathbb{F}_p$. You may use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other.]

Solution. Observe that the total number of 2×2 matrices over $\mathbb{F}_p$ is p^4 since each of the 4 entries has p choices. Next, we count the number of non-invertible matrices. Using the given fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other, we may view a 2×2 matrix as the matrix $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}^T$ where r_1 and r_2 are the first and second rows respectively. Thus, this matrix is not invertible if and only if $r_2 = \alpha r_1$ for some $\alpha \in \mathbb{F}_p$. We have two cases:

- If $r_1 = \mathbf{0}_{1\times 2}$, then r_2 has p^2 choices as it has 2 entries with p choices each.
- If $r_1 \neq \mathbf{0}_{1\times 2}$, then r_1 has $p^2 - 1$ choices (all possible rows except the zero row). For each such r_1, there are p choices for α, so r_2 has p choices. Then there are $(p^2 - 1)p = p^3 - p$ such matrices.

Then the total number of non-invertible matrices is $p^2 + p^3 - p = p^3 + p^2 - p$. Subtracting this from the total number of matrices, we obtain $|\mathrm{GL}_2(\mathbb{F}_p)| = p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p$. ■

Exercise 1.4.8

Show that $\mathrm{GL}_n(F)$ is non-abelian for any $n \geq 2$ and any F.

Solution. Note that for any field F, the field $\mathbb{F}_2 = \{0, 1\}$ is a subset of F. We proceed with the proof over $\mathbb{F}_2$, which will imply the result for any field F.

We proceed by induction on n. For $n = 2$, see Exercise 1.4.3. Suppose that $\mathrm{GL}_n(\mathbb{F}_2)$ is non-abelian for some $n \geq 2$. Let $A, B \in \mathrm{GL}_{n+1}(\mathbb{F}_2)$, and let $A_0, B_0 \in \mathrm{GL}_n(\mathbb{F}_2)$ be the top-left $n \times n$ block matrices of A and B respectively. Then

$$AB = \begin{pmatrix} A_0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} B_0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A_0B_0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} B_0A_0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} B_0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A_0 & 0 \\ 0 & 1 \end{pmatrix} = BA$$

since $A_0B_0 \neq B_0A_0$ by the inductive hypothesis. Thus, $\mathrm{GL}_{n+1}(\mathbb{F}_2)$ is non-abelian. By induction, $\mathrm{GL}_n(\mathbb{F}_2)$ is non-abelian for all $n \geq 2$, which implies that $\mathrm{GL}_n(F)$ is non-abelian for any field F. ■

Exercise 1.4.9

Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.

Solution.

$$\begin{aligned}
\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right]\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} &= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\
&= \begin{pmatrix} (aa'+bc')a''+(ab'+bd')c'' & (aa'+bc')b''+(ab'+bd')d'' \\ (ca'+dc')a''+(cb'+dd')c' & (ca'+dc')b''+(cb'+dd')d'' \end{pmatrix} \\
&= \begin{pmatrix} aa'a''+bca''+ab'c''+bd'c'' & aa'b''+bc'b''+ab'd''+bd'd'' \\ ca'a''+dc'a''+cb'c'+dd'c' & ca'b''+dc'b''+cb'd''+dd'd'' \end{pmatrix} \\
&= \begin{pmatrix} a(a'a''+b'c'')+b(c'a''+d'c'') & a(a'b''+b'd'')+b(c'b''+d'd'') \\ c(a'a''+b'c'')+d(c'a''+d'c'') & c(a'b''+b'd'')+d(c'b''+d'd'') \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a'a''+b'c'' & a'b''+b'd'' \\ c'a''+d'c'' & c'b''+d'd'' \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right]
\end{aligned}$$

■

Exercise 1.4.10

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$$

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

(c) Deduce that G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$ (cf. Exercise 1.1.26).

(d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Solution.

(a)

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

Since $a_i \neq 0$ and $c_i \neq 0$, then $a_1a_2 \neq 0$ and $c_1c_2 \neq 0$ so that G is closed under matrix multiplication.

(b) The determinant is ac. We then have the inverse

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$$

(c) Since G is closed under inverses and matrix multiplication, the result follows.

(d) Let $H = \{A \in G \mid a = c\}$. Then

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \in H$$

and

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \frac{1}{a^2}\begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/a^2 \\ 0 & 1/a \end{pmatrix} \in H$$

Then H is closed under inverses and matrix multiplication, hence it is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. ■

Exercise 1.4.11

Let

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in F \right\}$$

called the *Heisenberg group* over F. Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity of the group $H(\mathbb{R})$ has infinite order.

Solution.

(a) Calculating the product, we have

$$XY = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \in H(F)$$

Moreover, we exhibit matrices A, B such that $AB \neq BA$:

$$AB = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = BA$$

(b) Using augmented matrices, we have

$$\left(\begin{array}{ccc|ccc} 1 & a & b & 1 & 0 & 0 \\ 0 & 1 & c & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right) \Longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & ac-b \\ 0 & 1 & 0 & 0 & 1 & -c \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$$

Calling the right matrix Z, it is easy to see that $XZ = ZX = I_3$, hence $Z = X^{-1}$.

(c) It is clear that each of a, b, c has $|F|$ choices, so that there are $|F|^3$ elements in $H(F)$. Moreover:

$$\begin{aligned} \left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right] \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+d+g & ai+ad+af+b+e+h \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d+g & di+e+h \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \left[\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \right] \end{aligned}$$

(d) Denote a matrix in $H(\mathbb{Z}/2\mathbb{Z})$ as (a,b,c), where $a,b,c \in \mathbb{Z}/2\mathbb{Z}$. We may view matrix multiplication in $H(\mathbb{Z}/2\mathbb{Z})$ as

$$(a,b,c)(d,e,f) = (a+d, af+b+e, c+f)$$

Moreover, we identify the identity matrix as $(0,0,0)$. Lastly, the elements of $H(\mathbb{Z}/2\mathbb{Z})$ are

$$(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1),(1,1,1)$$

Noting that $(a,b,c)^2 = (2a, ac+2b, 2c) = (0,ac,0)$ in $\mathbb{Z}/2\mathbb{Z}$, we may consider two cases instead of computing the order of each element directly:

- If $ac = 0$, then at least one of a or c is 0, while b varies. These are the matrices

$$(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1)$$

  Except for the identity matrix which has order 1, squaring any of these matrices results in $(0,0,0)$ so that they all have order 2.
- If $ac = 1$, then both a and c are 1, while b varies. These are the matrices

$$(1,0,1),(1,1,1)$$

  The square of either matrix is $(0,1,0)$, which has order 2. Then the matrices have order 4.

(e) Utilizing the same formulation as in part (d), let $A = (a,b,c) \in H(\mathbb{R})$. We prove that

$$(a,b,c)^n = (na, n(n-1)ac/2 + nb, nc)$$

To that end, it is clear that $n = 1$ holds true. Suppose it holds for some n. Then for $n+1$, we have

$$\begin{aligned}(a,b,c)^{n+1} &= (a,b,c)^n(a,b,c)\\ &= (na, n(n-1)ac/2 + nb, nc)(a,b,c)\\ &= (na+a, (na)c + n(n-1)ac/2 + nb + b, nc + c)\\ &= ((n+1)a, n(n+1)ac/2 + (n+1)b, (n+1)c)\end{aligned}$$

so that the relationship is true by induction. Since $A \neq I$, then at least one of a,b,c must be nonzero. Then for any $n \in \mathbb{Z}^+$, none of the integers $na, n(n-1)ac/2 + nb$, or nc are 0. Then no power of (a,b,c) results in $(0,0,0)$, hence no nonidentity element of $H(\mathbb{R})$ has any finite order. Therefore, every nonidentity element of $H(\mathbb{R})$ has infinite order. ■

1.5 The Quaternion Group

Exercise 1.5.1

Compute the order of each of the elements in Q_8.

Solution.

a	1	-1	i	$-i$	j	$-j$	k	$-k$
$\lvert a\rvert$	1	2	4	4	4	4	4	4

■

Exercise 1.5.2

Write out the group tables for S_3, D_8, and Q_8.

Solution. S_3:

$\circ$	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
1	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	1	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	1	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	1	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	1
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	1	(1 2 3)

D_8:

$\circ$	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

■

Q_8:

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	j	$-j$
$-i$	$-i$	i	1	-1	$-k$	k	$-j$	j
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Exercise 1.5.3

Find a set of generators and relations for Q_8.

Solution. An extra relation is necessary to intertwine i, j, k together, so a presentation for Q_8 is:

$$Q_8 = \langle -1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$$

■

1.6 Homomorphisms and Isomorphisms

Exercise 1.6.1

Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Solution.

(a) We proceed by induction on n. For $n = 1$, the result holds. Suppose it holds for some $n \in \mathbb{Z}^+$. Then for $n+1$, we have

$$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$$

so that the result holds by induction.

(b) We first show that the result holds for $n = 0$, i.e., identities map to identities. Let 1_G and 1_H be the identities of G and H respectively. Then

$$\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G)$$

so that multiplying both sides on the left by $\varphi(1_G)^{-1}$ yields $\varphi(1_G) = 1_H$. Let $x \in G$. Then for $n = -1$, we have

$$1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$$

Left multiplying both sides by $\varphi(x)^{-1}$ yields $\varphi(x^{-1}) = \varphi(x)^{-1}$. Finally, for $n < -1$, we have

$$\varphi(x^n) = \varphi(x^{-1})^{-n} = \varphi(x)^{-n} = \varphi(x)^n$$

so that the result holds for all $n \in \mathbb{Z}$. ■

(∗) Exercise 1.6.2

If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

Solution. Let $x \in G$. Let $|x| = m$ and $|\varphi(x)| = n$. Then

$$1_H = \varphi(1_G) = \varphi(x^m) = \varphi(x)^m$$

so that $n \leq m$. Similarly,

$$1_G = \varphi^{-1}(1_H) = \varphi^{-1}(\varphi(x)^n) = x^n$$

so that $m \leq n$. It follows that $m = n$, i.e., $|\varphi(x)| = |x|$.

Assume, by way of contradiction and without loss of generality that x has infinite order in G but $\varphi(x)$ has finite order in H. Then by the above result, $|\varphi(x)| = |x|$ implies that x must also have finite order, a contradiction. Thus, both x and $\varphi(x)$ both must have either finite or infinite order. Moreover, for any $n \in \mathbb{Z}^+$, the number of elements of order n in G must equal the number of elements of order n in H since φ is bijective and preserves order.

The result does not always hold if φ is only a homomorphism. Let G be any group, and let H be the trivial group. Consider the mapping $\varphi : G \to H$ defined by $\varphi(g) = 1_H$ for all $g \in G$. Clearly, φ is a homomorphism, but all elements of H have order 1, while G may have elements of various orders. ■

Exercise 1.6.3

If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

Solution. Since φ is bijective, then φ^{-1} exists and is also an isomorphism.

- ($\Rightarrow$) Suppose G is abelian. Then for any $h_1, h_2 \in H$, there exists $g_1, g_2 \in G$ such that $g_1 = \varphi^{-1}(h_1)$ and $g_2 = \varphi^{-1}(h_2)$. Then

$$h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1$$

  so that H is abelian.
- ($\Leftarrow$) Suppose H is abelian. Then for any $g_1, g_2 \in G$, there exists $h_1, h_2 \in H$ such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. Then

$$g_1g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2) = \varphi^{-1}(h_1h_2) = \varphi^{-1}(h_2h_1) = \varphi^{-1}(h_2)\varphi^{-1}(h_1) = g_2g_1$$

  so that G is abelian.

To see what conditions are sufficient for the homomorphism to imply that its codomain is abelian if its domain is abelian, let $\varphi : G \to H$ be a homomorphism. Then for $h_1, h_2 \in H$, then see by the previous proof that if there exists $g_1, g_2 \in G$ such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$, then H is abelian whenever G is abelian. Thus, it suffices to ensure that such g_1 and g_2 always exist, which is true if φ is surjective. Hence, we may deduce that to ensure that if G is abelian, then so is H, it suffices to require that φ is surjective. ■

Exercise 1.6.4

Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Solution. Note that $i \in C - \{0\}$ has order 4, but there is no element in $\mathbb{R} - \{0\}$ that has order 4. ■

Exercise 1.6.5

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution. Since $\mathbb{R}$ is uncountable while $\mathbb{Q}$ is countable, there cannot exist a bijection between the two groups, hence they cannot be isomorphic. ■

Exercise 1.6.6

Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Solution. For every $n \in \mathbb{Z}$, there exists no $x \in \mathbb{Z}$ such that $nx = 0$. However, for every $q \in \mathbb{Q}$ of the form $1/k$ for some $k \in \mathbb{Z}$ with $k \neq 0$, we have $kq = 0$. Thus, there cannot exist a bijection between the two groups that preserves addition, hence they cannot be isomorphic. ■

Exercise 1.6.7

Prove that D_8 and Q_8 are not isomorphic.

Solution. D_8 has only 1 element of order 4, while Q_8 has 3 elements of order 4. ■

Exercise 1.6.8

Prove that if $n \neq m$, then S_n and S_m are not isomorphic.

Solution. If $n \neq m$, then $n! \neq m!$ so that $|S_n| \neq |S_m|$. ■

Exercise 1.6.9

Prove that D_{24} and S_4 are not isomorphic.

Solution. D_{24} has elements of order 12 (e.g. r) but S_4 has no elements of order 12, since every element of S_4 is either a 2-cycle, 3-cycle, 4-cycle, or a combination of 2-cycles. ■

Exercise 1.6.10

Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \to \Omega$ be a bijection. Define

$$\varphi : S_\Delta \to S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

and prove the following:

(a) Prove that φ is well-defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

(b) Prove that φ is a bijection from S_Δ onto S_Ω by finding a two-sided inverse for φ.

(c) Prove that φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Note the similarity to the change of basis or similarity transformations for matrices (we shall see the connections between these later in the text).

Solution.

(a) We show that a composition of bijections is a bijection. Let A, B, C be nonempty sets, and let $f : A \to B$ and $g : B \to C$ be bijections. We show that $g \circ f : A \to C$ is a bijection. For injectivity, let $a_1, a_2 \in A$ such that $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then $g(f(a_1)) = g(f(a_2))$, and since g is injective, then $f(a_1) = f(a_2)$. Since f is also injective, then $a_1 = a_2$. For surjectivity, let $c \in C$. Since g is surjective, there exists some $b \in B$ such that $g(b) = c$. Since f is surjective, there exists some $a \in A$ such that $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = c$. Hence, $g \circ f$ is a bijection.

Now, by assumption, $\theta : \Delta \to \Omega$ is a bijection, and since $\sigma : \Delta \to \Delta$ is also a bijection, then by the above result, $\theta \circ \sigma : \Delta \to \Omega$ is a bijection. Finally, since $\theta^{-1} : \Omega \to \Delta$ is a bijection, then by the above result again, $\theta \circ \sigma \circ \theta^{-1} : \Omega \to \Omega$ is a bijection. Hence, φ is well-defined.

(b) Consider the mapping

$$\psi : S_\Omega \to S_\Delta \quad \text{by} \quad \psi(\tau) = \theta^{-1} \circ \tau \circ \theta \quad \text{for all } \tau \in S_\Omega$$

By the above discussion, ψ is well-defined. For any $\sigma \in S_\Delta$, we have

$$\psi(\varphi(\sigma)) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = \mathrm{id}_{S_\Delta} \circ \sigma \circ \mathrm{id}_{S_\Delta} = \sigma$$

and for any $\tau \in S_\Omega$, we have

$$\varphi(\psi(\tau)) = \theta \circ (\theta^{-1} \circ \tau \circ \theta) \circ \theta^{-1} = \mathrm{id}_{S_\Omega} \circ \tau \circ \mathrm{id}_{S_\Omega} = \tau$$

so that ψ is a two-sided inverse for φ. Hence, φ is a bijection from S_Δ onto S_Ω.

(c) Let $\sigma, \tau \in S_\Delta$. Then

$$\varphi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = (\theta \circ \sigma) \circ (\tau \circ \theta^{-1}) = (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \varphi(\sigma) \circ \varphi(\tau)$$

so that φ is a homomorphism. By the above, φ is an isomorphism, and hence $S_\Delta \cong S_\Omega$. ■

Exercise 1.6.11

Let A and B be groups. Prove that $A \times B \cong B \times A$.

Solution. Consider the mapping

$$\varphi : A \times B \to B \times A \quad \text{by} \quad (a, b) \mapsto (b, a)$$

for all $a \in A$ and $b \in B$. For any $(a_1, b_1), (a_2, b_2) \in A \times B$, we have

$$\varphi((a_1, b_1)(a_2, b_2)) = \varphi((a_1a_2, b_1b_2)) = (b_1b_2, a_1a_2) = (b_1, a_1)(b_2, a_2) = \varphi(a_1, b_1)\varphi(a_2, b_2)$$

so that φ is a homomorphism. Moreover, suppose $(a_1, b_1), (a_2, b_2) \in A \times B$ are such that $\varphi(a_1, b_1) = \varphi(a_2, b_2)$. Then $(b_1, a_1) = (b_2, a_2)$ so that $a_1 = a_2$ and $b_1 = b_2$. Hence, φ is injective. Finally, for any $(b, a) \in B \times A$, then $\varphi(a, b) = (b, a)$ so that φ is surjective. Therefore, φ is an isomorphism and $A \times B \cong B \times A$. ■

Exercise 1.6.12

Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

Solution. Consider the mapping

$$\varphi : G \times C \to A \times H \quad \text{by} \quad ((a, b), c) \mapsto (a, (b, c))$$

for all $a \in A$, $b \in B$, and $c \in C$. The proof is similar to the previous exercise, hence we omit the details to conclude that φ is an isomorphism and $G \times C \cong A \times H$. ■

(∗) Exercise 1.6.13

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H (cf. Exercise 1.1.26). Prove that if φ is injective then $G \cong \varphi(G)$.

Solution. We first show that $\varphi(G) = \{\varphi(g) \mid g \in G\}$ is a subgroup of H. Note that $1_H = \varphi(1_G) \in \varphi(G)$ so that it is nonempty. To show closure, let $h_1, h_2 \in \varphi(G)$. Then there exists $g_1, g_2 \in G$ such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. Then

$$h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in \varphi(G)$$

so that $\varphi(G)$ is closed under the group operation of H. Finally, for any $h \in \varphi(G)$, there exists some $g \in G$ such that $h = \varphi(g)$. Then

$$h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \varphi(G)$$

so that $\varphi(G)$ is closed under taking inverses. Therefore, $\varphi(G)$ is a subgroup of H.

Now suppose φ is injective. Consider the mapping

$$\psi : G \to \varphi(G) \quad \text{by} \quad g \mapsto \varphi(g)$$

for all $g \in G$. For any $g_1, g_2 \in G$, we have

$$\psi(g_1g_2) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1)\psi(g_2)$$

so that ψ is a homomorphism. Moreover, suppose $g_1, g_2 \in G$ are such that $\psi(g_1) = \psi(g_2)$. Then $\varphi(g_1) = \varphi(g_2)$, and since φ is injective, then $g_1 = g_2$. Hence, ψ is injective. Finally, for any $h \in \varphi(G)$, there exists some $g \in G$ such that $h = \varphi(g) = \psi(g)$ so that ψ is surjective. Therefore, ψ is an isomorphism and $G \cong \varphi(G)$. ■

(∗) Exercise 1.6.14

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Solution. Let $\ker\varphi$ denote the kernel of φ. Note that $1_G \in \ker\varphi$ since $\varphi(1_G) = 1_H$, so that $\ker\varphi$ is nonempty. To show closure, let $g_1, g_2 \in \ker\varphi$. Then

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = 1_H1_H = 1_H$$

so that $g_1g_2 \in \ker\varphi$. Finally, for any $g \in \ker\varphi$, we have

$$\varphi(g^{-1}) = \varphi(g)^{-1} = 1_H^{-1} = 1_H$$

so that $g^{-1} \in \ker\varphi$. Therefore, $\ker\varphi$ is a subgroup of G.

- ($\Rightarrow$) Suppose φ is injective. Let $g \in \ker\varphi$. Then $\varphi(g) = 1_H = \varphi(1_G)$, and since φ is injective, then $g = 1_G$. Hence, $\ker\varphi = \{1_G\}$.
- ($\Leftarrow$) Suppose $\ker\varphi = \{1_G\}$. Let $g_1, g_2 \in G$ be such that $\varphi(g_1) = \varphi(g_2)$. Then

$$1_H = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1g_2^{-1})$$

so that $g_1g_2^{-1} \in \ker\varphi$. By assumption, then $g_1g_2^{-1} = 1_G$, and hence $g_1 = g_2$. Therefore, φ is injective.

■

Exercise 1.6.15

Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Solution. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. Then

$$\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 = \pi((x_1, y_1)) + \pi((x_2, y_2))$$

so that π is a homomorphism. Moreover, if $(x, y) \in \ker(\pi)$, then $\pi((x, y)) = x = 0$. Hence,

$$\ker(\pi) = \{(0, y) \mid y \in \mathbb{R}\}$$

■

Exercise 1.6.16

Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.

Solution. For any $(a_1, b_1), (a_2, b_2) \in G$, we have

$$\pi_1((a_1, b_1)(a_2, b_2)) = \pi_1((a_1a_2, b_1b_2)) = a_1a_2 = \pi_1((a_1, b_1))\pi_1((a_2, b_2))$$

and

$$\pi_2((a_1, b_1)(a_2, b_2)) = \pi_2((a_1a_2, b_1b_2)) = b_1b_2 = \pi_2((a_1, b_1))\pi_2((a_2, b_2))$$

so that both π_1 and π_2 are homomorphisms. Moreover, if $(a, b) \in \ker(\pi_1)$, then $\pi_1((a, b)) = a = 1_A$. Also, if $(a, b) \in \ker(\pi_2)$, then $\pi_2((a, b)) = b = 1_B$. Hence,

$$\ker(\pi_1) = \{(1_A, b) \mid b \in B\} \quad \text{and} \quad \ker(\pi_2) = \{(a, 1_B) \mid a \in A\}$$

■

Exercise 1.6.17

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution.

- ($\Rightarrow$) Suppose φ is a homomorphism. Then for $g, h \in G$, we have
$$(gh)^{-1} = \varphi(gh) = \varphi(g)\varphi(h) = g^{-1}h^{-1}$$
Since inverses are unique, then $hg = gh$ so that G is abelian.
- ($\Leftarrow$) Suppose G is abelian. Then for $g, h \in G$, we have
$$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$$
so that φ is a homomorphism. ■

Exercise 1.6.18

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Solution.

- ($\Rightarrow$) Suppose φ is a homomorphism. Then for $g, h \in G$, we have
$$(gh)^2 = \varphi(gh) = \varphi(g)\varphi(h) = g^2h^2$$
Then $ghgh = g^2h^2$, so that multiplying both sides on the left by g^{-1} and on the right by h^{-1} yields $hg = gh$ and G is abelian.
- ($\Leftarrow$) Suppose G is abelian. Then for $g, h \in G$, we have
$$\varphi(gh) = (gh)^2 = g^2h^2 = \varphi(g)\varphi(h)$$
so that φ is a homomorphism. ■

Exercise 1.6.19

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

Solution. Recall that the polar form of a complex number is $z = r(\cos\theta + i\sin\theta) = re^{i\theta}$, where r is the modulus and $\theta = \arg(z)$ is the argument. By definition, every $z \in G$ has modulus $r = 1$ so that every element of G is of the form $e^{i\theta}$. Moreover, $z \in G$ implies that $z^n = 1$ for some $n \in \mathbb{Z}^+$. Using the polar representation of $1 = e^{2\pi im}$ for some $m \in \mathbb{Z}$, then we have $e^{in\theta} = e^{2\pi im}$. This implies that $\theta = 2\pi m/n$, and we can reformulate G as the following:
$$G = \{e^{2\pi im/n} \in \mathbb{C} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\}$$
We show that φ is a homomorphism. For any $z, w \in G$, we have
$$\varphi(zw) = (zw)^k = z^k w^k = \varphi(z)\varphi(w)$$
so that φ is a homomorphism. To show surjectivity, let $w \in G$. Then $w = e^{2\pi im/n}$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Since $z = e^{2\pi im/nk} \in G$ because $nk \in \mathbb{Z}^+$, then
$$z^k = (e^{2\pi im/nk})^k = e^{2\pi im/n} = w$$
so that $\varphi(z) = w$ and φ is surjective. Lastly, we show that φ is not an isomorphism by finding its kernel. Note that every $z \in \ker\varphi$ satisfies $z^k = 1$. Then $z = e^{2\pi im/k}$ for some $m \in \mathbb{Z}$. Since there are k distinct values of m modulo k, then $\ker\varphi$ contains k distinct elements, namely
$$\ker\varphi = \{e^{2\pi im/k} \mid m = 0, 1, \ldots, k-1\}$$
Since $k > 1$, then $\ker\varphi$ contains more than just the identity element, so that φ is not injective by Exercise 1.6.14. Hence, φ is not an isomorphism. ■

(∗) Exercise 1.6.20

Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\mathrm{Aut}(G)$ are called *automorphisms* of G).

Solution. Since function composition is associative, then it is also associative on $\mathrm{Aut}(G)$. By the proof in Exercise 1.6.10, the composition of two bijections is a bijection. We now show that the composition of two isomorphisms is an isomorphism. Let $\varphi, \psi \in \mathrm{Aut}(G)$. Then for any $g_1, g_2 \in G$, we have

$$(\varphi \circ \psi)(g_1 g_2) = \varphi(\psi(g_1 g_2)) = \varphi(\psi(g_1)\psi(g_2)) = \varphi(\psi(g_1))\varphi(\psi(g_2)) = (\varphi \circ \psi)(g_1)(\varphi \circ \psi)(g_2)$$

so that $\varphi \circ \psi$ is a homomorphism. Since $\varphi \circ \psi$ is also a bijection, then it is an isomorphism and $\varphi \circ \psi \in \mathrm{Aut}(G)$. The identity map $\mathrm{id}_G : G \to G$ defined by $\mathrm{id}_G(g) = g$ for all $g \in G$ is an isomorphism, so that $\mathrm{id}_G \in \mathrm{Aut}(G)$ and is the identity element of $\mathrm{Aut}(G)$. Finally, for any $\varphi \in \mathrm{Aut}(G)$, since φ is a bijection, then φ^{-1} exists. We show that φ^{-1} is also an isomorphism. For any $g_1, g_2 \in G$, we have

$$\varphi^{-1}(g_1 g_2) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1 g_2))) = \varphi^{-1}(\varphi(\varphi^{-1}(g_1)\varphi^{-1}(g_2))) = \varphi^{-1}(g_1)\varphi^{-1}(g_2)$$

so that φ^{-1} is a homomorphism. Since φ^{-1} is also a bijection, then it is an isomorphism and $\varphi^{-1} \in \mathrm{Aut}(G)$. Therefore, $\mathrm{Aut}(G)$ is a group under function composition. ■

Exercise 1.6.21

Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$.

Solution. Let $\varphi : \mathbb{Q} \to \mathbb{Q}$ be defined by $\varphi(q) = kq$ for all $q \in \mathbb{Q}$. For any $q_1, q_2 \in \mathbb{Q}$, we have

$$\varphi(q_1 + q_2) = k(q_1 + q_2) = kq_1 + kq_2 = \varphi(q_1) + \varphi(q_2)$$

so that φ is a homomorphism. Moreover, suppose $q_1, q_2 \in \mathbb{Q}$ are such that $\varphi(q_1) = \varphi(q_2)$. Then $kq_1 = kq_2$, and since $k \neq 0$, then $q_1 = q_2$. Hence, φ is injective. Finally, for any $q \in \mathbb{Q}$, we have $\varphi(q/k) = k(q/k) = q$ so that φ is surjective. Therefore, φ is an automorphism of $\mathbb{Q}$. ■

Exercise 1.6.22

Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

Solution. Let $\varphi : A \to A$ be defined by $\varphi(a) = a^k$ for all $a \in A$. For any $a_1, a_2 \in A$, we have

$$\varphi(a_1 a_2) = (a_1 a_2)^k = a_1^k a_2^k = \varphi(a_1)\varphi(a_2)$$

so that φ is a homomorphism. For $k = -1$, see Exercise 1.6.17 to conclude that $\varphi \in \mathrm{Aut}(A)$. ■

Exercise 1.6.23

Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Solution. To show that every $g \in G$ is of the form $x^{-1}\sigma(x)$ for some $x \in G$, we must show that the map

$$\varphi : G \to G \quad \text{by} \quad x \mapsto x^{-1}\sigma(x)$$

is injective. Supppose $x, y \in G$ are such that $\varphi(x) = \varphi(y)$. Then

$$x^{-1}\sigma(x) = y^{-1}\sigma(y)$$

so that $yx^{-1} = \sigma(yx^{-1})$. Since σ is fixed point free, then $yx^{-1} = 1$ and $x = y$. Hence, φ is injective. Since G is finite, then φ is also surjective, and every element of G may be written in the form $x^{-1}\sigma(x)$ for some $x \in G$.

To show that G is abelian, observe for any $g \in G$ that

$$\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x^{-1})\sigma^2(x) = \sigma(x)^{-1}x = (x^{-1}\sigma(x))^{-1} = g^{-1}$$

where $\sigma^2 = \mathrm{id}_G$ was used. Now, for any $g, h \in G$, we have

$$\sigma(gh) = (gh)^{-1} = h^{-1}g^{-1} = \sigma(h)\sigma(g) = \sigma(hg)$$

Since σ is injective, then $gh = hg$ and G is abelian. ■

Exercise 1.6.24

Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$.

Solution. To show that G is isomorphic to D_{2n}, we first need to produce an element $t \in G$ of order n along with an element $x \in G$ of order 2 such that $xt = t^{-1}x$. The clear choice is to let $t = xy$ and keep x as is. Note that $|t| = |xy| = n$ by assumption, and $|x| = 2$ by assumption. Moreover,

$$xt = x(xy) = (xx)y = y = (xy)^{-1}x = t^{-1}x$$

so that the elements $x, t \in G$ satisfy the relations of D_{2n}. Moreover, observe that $y = xt$ so that t and x generate G. Following this, it is easy to see that every element of G can be written in the form $x^i t^j$ for $i \in \{0, 1\}$ and $0 \leq j < n$. For $x = 0$, we have the elements in the cyclic subgroup generated by t, and for $x = 1$, we have the elements $\{x, xt, xt^2, \ldots, xt^{n-1}\}$. Since $|t| = n$, then these are all distinct elements of G. Hence, $|G| = 2n$.

Since the relations of D_{2n} are satisfied by $x, t \in G$, G is generated by x and t, and $|G| = |D_{2n}| = 2n$, it follows that the map

$$\varphi : D_{2n} \to G \quad \text{by} \quad r \mapsto t, s \mapsto x$$

extends to an isomorphism from D_{2n} onto G. Therefore, $G \cong D_{2n}$. ■

Exercise 1.6.25

Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.

(a) Prove that the matrix
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
is the matrix of the linear transformation which rotates the x, y-plane about the origin in a counterclockwise direction by θ radians.

(b) Prove that the map $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ defined on generators by
$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{and} \quad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
extends to a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$.

(c) Prove that the homomorphism φ defined above is injective.

Solution.

(a) Let $\mathbb{R}^2$ be generated by the standard basis vectors $\mathbf{e}_1 = (1 \quad 0)^T$ and $\mathbf{e}_2 = (0 \quad 1)^T$. Let T denote the linear transformation which rotates the x, y-plane about the origin in a counterclockwise direction by θ radians. Then
$$T(\mathbf{e}_1) = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \quad \text{and} \quad T(\mathbf{e}_2) = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$
So the matrix of T with respect to the standard basis is
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

(b) It is easy to show by induction that for any positive k, then $\varphi(r)^k$ is given by the following matrix:
$$\varphi(r)^k = \begin{pmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{pmatrix}$$
so that $\varphi(r)^n = I$. It is fairly straightforward to see that the set of vectors $\{T(\mathbf{e}_1), T(\mathbf{e}_2)\}$ is orthonormal, so $\varphi(r)$ is orthogonal. Hence, $\varphi(r)^{-1} = \varphi(r)^T$. Moreover, we can calculate that
$$\varphi(s)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
so that $\varphi(s)^2 = I$. Lastly, we calculate that
$$\varphi(s)\varphi(r) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \varphi(r)^{-1}\varphi(s)$$
so that $\varphi(s)\varphi(r) = \varphi(r)^{-1}\varphi(s)$. Since these relations match those of D_{2n}, then φ extends to a homomorphism from D_{2n} to $\mathrm{GL}_2(\mathbb{R})$.

(c) To show that φ is injective, we show that $\ker\varphi$ is trivial. Let $g \in \ker\varphi$.
- If $g = r^k$ for some $0 \le k < n$, then $\varphi(r^k) \neq I$, since $\varphi(r)^k$ is a rotation matrix and only $\varphi(r)^n = I$.
- If $g = sr^k$ for some $0 \le k < n$, then $\varphi(sr^k) = \varphi(s)\varphi(r)^k$. Note that $\varphi(s)$ has determinant -1 while $\varphi(r)^k$ has determinant 1 since it is a rotation matrix. Hence, $\varphi(sr^k)$ has determinant -1 and cannot be the identity matrix.

Therefore, the only element in $\ker\varphi$ is the identity element of D_{2n}, so that φ is injective. ■

Exercise 1.6.26

Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $\mathrm{GL}_2(\mathbb{C})$ defined on generators by

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that φ is injective.

Solution. It is easy to see that

$$\varphi(i)^2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

and

$$\varphi(j)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

Also note that

$$\varphi(i)\varphi(j) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

So we may set $\varphi(i)\varphi(j) = \varphi(k)$. We can calculate that $\varphi(k)^2 = -I$. It then follows that

$$\varphi(i)^2 = \varphi(j)^2 = \varphi(k)^2 = \varphi(i)\varphi(j)\varphi(k) = \varphi(-1)$$

The elements $\varphi(i), \varphi(j)$, and $\varphi(k)$ satisfy the relations of Q_8 as described in Exercise 1.5.3 so that φ extends to a homomorphism from Q_8 to $\mathrm{GL}_2(\mathbb{C})$. Moreover, φ is injective since the only element that maps to the identity matrix is $1 \in Q_8$. Therefore, φ is an injective homomorphism. ■

1.7 Group Actions

Exercise 1.7.1

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definition of a field are used).

Solution. Let $g, h \in F^\times$ and $f \in F$. Then

$$g \cdot (h \cdot f) = g \cdot (hf) = g(hf) = (gh)f = (gh) \cdot f$$

where the associativity of multiplication in F was used to conclude that $g(hf) = (gh)f$. Moreover, $1 \cdot f = 1f = f$ where 1 is the multiplicative identity in F. Therefore, the group action axioms are satisfied and $F^\times$ acts on F. ■

Exercise 1.7.2

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Solution. Let $z, w \in \mathbb{Z}$ and $a \in \mathbb{Z}$. Then

$$z \cdot (w \cdot a) = z \cdot (w + a) = z + (w + a) = (z + w) + a = (z + w) \cdot a$$

Moreover, $0 \cdot a = 0 + a = a$ so that the group action axioms are satisfied and $\mathbb{Z}$ acts on itself. ■

Exercise 1.7.3

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + r, y)$.

Solution. Let $r, s \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$. Then

$$r \cdot (s \cdot (x, y)) = r \cdot (x + s, y) = (x + s + r, y) = (x + (r + s), y) = (r + s) \cdot (x, y)$$

Moreover, $0 \cdot (x, y) = (x + 0, y) = (x, y)$ so that the group action axioms are satisfied and $\mathbb{R}$ acts on $\mathbb{R}^2$. ■

(∗) Exercise 1.7.4

Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. Exercise 1.1.26):

(a) the kernel of the action,

(b) $\{g \in G \mid ga = a\}$ — this subgroup is called the *stabilizer* of a in G.

Solution.

(a) Suppose g, h are in the kernel of the action. Then for any $a \in A$, we have

$$gh \cdot a = g \cdot (h \cdot a) = g \cdot a = a$$

so that gh is in the kernel of the action. Also, for any g in the kernel of the action and any $a \in A$, we have

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a$$

so that g^{-1} is in the kernel of the action. Therefore, the kernel of the action is a subgroup of G.

(b) Let G_a denote the stabilizer of a in G. Suppose $g, h \in G_a$. Then

$$gh \cdot a = g \cdot (h \cdot a) = g \cdot a = a$$

so that $gh \in G_a$. Also, for any $g \in G_a$, we have

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a$$

so that $g^{-1} \in G_a$. Therefore, G_a is a subgroup of G. ■

Exercise 1.7.5

Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$ (cf. Exercise 1.6.14).

Solution. Let K denote the kernel of the action, and let K' denote $\ker \varphi$, where $\varphi : G \to S_A$ is the permutation representation corresponding to the action. Suppose $g \in K$. Then $g \cdot a = a$ for every $a \in A$, hence $\varphi(g)$ is the identity permutation in S_A and $g \in K'$. Conversely, suppose $g \in K'$. Then $\varphi(g)$ is the identity permutation in S_A, so that for every $a \in A$, we have $\varphi(g)(a) = a$. But $\varphi(g)(a) = g \cdot a$ by definition of the permutation representation, so that $g \cdot a = a$ for every $a \in A$ and $g \in K$. Therefore, $K = K'$. ■

(∗) Exercise 1.7.6

Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

Solution.

- ($\Rightarrow$) Suppose G acts faithfully on A. Let g be in the kernel of the action. Then for every $a \in A$, we have $g \cdot a = a$. Since the action is faithful, then g must be the identity element of G. Hence, the kernel of the action is the set consisting only of the identity.
- ($\Leftarrow$) Suppose the kernel of the action is the set consisting only of the identity. Let $g, h \in G$ be such that $g \cdot a = h \cdot a$ for every $a \in A$. Then

$$h^{-1}g \cdot a = h^{-1} \cdot (g \cdot a) = h^{-1} \cdot (h \cdot a) = (h^{-1}h) \cdot a = 1 \cdot a = a$$

so that $h^{-1}g$ is in the kernel of the action. By assumption, then $h^{-1}g$ is the identity element of G, and $g = h$. Therefore, the action is faithful. ■

Exercise 1.7.7

Prove that in Example 2 in this section the action is faithful.

Solution. Let V be a vector space over a field F. Let $F^\times$ act on V by $r \cdot v = rv$ for all $r \in F^\times$ and $v \in V$. Suppose $r \in F^\times$ is in the kernel of the action. Then for every $v \in V$, we have $r \cdot v = v$, so that $rv = v$. Since V is a vector space, then it contains the nonzero vector $v = 1$. Hence, $r(1) = 1$ so that $r = 1$. Therefore, the kernel of the action is the set consisting only of the identity, and by the previous exercise, the action is faithful. ■

Exercise 1.7.8

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by

$$\sigma(\{a_1, \ldots, a_k\}) = \{\sigma(a_1), \ldots, \sigma(a_k)\}.$$

(a) Prove that this is a group action.

(b) Describe explicitly how the elements (1 2) and (1 2 3) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Solution.

(a) Let $\sigma, \tau \in S_A$. Then for any cardinality k subset $\{x_1, \ldots, x_k\}$ of A, we have

$$\begin{aligned} \sigma \cdot (\tau \cdot \{x_1, \ldots, x_k\}) &= \sigma \cdot \{\tau(x_1), \ldots, \tau(x_k)\} \\ &= \{\sigma(\tau(x_1)), \ldots, \sigma(\tau(x_k))\} \\ &= (\sigma \circ \tau) \cdot \{x_1, \ldots, x_k\} \end{aligned}$$

Moreover, $1 \cdot \{x_1, \ldots, x_k\} = \{1(x_1), \ldots, 1(x_k)\} = \{x_1, \ldots, x_k\}$. Then it is a group action.

(b)

A	$(1\,2)\cdot A$	$(1\,2\,3)\cdot A$
$\{1,2\}$	$\{2,1\}$	$\{2,3\}$
$\{1,3\}$	$\{2,3\}$	$\{2,1\}$
$\{1,4\}$	$\{2,4\}$	$\{2,4\}$
$\{2,3\}$	$\{1,3\}$	$\{3,1\}$
$\{2,4\}$	$\{1,4\}$	$\{3,4\}$
$\{3,4\}$	$\{3,4\}$	$\{1,4\}$

■

Exercise 1.7.9

Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses (note that, for example, the 2-tuples $(1,2)$ and $(2,1)$ are different even though the sets $\{1,2\}$ and $\{2,1\}$ are the same, so the sets being acted upon are different).

Solution. The work is similar as above, except there are 12 2-tuples as $(1,2) \neq (2,1)$. ■

Exercise 1.7.10

With reference to the preceding two exercises determine:

(a) for which values of k the action of S_n on k-element subsets is faithful, and

(b) for which values of k the action of S_n on ordered k-tuples is faithful.

Solution.

(a) If $k = |A|$, then any subset S of A with cardinality k is equal to A. Then any $\sigma \in S_n$ will fix S, so the action is not faithful.

Let $\sigma \in S_n$ be a non-identity permutation. Then there exists some $a \in A$ such that $\sigma(a) \neq a$. If $k < |A|$, then we can choose a k-element subset S of A such that $a \in S$ and $\sigma(a) \notin S$. Then $\sigma(S) \neq S$, hence no non-identity permutation fixes every k-element subset of A. Therefore, the action is faithful for all $1 \leq k < |A|$.

(b) Let $\sigma \in S_n$ be a non-identity permutation. Then there exists some $a \in A$ such that $\sigma(a) \neq a$. Consider the ordered k-tuple $T = (a, x_2, x_3, \ldots, x_k)$ where $x_2, x_3, \ldots, x_k$ are distinct elements of A different from a and $\sigma(a)$. Then $\sigma(T) = (\sigma(a), \sigma(x_2), \sigma(x_3), \ldots, \sigma(x_k)) \neq T$ because the first element is different. Hence, no non-identity permutation fixes every ordered k-tuple of elements of A. Therefore, the action is faithful for all $1 \leq k \leq |A|$. ■

Exercise 1.7.11

Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labeled as in Section 2).

Solution. Let $\varphi : D_8 \to S_4$ be the permutation representation of the action of D_8 on the vertices of a square $\{1,2,3,4\}$, where the vertices are labeled in order around the square starting in the top left corner, then going clockwise. Then the cycle decompositions are as follows:

$$\begin{aligned} \varphi(1) &= 1 & \varphi(r) &= (1\,2\,3\,4) \\ \varphi(r^2) &= (1\,3)(2\,4) & \varphi(r^3) &= (1\,4\,3\,2) \\ \varphi(s) &= (2\,4) & \varphi(sr) &= (1\,4)(2\,3) \\ \varphi(sr^2) &= (1\,3) & \varphi(sr^3) &= (1\,2)(3\,4) \end{aligned}$$

■

(∗) Exercise 1.7.12

Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

Solution. Let the vertices of the regular n-gon be labeled $1, 2, \ldots, n$ in order around the polygon. Let P_k denote the pair of opposite vertices, i.e.,

$$P_k = \{k, k + n/2\} \quad \text{defined for all } 1 \leq k \leq n/2$$

Let P denote the set of all such pairs of opposite vertices. Note that $|P| = n/2$. Define a mapping from $D_{2n} \times P \to P$ by

$$g \cdot P_i = g(P_i) = P_j$$

where P_j is the pair of opposite vertices containing the images of the vertices in P_i under the action of g on the vertices of the n-gon. It is straightforward to verify that this mapping satisfies the group action axioms, since any rotation or reflection of the n-gon will map pairs of opposite vertices to other pairs of opposite vertices. Hence, D_{2n} acts on P.

To find the kernel of this action, let $g \in D_{2n}$ be in the kernel. Then for every pair of opposite vertices $P_i \in P$, we have $g \cdot P_i = P_i$. In particular, consider the pair $P_1 = \{1, 1 + n/2\}$. Then g must map vertex 1 to either vertex 1 or vertex $1 + n/2$. If g maps vertex 1 to vertex $1 + n/2$, then it must also map vertex $1 + n/2$ to vertex 1, which is only possible if g is a rotation by $180^\circ = r^{n/2}$. On the other hand, if g maps vertex 1 to vertex 1, then g is the identity element. Moreover, no reflection can be in the kernel:

- If the reflection is about an axis through vertex k and $k + n/2$, then the vertex $k + 1$ is mapped to vertex $k - 1$, which in general is not equal to either $k + 1$ or $k + 1 + n/2$.
- If the reflection is about an axis through the midpoints of the edges between vertices k and $k + 1$ and between vertices $k + n/2$ and $k + n/2 + 1$, then vertex k is mapped to vertex $k + 1$, which in general is not equal to either k or $k + n/2$.

Therefore, the kernel of this action is $\{1, r^{n/2}\}$. In particular, the kernel for $n = 2$ is the whole group D_4 since there is only one pair of opposite vertices. ■

Exercise 1.7.13

Find the kernel of the left regular action.

Solution. If g is in the kernel of the left regular action of G on itself, then $g \cdot 1 = 1$ in particular. Then $g1 = 1$, implying that $g = 1$. Then the kernel of the left regular action is trivial. ■

Exercise 1.7.14

Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by

$$g \cdot a = ag \quad \text{for all } g, a \in G$$

do not satisfy the axioms of a (left) group action of G on itself.

Solution. Since G is non-abelian, there exists $g, h \in G$ such that $gh \neq hg$. Assume, by way of contradiction, that the above maps do satisfy the axioms of a left group action. Then for any $a \in A$, we have

$$g \cdot (h \cdot a) = g \cdot (ah) = (ah)g = a(hg)$$

On the other hand, $(gh) \cdot a = a(gh)$. Since $gh \neq hg$, then $a(hg) \neq a(gh)$ for some $a \in A$. This contradicts the assumption that the above maps satisfy the axioms of a left group action. Therefore, the maps do not satisfy the axioms of a left group action. ■

Exercise 1.7.15

Let G be any group and let $A = G$. Show that the maps defined by

$$g \cdot a = ag^{-1} \quad \text{for all } g, a \in G$$

do satisfy the axioms of a (left) group action of G on itself.

Solution. Let $g, h \in G$. Then for any $a \in A$, we ahve

$$g \cdot (h \cdot a) = g \cdot (ah^{-1}) = a(h^{-1}g^{-1}) = a(gh)^{-1} = (gh) \cdot a$$

Moreover, $1 \cdot a = a1^{-1} = a1 = a$. Then the maps define a left group action. ■

(∗) Exercise 1.7.16

Let G be any group and let $A = G$. Show that the maps defined by

$$g \cdot a = gag^{-1} \quad \text{for all } g, a \in G$$

do satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).

Solution. Let $g, h \in G$. Then for any $a \in A$, we have

$$g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = (gh) \cdot a$$

Moreover, $1 \cdot a = 1a1^{-1} = a$. Then the maps define a left group action. ■

Exercise 1.7.17

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e. an automorphism of G). Deduce that x and gxg^{-1} have the same order for all $x \in G$ and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

Solution. We prove that the associated permutation $\varphi : G \to G$ defined by $\varphi(x) = gxg^{-1}$ is an isomorphism. Let $x, y \in G$. Then

$$\varphi(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi(x)\varphi(y)$$

so that φ is a homomorphism. To show that φ is bijective, we show that it is injective. Suppose $\varphi(x) = \varphi(y)$ for some $x, y \in G$. Then

$$gxg^{-1} = gyg^{-1}$$

implying that $x = y$. Surjectivity is clear from conjugation by g^{-1}, so φ is a bijection. Therefore, φ is an isomorphism from G onto itself.

From Exercise 1.6.2, we know that isomorphisms preserve order, so $|x| = |gxg^{-1}|$ for all $x \in G$. If we consider the restriction of φ to a subset A of G, then $\varphi|_A : A \to gAg^{-1}$ remains a bijection so that $|A| = |gAg^{-1}|$. ■

(∗) Exercise 1.7.18

Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \quad \text{if and only if} \quad a = hb \text{ for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

Solution. We verify that $\sim$ is an equivalence relation by checking the three properties:

- Reflexivity: For any $a \in A$, we have $a = 1 \cdot a$ where 1 is the identity element of H. Hence, $a \sim a$.
- Symmetry: Suppose $a, b \in A$ such that $a \sim b$. Then there exists some $h \in H$ such that $a = hb$. Multiplying both sides by h^{-1}, we have $h^{-1}a = b$, so that $b = h^{-1}a$. Since $h^{-1} \in H$, then $b \sim a$.
- Transitivity: Suppose $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then there exist some $h_1, h_2 \in H$ such that $a = h_1 b$ and $b = h_2 c$. Substituting the second equation into the first, we have

$$a = h_1(h_2 c) = (h_1 h_2)c$$

Since $h_1 h_2 \in H$, then $a \sim c$.

Therefore, $\sim$ is an equivalence relation on A. ■

(∗) Exercise 1.7.19

Let H be a subgroup of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let O be the orbit of x under this action of H. Prove that the map

$$H \to O, \qquad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce *Lagrange's Theorem*:

If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$

Solution. Let $\varphi : H \to O$ be the map defined by $\varphi(h) = hx$ for all $h \in H$. We show that φ is a bijection. To show injectivity, suppose $\varphi(h_1) = \varphi(h_2)$ for some $h_1, h_2 \in H$. Then

$$h_1 x = h_2 x$$

implying that $h_1 = h_2$. To show surjectivity, let $y \in O$. Then by definition of the orbit, there exists some $h \in H$ such that $y = hx$. Hence, $\varphi(h) = y$. Therefore, φ is a bijection and $|O| = |H|$.

To deduce Lagrange's Theorem, note by the previous exercise that the orbits of the action of H on G partition G. Since each orbit has cardinality $|H|$, then $|G|$ is a sum of multiples of $|H|$. Therefore, $|H|$ divides $|G|$. ■

Exercise 1.7.20

Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.

Solution. Let G be the group of rigit motions of a tetrahedron with vertices labeled $1, 2, 3, 4$. Then each $\alpha \in G$ sends some vertex to another vertex so that G acts on the set of vertices $A = \{1, 2, 3, 4\}$.

Since G acts on A, this gives rise to a homomorphism

$$\varphi : G \to S_4 \quad \text{where} \quad \varphi(\alpha)(i) = \alpha(i) \quad \text{for all} \quad i \in A.$$

To see that φ is injective, suppose $\varphi(\alpha)$ is the identity permutation in S_4 for some $\alpha \in G$. Then for every vertex $i \in A$, we have $\varphi(\alpha)(i) = i$, so that $\alpha(i) = i$. Since a rigid motion that fixes all vertices must be the identity rigid motion, then α is the identity element of G. Therefore, φ is injective and G is isomorphic to a subgroup of S_4. ■

Exercise 1.7.21

Show that the group of rigid motions of a cube is isomorphic to S_4. (This group acts on the set of four pairs of opposite vertices.)

Solution. Recall that $|G| = 24$ from Exercise 1.2.10. Let G be the group of rigid motions of a cube, and let $A = \{a_1, a_2, a_3, a_4\}$ be the set of pairs of opposite vertices of the cube. Then each $\alpha \in G$ sends some pair of opposite vertices to another pair of opposite vertices so that G acts on A.

Using similar reasoning as in the exercise, we have an injective homomorphism

$$\varphi : G \to S_4 \quad \text{where} \quad \varphi(\alpha)(a_i) = \alpha(a_i) \quad \text{for all} \quad a_i \in A.$$

Since $|G| = 24 = |S_4|$, it follows that φ is surjective as well, hence $G \cong S_4$. ■

Exercise 1.7.22

Show that the group of rigid motions of an octahedron is isomorphic to a subgroup of S_4. (This group acts on the set of four pairs of opposite faces.) Deduce that the groups of rigid motions of a cube and of an octahedron are isomorphic. (These two groups are isomorphic because these solids are "dual.")

Solution. Let G be the group of rigid motions of an octahedron. Let $A = \{f_1, f_2, f_3, f_4\}$ be the set of pairs of opposite faces of the octahedron. Then each $\alpha \in G$ sends some pair of opposite faces to another pair of opposite faces so that G acts on A.

Using similar reasoning as in the previous exercises, we have an injective homomorphism

$$\varphi : G \to S_4 \quad \text{where} \varphi(\alpha)(f_i) = \alpha(f_i) \quad \text{for all} \quad f_i \in A.$$

Therefore, G is isomorphic to a subgroup of S_4. From Exercise 1.2.11, we know that $|G| = 24$, hence $G \cong S_4$. From the previous exercise, we know that the group of rigid motions of a cube is also isomorphic to S_4, so the groups of rigid motions of a cube and of an octahedron are isomorphic. ■

Exercise 1.7.23

Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

Solution. The group of rigid motions of a cube has 24 elements, while permutations of the set of three pairs of opposing faces has 6 elements, so the action cannot be faithful as no homomorphism can be injective between finite groups of different sizes (if there was some injective homomorphism, it would imply bijectivity between the two groups of different cardinality, which is impossible).

Consider a cube such that its center is at the origin of $\mathbb{R}^3$ space. Then any rotation around the axes fixes a pair of faces, while sends the other two pairs back to themselves (to visualize this explicitly, consider the cube with vertices $(\pm 1, \pm 1, \pm 1)$ and the z-axis. A rotation around the z-axis would fix the faces $(\pm 1, \pm 1, 1)$ and $(\pm 1, \pm 1, -1)$, while it rotates the pair of faces $(1, \pm 1, \pm 1)$ and $(-1, \pm 1, \pm 1)$ back to each other–these are the faces that vary along the x-axis. One can construct the same for the pair of faces that lie along the y-axis and deduce the same thing). There are exactly 3 of these 180° rotations, so the kernel of this action consists of these rotations and the identity. ■

2 Subgroups

2.1 Definitions and Examples

(1) In each of (a)-(e) prove that the specified subset is a subgroup of the given group:

(a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

(e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Solution. Let G be the group in question and let H be the set that we are trying to prove is a subgroup of G.

(a) Clearly $0 = 0 + 0i \in H$ so that H is nonempty. Suppose $a + ai, b + bi \in H$. Then $a - b \in \mathbb{R}$ so that $(a + ai) - (b + bi) = (a - b) + (a - b)i \in H$ so that $H \leq G$.

(b) Since $|1| = 1$, then $1 \in H$ so that it is nonempty. Suppose $z, w \in H$. Note that $|w^{-1}| = 1$ since $|w^{-1}| = |\overline{w}|/|w|^2 = 1/1 = 1$. Then

$$|zw^{-1}| = |z||w^{-1}| = (1)(1) = 1$$

so that $zw^{-1} \in H$. Then $H \leq G$.

(c) Let $n \in \mathbb{Z}^+$ be fixed. Since $0 = 0/k$ where $k \mid n$, then $0 \in H$ so that it is nonempty. Suppose $a/b, c/d \in H$, where $(a, b) = (c, d) = 1$, and $br = ds = n$ for $r, s \in \mathbb{Z}$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ar}{n} - \frac{cs}{n} = \frac{ar - bs}{n}$$

After reduction, the denominator will still be a divisor of n, so $a/b - c/d \in H$, and $H \leq G$.

(d) Fix $n \in \mathbb{Z}^+$, and note that $0 = 0/1 \in H$ so that H is nonempty. Suppose $a/b, c/d \in H$ such that $(b, n) = (d, n) = 1$. For any prime p such that $p \mid n$, then $p \nmid b$ and $p \nmid d$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

Consider $x = (bd, n)$. Then $p \nmid x$, for otherwise $p \mid bd$ implying that $p \mid b$ or $p \mid d$. Then $x = 1$, and $a/b - c/d \in H$ so that $H \leq G$.

(e) Since $1 = 1^2 = 1/1 \in H$, then H is nonempty. Suppose $a, b \in H$. Then $a^2, b^2 \in \mathbb{Q}$ so that

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \in H$$

then $a/b \in H$, and $H \leq G$. ■

(2) In each of (a)–(e) prove that the specified subset is *not* a subgroup of the given group:

(a) the set of 2-cycles in S_n for $n \geq 3$

(b) the set of reflections in D_{2n} for $n \geq 3$

(c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \mid |x| = n\} \cup \{1\}$

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0

(e) the set of real numbers whose square is a rational number (under addition)

Solution. Let H be the set in question and G be the group.

(a) Note that $(1\ 2), (1\ 3) \in H$, but $(1\ 2)(1\ 3) = (1\ 3\ 2) \notin H$.

(b) $s, sr \in H$, but $s(sr) = r \notin H$ as r is not a reflection.

(c) Let $p \in \mathbb{Z}^+$ such that $p \mid n$. Pick $x \in H$ so that $x^{n/p} \in H$. But $|x^{n/p}| < n$, since $(x^{n/p})^p = x^n = 1$, so H is not closed under the operation.

(d) $1 \in H$, but $1 + 1 = 2 \notin H$.
(e) $\sqrt{2}, \sqrt{3} \in H$, but $(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 \notin H$, so $\sqrt{2} + \sqrt{3} \notin H$. ■

(3) Show that the following subsets of the dihedral group D_8 are actually subgroups:
(a) $\{1, r^2, s, sr^2\}$
(b) $\{1, r^2, sr, sr^3\}$

Solution.
(a)

$\circ$	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

(b)

$\circ$	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	r^2	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

Both tables show closure, since no product is an element outside of the subset. ■

(4) Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Solution. Consider $\mathbb{Z}^+$ and $\mathbb{Z}$ under addition. Then $|\mathbb{Z}^+| = \infty$ and $m+n \in \mathbb{Z}^+$ for any $m, n \in \mathbb{Z}^+$, but $m-n \notin \mathbb{Z}^+$ when $m < n$. Then $\mathbb{Z}^+$ is not a subgroup of $\mathbb{Z}$. ■

(5) Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution. Suppose that there did exist H such that $|H| = n-1$. By Lagrange's Theorem, then $n-1 \mid n$. Then there exists k such that $k(n-1) = kn - k = n$, or that $n = k/(k-1)$. Since $n > 2$, we may safely assume that $k > 2$. Since $n \notin \mathbb{Z}^+$ for any $k > 2$, this contradicts Lagrange's Theorem. ■

(6) Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

Solution. Let $\mathrm{Tor}(G)$ denote the torsion subgroup of G. Since $|1| = 1$, then $1 \in \mathrm{Tor}(G)$. Now suppose $g, h \in \mathrm{Tor}(G)$, and put $|g| = m$ and $|h| = n$ for finite m, n. Then

$$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn} = (g^m)^n((h^{-1})^n)^m = 1^n 1^m = 1$$

so that $gh^{-1} \in \mathrm{Tor}(G)$. Then $\mathrm{Tor}(G) \leq G$.

Now suppose $G = \mathrm{Aut}(\mathbb{R})$ and consider $\mathrm{Tor}(G) = \{f \in \mathrm{Aut}(\mathbb{R}) \mid |f| < \infty\}$. Then $f(x) = -x$ and $g(x) = 1/x$ are both in $\mathrm{Tor}(G)$, since $f^2(x) = g^2(x) = x$, but $f(g(x)) = -1/x \notin \mathrm{Tor}(G)$, since $(f \circ g)^n(x) = (-1)^n x^{(-1)^n} \neq 1$ for any $n \in \mathbb{Z}$. ■

(7) Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is *not* a subgroup of this direct product.

Solution. Since every nonidentity element of $\mathbb{Z}$ has infinite order, then $\mathrm{Tor}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \{(0, x) \mid x \in \mathbb{Z}/n\mathbb{Z}\}$, since every $x \in \mathbb{Z}/n\mathbb{Z}$ has finite order as $\mathbb{Z}/n\mathbb{Z}$ is finite. Moreover, if we let H be the set of elements of infinite order along with the identity $(0,0)$, then $(1,1), (-1,0) \in H$, but $(1,1) + (-1,0) = (0,1) \notin H$ because it belongs to the torsion subgroup. ■

(8) Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Solution. Suppose $H \cup K$ is a subgroup. If $H \subseteq K$, we are done. Now suppose $H \not\subseteq K$. Then there exists $h \in H$ such that $h \notin K$. Let $k \in K$. Then $hk \in H \cup K$. If $hk \in K$, then $hk(k^{-1}) = h \in K$, which is a contradiction. Then $hk \in H$. Then $h^{-1} \in H$ so that $h^{-1}(hk) = k \in H$ so that $K \subseteq H$.

If $H \subseteq K$ then $H \cup K = K$. If $K \subseteq H$, then $H \cup K = H$, both of which are subgroups of G. The result follows. ■

(9) Let $G = \mathrm{GL}_n(F)$, where F is any field. Define

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det(A) = 1\}$$

(called the special linear group). Prove that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$.

Solution. Since $\det(I_n) = 1$, then $I_n \in \mathrm{SL}_n(F)$ so that $\mathrm{SL}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{SL}_n(F)$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \frac{\det(A)}{\det(B)} = \frac{1}{1} = 1$$

so that $AB^{-1} \in \mathrm{SL}_n(F)$. It follows that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$. ■

(10) (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Solution.

(a) Put $L = H \cap K$. Since $1 \in H$ and $1 \in K$, then $1 \in L$ so that L is nonempty. Pick $a, b \in L$. Then $a, b \in H$ and $a, b \in K$. Then $ab^{-1} \in H$ and $ab^{-1} \in K$ so that $ab^{-1} \in L$, hence $L \leq G$.

(b) Let H_i be a subgroup of G with i belonging to an indexing set I. Let

$$H = \bigcap_{i \in I} H_i$$

Since $1 \in H_i$ for all i, then $1 \in H$. Suppose $a, b \in H$. Then $a, b \in H_i$ so that $ab^{-1} \in H_i$ for all $i \in I$. It follows that $ab^{-1} \in H$, hence $H \leq G$. ■

(11) Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

(a) $\{(a, 1) \mid a \in A\}$

(b) $\{(1, b) \mid b \in B\}$

(c) $\{(a, a) \mid a \in A\}$, where we assume $B = A$ (called the diagonal subgroup)

Solution. Let C be the set in each part.

(a) Since $1 \in A$, then $(1, 1) \in C$ so that C is nonempty. Suppose $(a_1, 1), (a_2, 1) \in C$ for $a_1, a_2 \in A$. Then $a_1 a_2^{-1} \in A$. Then

$$(a_1, 1)(a_2, 1)^{-1} = (a_1, 1)(a_2^{-1}, 1) = (a_1 a_2^{-1}, 1) \in C$$

so that $C \leq A \times B$.

(b) See above proof, but suppose $(1, b_1), (1, b_2) \in C$ for $b_1, b_2 \in B$.

(c) $1 \in A$ so $(1, 1) \in C$, and C is nonempty. For $a_1, a_2 \in A$, then $a_1 a_2^{-1} \in A$ so that

$$(a_1, a_1)(a_2, a_2)^{-1} = (a_1 a_2^{-1}, a_1 a_2^{-1}) \in C$$

so that $C \leq A^2$. ■

(12) Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $\{a^n \mid a \in A\}$

(b) $\{a \in A \mid a^n = 1\}$

Solution. Let B be the sets in question.

(a) $1^n = 1$, so $1 \in B$. Suppose $a^n, b^n \in B$. Then

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

where the last equality follows, since A is abelian. Then $ab^{-1} \in B$, hence $B \leq A$.

(b) $1^n = 1$, so $1 \in B$. Suppose $a, b \in B$. Then

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

so that $ab^{-1} \in B$, and $B \leq A$. ■

(13) Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Solution. Let $H \leq \mathbb{Q}$. Then $0 \in H$. If no other element is in H, then $H = 0$ and we are done. Suppose that $H \neq 0$ so that there exists $x = a/b \in H$. Moreover, we may take $x > 0$, because if $x < 0$, take $-x > 0$ instead since H has inverses. Note that $bx = a \in H$ so that $1/a \in H$. Then $a(1/a) = 1 \in H$. Then $\mathbb{Z} \subseteq H$, since we may use 1 to build every integer.

Now suppose $r \in \mathbb{Q}$, and put $r = p/q$ for $p, q \in \mathbb{Z}$. Then $q \in H$ so that $1/q \in H$, hence $p(1/q) = r \in H$. Then $\mathbb{Q} \subseteq H$, and $H = \mathbb{Q}$. ■

(14) Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is *not* a subgroup of D_{2n} (here $n \geq 3$).

Solution. Let H be the set in question. Then $s, sr \in H$, since $|s| = 2$, and $(sr)^2 = s(sr^{-1})r = 1$. But $s(sr) = r \notin H$, because $|r| \geq 3$. ■

(15) Let $H_1 \subseteq H_2 \subseteq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Solution. Let $H = \bigcup_{i=1}^{\infty} H_i$. Since $1 \in H_i$ for all i, then $1 \in H$ so that H is nonempty. Pick $a, b \in H$. Then $a \in H_i$ and $b \in H_j$ for some $i, j \in \mathbb{Z}^+$. Then $a, b \in H_k$, where $k = \max(i, j)$. Then $ab^{-1} \in H_k$ so that $ab^{-1} \in H$, hence $H \leq G$. ■

(16) Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $\mathrm{GL}_n(F)$ (called the group of upper triangular matrices).

Solution. Let $\mathrm{UT}_n(F)$ denote the set of $n \times n$ upper triangular matrices with entries from F. Since I_n has all 0s except the diagonal, then $I_n \in \mathrm{UT}_n(F)$ so that $\mathrm{UT}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{UT}_n(F)$. Since $A, B \in \mathrm{GL}_n(F)$, then $\det(A)$ and $\det(B)$ are nonzero. Putting $AB = C = (c_{ij})$ it follows that $\det(C)$ is also nonzero. Note that

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Suppose $i > j$. Then if $i > k$, then $a_{ik} = 0$, and if $k > j$, then $b_{kj} = 0$ so that $c_{ij} = 0$, hence $C \in \mathrm{UT}_n(F)$.

To show that $A^{-1} \in \mathrm{UT}_n(F)$, put $D \in \mathrm{UT}_n(F)$ such that $AD = DA = I_n$. Proceeding by induction, we show the case for $n = 2$: Consider the matrices

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \quad D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}$$

such that $AD = I_2$. While we may solve for each d_{ij} explicitly, since $D \in \mathrm{GL}_2(F)$, it must be that $d_{ii} \neq 0$, and $d_{12} \in F$, so it remains to show that $d_{21} = 0$. To that end, note that $a_{22}d_{21} = 0$. Since $a_{22} \neq 0$ (otherwise $\det(A) = 0$ and $A \notin \mathrm{GL}_2(F)$), it must be that $d_{21} = 0$, hence $D \in \mathrm{UT}_2(F)$. Suppose now that the inverse D of $A \in \mathrm{GL}_n(F)$ is also upper triangular, and consider $A \in \mathrm{UT}_{n+1}(F)$ and $D \in \mathrm{GL}_{n+1}(F)$ such that $AD = DA = I_{n+1}$. Using block matrices, we may write this as

$$\begin{pmatrix} A_0 & \mathbf{a}_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} D_0 & \mathbf{d}_{12} \\ \mathbf{d}_{21}^T & d_{22} \end{pmatrix} = \begin{pmatrix} D_0 & \mathbf{d}_{12} \\ \mathbf{d}_{21}^T & d_{22} \end{pmatrix} \begin{pmatrix} A_0 & \mathbf{a}_{12} \\ 0 & a_{22} \end{pmatrix} = \begin{pmatrix} I_n & \mathbf{0}_{n\times 1} \\ \mathbf{0}_{n\times 1}^T & 1 \end{pmatrix}$$

where $\mathbf{a}_{12}, \mathbf{d}_{12}, \mathbf{d}_{21}^T, \mathbf{0}_{n\times 1}^T$ are $n \times 1$ column vectors, and $a_{22}, d_{22} \in F$. We can see that $D_0 A_0 = I_n$ so that $D_0 \in \mathrm{UT}_n(F)$ by assumption. Moreover, $a_{22}\mathbf{d}_{21}^T = \mathbf{0}_{n\times 1}^T$. Since $a_{22} \neq 0$ because $A \in \mathrm{UT}_{n+1}(F)$, then $\mathbf{d}_{21}^T = \mathbf{0}_{n\times 1}^T$. By induction, then $D \in \mathrm{UT}_{n+1}(F)$, hence the inverse of any upper triangular matrix is also upper triangular. ■

(17) Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$ is a subgroup of $\mathrm{GL}_n(F)$.

Solution. Let H be the set in question. Since the diagonal of I_n is only 1's, then $I_n \in H$. Suppose $A, B \in H$. By the previous exercise, $A, B \in \mathrm{UT}_n(F)$, so it remains to show that $a_{ii} = b_{ii} = 1$ for all $1 \leq i \leq n$. Then

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}$$

Since $a_{ik} = 0$ for $k < i$ and $b_{ki} = 0$ for $k > i$, then the sum degrades to $a_{ii} b_{ii} = 1$. Then H is closed under multiplication. Moreover, suppose $D \in \mathrm{UT}_n(F)$ such that $DA = I_n$. Then

$$1 = (DA)_{ii} = d_{ii} a_{ii}$$

where we use the above to collapse the ii-th term of DA. Then $d_{ii} = 1$, hence $D \in H$, and H is closed under inverses. Hence, $H \leq \mathrm{GL}_n(F)$. ■

2.2 Centralizers and Normalizers, Stabilizers and Kernels

(1) Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Solution. $g \in C_G(A)$ if and only if $gag^{-1} = a$ if and only if $a = g^{-1}ag$. ■

(2) Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Solution. Recall that $C_G(Z(G)) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in Z(G)\}$. Clearly $C_G(Z(G)) \subseteq G$. Now suppose $g \in G$ and pick $z \in Z(G)$. Then $gz = zg$, or $gzg^{-1} = z$. Then $g \in C_G(Z(G))$, hence $G \subseteq C_G(Z(G))$. It follows that $C_G(Z(G)) = G$. Moreover, because $G = C_G(Z(G)) \leq N_G(Z(G))$ and $N_G(Z(G)) \leq G$ by definition, then $N_G(Z(G)) = 0$. ■

(3) Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution. Pick $g \in C_G(B)$. Then $gbg^{-1} = b$ for all $b \in B$. In particular, $gag^{-1} = a$ for all $a \in A$ because $A \subseteq B$. Then $C_G(B) \subseteq C_G(A)$. Since $C_G(B)$ and $C_G(A)$ are subgroups of G, then $C_G(B) \leq C_G(A)$. ■

(4) For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 1.7.19) simplify your work?

Solution. Note that for any group G, then $C_G(1) = G$ since every element of G commutes with the identity. Now take $a = (1\ 2) \in S_3$. Note that $A = \{1, a\} \leq C_{S_3}(a)$ so that 2 divides $|C_{S_3}(a)|$ by Lagrange's Theorem. Similarly, $|C_{S_3}(a)|$ divides $6 = |S_3|$. Since $(1\ 3) \notin C_{S_3}(a)$ as $a(1\ 3) \neq (1\ 3)a$, and a and $(1\ 3)$ generate S_3, then no other element of S_3 lies in $C_{S_3}(a)$, hence $C_{S_3}(a) = A$. One can use a similar argument to show that $C_{S_3}((1\ 3)) = \{1, (1\ 3)\}$ and $C_{S_3}((2\ 3) = \{1, (2\ 3)\}$. Moving on to the 3-cycles of S_3, let $a = (1\ 2\ 3)$ and consider $A = \{1, a, a^2\}$, where $a \neq a^2$ since $|a| = 3$. It similarly follows that $A \leq C_{S_3}(a)$ so that 3 divides $|C_G(A)|$ and again, $|C_G(a)|$ divides 6. Since $(1\ 2)a \neq a(1\ 2)$, then $(1, 2) \notin C_{S_3}(a)$ so that $|C_{S_3}(a)| = 3$, and $C_{S_3}(a) = A$. Similarly, $C_{S_3}((1\ 3\ 2)) = \{1, (1\ 3\ 2), (1\ 2\ 3)\}$. Lastly, there is no element in S_3 that commutes with other elements of S_3 except for the identity, so $Z(S_3) = 1$.

The following are the centralizers for each element in D_8:

$$\begin{aligned} C_{D_8}(r) &= \{1, r, r^2, r^3\} \\ C_{D_8}(r^2) &= D_8 \\ C_{D_8}(r^3) &= \{1, r, r^2, r^3\} \\ C_{D_8}(s) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(sr) &= \{1, r^2, sr, sr^3\} \\ C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\} \end{aligned}$$

and $Z(D_8) = \{1, r^2\}$. Lastly, the centralizers of Q_8 are

$$\begin{aligned} C_{Q_8}(-1) &= Q_8 \\ C_{Q_8}(i) &= \{1, -1, i, -i\} \\ C_{Q_8}(-i) &= \{1, -1, i, -i\} \\ C_{Q_8}(j) &= \{1, -1, j, -j\} \\ C_{Q_8}(-j) &= \{1, -1, j, -j\} \\ C_{Q_8}(k) &= \{1, -1, k, -k\} \\ C_{Q_8}(-k) &= \{1, -1, k, -k\} \end{aligned}$$

and $Z(Q_8) = \{1, -1\}$. ■

(5) In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Solution.

(a) Since A is generated by (1 2 3), then $A \leq C_G(A)$. By Lagrange's Theorem, then 3 divides $|C_G(A)|$ and $|C_G(A)|$ divides 6. Since (1 2) $\notin C_G(A)$ because (1 2)(1 2 3) $\neq$ (1 2 3)(1 2), then $C_G(A) = A$.

Since $C_G(A) \leq N_G(A)$, check (1 2):

$$(1\ 2)A(1\ 2) = \{(1\ 2)(1\ 2), (1\ 2)(1\ 2\ 3)(1\ 2), (1\ 2)(1\ 3\ 2)(1\ 2)\} = \{1, (1\ 3\ 2), (1\ 2\ 3)\} = A$$

so that (1 2) $\in N_G(A)$. Then $N_G(A) = G$, since (1 2 3)(1 2) = (1 3).

(b) Note that A is a subgroup so that $A \leq C_G(A)$. Then Lagrange's implies that 4 divides $|C_G(A)|$ and 8 divides $|C_G(A)|$. Since $r \notin C_G(A)$, then $|C_G(A)| = 4$ so that $C_G(A) = A$.

Take $r \in G$, so that

$$rAr^{-1} = \{r1r^{-1}, rsr^{-1}, rr^2r^{-1}, rsr^2r^{-1}\} = \{1, sr^2, r^2, s\} = A$$

so that $r \in N_G(A)$. Since $C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$, then 4 divides $|N_G(A)|$ which divides 8. Then $N_G(A) = D_8$.

(c) A is the subgroup of rotations, so 5 divides $|C_G(A)|$ which divides 10. Since $s \notin C_G(A)$ as it doesn't commute with rotations, then $C_G(A) = A$. Moreover,

$$sAs = \{s1s, srs, sr^2s, sr^3s, sr^4s\} = \{1, r^4, r^3, r^2, r\} = A$$

so that $s \in N_G(A)$, hence $N_G(A) = G$. ■

(6) Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Solution.

(a) Fix $h \in H$, and pick $x \in hHh^{-1}$. Then $hxh^{-1} \in H$ since H is closed under inverses and the operation. Moreover, if $x \in H$, then $x \in hHh^{-1}$ by definition so that $hHh^{-1} = H$, hence $h \in N_G(H)$ so that $H \leq N_G(H)$.

Consider the set $G = D_6$ and $H = \{1, r, s\}$. Then $rHr^{-1} = \{1, r, sr\}$ so that $r \notin N_G(H)$, hence $H \not\leq N_G(H)$.

(b) Suppose $H \leq C_G(H)$, and consider any $g, h \in H$. In particular, $g \in G$ so that $ghg^{-1} = h$, or $gh = hg$. Then H is abelian.

If H was abelian, pick $h \in H$. Then for any $g \in H$, we have $hg = gh$, or $hgh^{-1} = g$. Then $h \in C_G(H)$, and $H \leq C_G(H)$. ■

(7) Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = \{1\}$ if n is odd.

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Solution. Instead of solving each problem individually, we proceed as follows: First, we show that every element of $Z(D_{2n})$ must be a rotation. To that end, consider sr^k for some $0 \leq k < n$, and consider $r \in D_{2n}$. Then

$$sr^kr = rsr^k \implies sr^{k+1} = sr^{k-1}$$

so that $r^{k+1} = r^{k-1}$, or $r^2 = 1$, contradicting that $n \geq 3$. Then no reflection lies in $Z(D_{2n})$, hence every element of the center must be a rotation.

Since rotations commute with other rotations, it suffices to check whether an arbitrary rotation r^k commutes with s:

$$r^ks = sr^k \implies r^ks = r^{-k}s$$

so that $r^{2k} = 1$. Since $|r| = n$, then $n \mid 2k$. Hence, $r^k \in Z(D_{2n})$ if and only if $n \mid 2k$.

(a) If n is odd, then $2 \nmid n$. Since $n \mid 2k$, it must be that $n \mid k$. Since $0 \leq k < n$, then $k = 0$ so that $Z(D_{2n}) = \{1\}$.
(b) If $n = 2m$, then $2m \mid 2k$ implies that $m \mid k$. Then $k = 0$ or $k = m = n/2 < n$ so that $Z(D_{2n}) = \{1, r^m\}$. ■

(8) Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Solution. Since $1(i) = i$, then $1 \in G_i$. Let $\sigma, \tau \in G_i$. Then

$$(\sigma \circ \tau^{-1}) \cdot i = \sigma \cdot (\tau^{-1} \cdot i) = \sigma \cdot (\tau^{-1}(i)) = \sigma \cdot i = \sigma(i) = i$$

where $\tau^{-1}(i) = i$ because $\tau \in S_n$ so that τ^{-1} exists. Then $\sigma \circ \tau^{-1} \in G_i$, hence $G_i \leq G$. Moreover, G_i is the set of permutations on $\{1, \ldots, n\}$ such that i is fixed while every other integer may be moved, i.e., $n - 1$ elements may be permuted. Hence, $G_i \cong S_{n-1}$ so that $|G_i| = (n-1)!$. ■

(9) For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Solution. Suppose $g \in N_H(A)$. By definition, $g \in H$. Moreover, $gAg^{-1} = A$ and that $g \in H \leq G$ implies that $g \in N_G(A)$. Hence, $g \in N_G(A) \cap H$.

Suppose $h \in N_G(A) \cap H$. Since $h \in N_G(A)$. then $hAh^{-1} = A$. Moreover, $h \in H$ implies that $h \in N_H(A)$. It follows that $N_H(A) = N_G(A) \cap H$. Since the intersection of two subgroups is a subgroup (see Section 2.1, Exercise 10), then $N_H(A) \leq H$. ■

(10) Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Solution. Since $|H| = 2$, then $H = \{1, h\}$ for some $h \in G$ where $|h| = 2$. Suppose $g \in N_G(H)$. Then $gHg^{-1} = \{gg^{-1}, ghg^{-1}\} = \{1, ghg^{-1}\} = H$. If $ghg^{-1} = 1$, then $h = 1$ which contradicts that $|H| = 2$. Then $ghg^{-1} = h$ so that $g \in C_G(H)$. We have $C_G(H) \leq N_G(H)$ so that $N_G(H) = C_G(H)$.

Now suppose $N_G(H) = G$, It follows that for any $g \in N_G(H) = G$, then $gHg^{-1} = H$. In particular, we have that $ghg^{-1} = h$ for any $h \in H$. Then $gh = hg$ so that $h \in Z(G)$. Hence, $H \leq Z(G)$. ■

(11) Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Solution. Let $g \in Z(G)$. Then $ga = ag$ for any $a \in A$ so that $gag^{-1} = a$. Hence, $gAg^{-1} = A$ so that $Z(G) \subseteq N_G(A)$. ■

(12) Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$ where a is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \tag{$*$}$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables). For example, if $\sigma = (1\,2)(3\,4)$ and $p(x_1, \ldots, x_4)$ is the polynomial in ($*$) above, then

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_4 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_4 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in ($*$) above, let $\sigma = (1\,2\,3\,4)$ and let $\tau = (1\,2\,3)$. Compute $\sigma \cdot p, \tau \cdot (\sigma \cdot p), (\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.
(b) Prove that these definitions give a (left) group action of S_4 on R.
(c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgroup isomorphic to S_3.

(d) Exhibit all permutations in S_4 that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.

(e) Exhibit all permutations in S_4 that stabilize the element $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

(f) Show that the permutations in S_4 that stabilizes the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)

Solution.

(a) Note that $\tau \circ \sigma = (1\ 3\ 4\ 2)$ and $\sigma \circ \tau = (1\ 3\ 2\ 4)$. Then

$$\begin{aligned}
\sigma \cdot p &= 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3 \\
\tau \cdot (\sigma \cdot p) &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3 \\
(\tau \circ \sigma) \cdot p &= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3 \\
(\sigma \circ \tau) \cdot p &= 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4
\end{aligned}$$

(b) Note that $1 \cdot p = p$ for any $p \in R$. Let $\sigma, \tau \in S_4$, then

$$\begin{aligned}
\sigma \cdot (\tau \cdot p(x_1, x_2, x_3, x_4)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)}) \\
&= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, x_{\sigma(\tau(3))}, x_{\sigma(\tau(4))}) \\
&= (\sigma \circ \tau) \cdot p(x_1, x_2, x_3, x_4)
\end{aligned}$$

(c) To stabilize x_4 means that $\sigma(4) = 4$ which are the permutations: 1, (1 2), (1 3), (2 3), (1 2 3), (1 3 2). Note that these correspond to the elements of S_3 so that they are a subgroup of S_4 that is isomorphic to S_3.

(d) If $\sigma \in S_{4_{x_1+x_2}}$, then $\sigma \cdot (x_1 + x_2) = x_1 + x_2$. This occurs in one of three ways: all digits are fixed, 1 and 2 get swapped, or 1 and 2 are the only digits fixed. The first is the identity permutation, the second are the permutations (1 2) and (1 2)(3 4), and the third is (3 4). Since (1 2) and (3 4) are disjoint, they commute with each other and thus the subset $\{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ is an abelian subgroup of S_4 with order 4.

(e) To stabilize $x_1x_2 + x_3x_4$, note that the identity permutation does this. Another way is to maintain the product x_3x_4 but interchange 1 and 2, or the permutation (1 2). Analogously, (3 4) is another permutation by interchanging 3 and 4 but fixing 1 and 2. Alternatively, we may also combine these two permutations as (1 2)(3 4) so that both interchanges occur at the same time. The next way is to interchange the placement of the products themselves, i.e., x_1x_2 in the place of x_3x_4, and vice versa. We obtain two more permutations (1 3)(2 4) and (1 4)(2 3), where 1 takes the place of 3 and 2 the place of 4 in the first product, and the second is explained similarly. Lastly, we may perform these interchanges in one full action, which results in the permutations (1 3 2 4) and (1 4 2 3).

Now consider the mapping $\varphi : S_{4_{x_1x_2+x_3x_4}} \to D_8$ given by the following:

$$\varphi((1\ 2)) = s \quad \text{and} \quad \varphi((1\ 3\ 2\ 4)) = r$$

Since $(1\ 2)^2 = (1\ 3\ 2\ 4)^4 = 1$ and $(1\ 2)(1\ 3\ 2\ 4) = (1\ 3\ 2\ 4)^{-1}(1\ 2)$, then φ is an isomorphism. ■

(13) Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, \ldots, x_n$, i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$ where a is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Prove that this defines a (left) group action of S_n on R.

Solution. Clearly $1 \cdot p(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n)$. Moreover, for $\sigma, \tau \in S_n$, then

$$\begin{aligned}
\sigma \cdot (\tau \cdot p(x_1, x_2, \ldots, x_n)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\
&= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\
&= (\sigma \circ \tau) \cdot p(x_1, x_2, \ldots, x_n)
\end{aligned}$$

Then it is a group action on R. ■

(14) Let $H(F)$ be the Heisenberg group over the field F introduced in Section 1.4, Exercise 11. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Solution. Let $X, Y \in H(F)$ be written as

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

where $X \in Z(H(F))$. Then $XY = YX$, implying that

$$XY = \begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & dc+e+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} = YX$$

Comparing entries, it follows that $af = dc$. Since $d, e, f \in F$ are arbitrary, it follows that this only occurs when $a = c = 0$, for otherwise if at least one of a or c were nonzero, then set f or d to be nonzero respectively to not have equality. Then elements of $Z(H(F))$ must be of the form

$$Z(H(F)) = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H(F) \;\middle|\; x \in F \right\}$$

Moreover, the mapping $\varphi : F \to Z(H(F))$ defined by

$$\varphi(x) = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is clearly an isomorphism, so $Z(H(F)) \cong F$. ■

2.3 Cyclic Groups and Cyclic Subgroups

(1) Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Solution. Recall that the containment relation is the following:

$$\langle x^a \rangle \leq \langle x^b \rangle \iff (b, 45) \mid (a, 45)$$

The subgroups of Z_{45} are:

$$\begin{aligned} Z_{45} = \langle x \rangle &> \langle x^3 \rangle, \langle x^5 \rangle, \langle x^9 \rangle, \langle x^{15} \rangle, 1 \\ \langle x^3 \rangle &> \langle x^9 \rangle, \langle x^{15} \rangle \\ \langle x^5 \rangle &> \langle x^{15} \rangle \\ \langle x^9 \rangle &> 1 \\ \langle x^{15} \rangle &> 1 \\ 1 = \langle x^0 \rangle & \end{aligned}$$

■

(2) If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Solution. For some $x \in G$ where $|x| = |G| = n$, then Proposition 2.2 says that $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of G. Since G has n elements only, it follows that these are the elements of G, hence $G = \langle x \rangle$. Moreover, this is not true if G is infinite, since $|\mathbb{Z}| = |2| = \infty$, but $\langle 2 \rangle$ generates only the even integers. ■

(3) Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Solution. Using Proposition 2.5 and $|\mathbb{Z}/48\mathbb{Z}| = 48$, then $\langle \overline{a} \rangle$ generates $\mathbb{Z}/48\mathbb{Z}$ when $(a, 48) = 1$. We then have $a = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47$. ■

(4) Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Solution. Note that $202 = 2 \cdot 101$, which are both prime numbers. Then its generators is every number between 1 and 202, except 101 and even numbers. ■

(5) Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution. Let φ denote the Euler-φ function. Then

$$\begin{aligned} \varphi(49000) &= \varphi(2^3)\varphi(5^3)\varphi(7^2) \\ &= 2^2(2-1)5^2(5-1)7(7-1) \\ &= 16800 \end{aligned}$$

■

(6) In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Solution. The elements of each subgroup are

$$\begin{aligned} \mathbb{Z}/48\mathbb{Z} = \langle \overline{1} \rangle &= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{46}, \overline{47}\} \\ \langle \overline{2} \rangle &= \{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{44}, \overline{46}\} \\ \langle \overline{3} \rangle &= \{\overline{0}, \overline{3}, \overline{6}, \ldots, \overline{42}, \overline{45}\} \\ \langle \overline{4} \rangle &= \{\overline{0}, \overline{4}, \overline{8}, \ldots, \overline{40}, \overline{44}\} \\ \langle \overline{6} \rangle &= \{\overline{0}, \overline{6}, \overline{12}, \ldots, \overline{36}, \overline{42}\} \\ \langle \overline{8} \rangle &= \{\overline{0}, \overline{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\} \\ \langle \overline{12} \rangle &= \{\overline{0}, \overline{12}, \overline{24}, \overline{36}\} \\ \langle \overline{16} \rangle &= \{\overline{0}, \overline{16}, \overline{32}\} \\ \langle \overline{24} \rangle &= \{\overline{0}, \overline{24}\} \\ \langle \overline{0} \rangle &= \{\overline{0}\} \end{aligned}$$

Moreover, the subgroup inclusions are

$$\begin{aligned}
\langle\bar{1}\rangle &\geq \langle\bar{0}\rangle, \langle\bar{1}\rangle, \langle\bar{2}\rangle, \langle\bar{3}\rangle, \langle\bar{4}\rangle, \langle\bar{6}\rangle, \langle\bar{8}\rangle, \langle\overline{12}\rangle, \langle\overline{16}\rangle, \langle\overline{24}\rangle \\
\langle\bar{2}\rangle &\geq \langle\bar{0}\rangle, \langle\bar{2}\rangle, \langle\bar{4}\rangle, \langle\bar{6}\rangle, \langle\bar{8}\rangle, \langle\overline{12}\rangle, \langle\overline{24}\rangle \\
\langle\bar{3}\rangle &\geq \langle\bar{3}\rangle, \langle\bar{6}\rangle, \langle\overline{12}\rangle, \langle\overline{24}\rangle \\
\langle\bar{4}\rangle &\geq \langle\bar{0}\rangle, \langle\bar{4}\rangle, \langle\bar{8}\rangle, \langle\overline{12}\rangle, \langle\overline{16}\rangle, \langle\overline{24}\rangle \\
\langle\bar{6}\rangle &\geq \langle\bar{0}\rangle, \langle\bar{6}\rangle, \langle\overline{12}\rangle, \langle\overline{24}\rangle \\
\langle\bar{8}\rangle &\geq \langle\bar{0}\rangle, \langle\bar{8}\rangle, \langle\overline{16}\rangle, \langle\overline{24}\rangle \\
\langle\overline{12}\rangle &\geq \langle\bar{0}\rangle, \langle\overline{12}\rangle, \langle\overline{24}\rangle \\
\langle\overline{16}\rangle &\geq \langle 0\rangle, \langle\bar{1}6\rangle \\
\langle\overline{24}\rangle &\geq \langle 0\rangle, \langle\overline{24}\rangle \\
\langle\bar{0}\rangle &\geq \langle\bar{0}\rangle
\end{aligned}$$

■

(7) Let $Z_{48} = \langle x\rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\bar{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.

Solution. The subgroups of Z_{48} are $\langle x\rangle, \langle x^2\rangle, \langle x^3\rangle, \langle x^4\rangle, \langle x^6\rangle, \langle x^8\rangle, \langle x^{12}\rangle, \langle x^{16}\rangle, \langle x^{24}\rangle$, and 1. ■

(8) Let $Z_{48} = \langle x\rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \mapsto x^a$ extend to an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ to Z_{48}?

Solution. Let a such that $(a, 48) = d > 1$, and put $b = 48/d$. Since φ_a is a homomorphism, then

$$\varphi_a(\bar{b}) = \varphi_a(b \cdot \bar{1}) = \varphi_a(\bar{1})^b = x^{ab} = (x^{48})^{a/d} = 1 = \varphi_a(\bar{0})$$

Since $\bar{1} \in \ker(\varphi_a)$, then φ_a is not injective. Now suppose we pick a such that $(a, 48) = 1$. Suppose $\bar{b} = \bar{c}$ in $\mathbb{Z}/48\mathbb{Z}$. Then $b - c = 48k$ for some $k \in \mathbb{Z}$, and

$$\varphi_a(\bar{b}) = \varphi_a(b \cdot \bar{1}) = x^{ab} = x^{ac+48ka} = x^{ac} = \varphi_a(\bar{c})$$

so that φ_a is well-defined when a is relatively prime to 48. Moreover,

$$\varphi_a(\bar{b} + \bar{c}) = x^{a(b+c)} = x^{ab+ac} = x^{ab}x^{ac} = \varphi_a(\bar{b})\varphi_a(\bar{c})$$

so that φ_a is a homomorphism. Now suppose $\varphi_a(\bar{b}) = \varphi_a(\bar{c})$ for $\bar{b}, \bar{c} \in \mathbb{Z}/48\mathbb{Z}$. Then $x^{ab} = x^{ac}$, or $x^{a(b-c)} = 1$. Then $48 \mid a(b - c)$, and since $(a, 48) = 1$, then $48 \mid b - c$ so that $\bar{b} = \bar{c}$, and φ_a is injective. Moreover, $|\mathbb{Z}/48\mathbb{Z}| = |Z_{48}|$ implies that φ_a is also surjective, hence it is an isomorphism. ■

(9) Let $Z_{36} = \langle x\rangle$. For which integers a does the map ψ_a defined by $\psi_a : \bar{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}. Can ψ_a ever be a surjective homomorphism?

Solution. Suppose $\bar{b} = \bar{c}$ for $\bar{b}, \bar{c} \in \mathbb{Z}/48\mathbb{Z}$. Suppose ψ_a is already well-defined. Then $\psi_a(\bar{b}) = \psi_a(\bar{c})$, or $x^{ab} = x^{ac}$, which implies that $x^{a(b-c)} = 1$. Then $36 \mid a(b - c)$, but recall that $48 \mid b - c$. Then $36m = a(b - c)$ and $48n = b - c$ for $m, n \in \mathbb{Z}$, or $36m = 48an$. If we choose b, c such that $n = 1$, then this reduces to $36m = 48a$ so that $36 \mid 48a$. Equivalently, we may reduce by $(36, 48)$ so that $3 \mid 4a$. Since $3 \nmid 4$, it must be that $3 \mid a$ so that ψ_a is well-defined only when $3 \mid a$. Moreover,

$$\psi_a(\bar{b} + \bar{c}) = x^{a(b+c)} = x^{ab}x^{ac} = \psi_a(\bar{b})\psi_a(\bar{c})$$

so that ψ_a is a homomorphism. Lastly, if ψ_a were to be surjective, then x^a must have order 36. But by Proposition 2.5, we have $|x^a| = 36/(36, a)$, and $(36, a) \geq 3$ because $3 \mid a$. Hence, ψ_a can never be surjective. ■

(10) What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle\overline{30}\rangle$.

Solution. By Proposition 2.5, we have $|\bar{1}| = 54$. Then

$$|\overline{30}| = |30 \cdot \bar{1}| = \frac{54}{(54, 30)} = \frac{54}{6} = 9$$

The first element of order 9 in $\mathbb{Z}/54\mathbb{Z}$ is $\bar{6}$, so

$$\langle\overline{30}\rangle = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\}$$

Moreover, the orders are

$$\begin{array}{lll} |\bar{0}| = 1 & |\bar{6}| = 9 & |\overline{12}| = 9 \\ |\overline{18}| = 3 & |\overline{24}| = 9 & |\overline{30}| = 9 \\ |\overline{36}| = 3 & |\overline{42}| = 9 & |\overline{48}| = 9 \end{array}$$

■

(11) Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

Solution. The cyclic subgroups of D_8 are

$$\begin{aligned} \langle 1\rangle &= \{1\} \\ \langle r\rangle = \langle r^3\rangle &= \{1, r, r^2, r^3\} \\ \langle r^2\rangle &= \{1, r^2\} \\ \langle s\rangle &= \{1, s\} \\ \langle sr\rangle &= \{1, sr\} \\ \langle sr^2\rangle &= \{1, sr^2\} \\ \langle sr^3\rangle &= \{1, sr^3\} \end{aligned}$$

Moreover, a proper subgroup that is not cyclic is $\langle r^2, s\rangle = \{1, r^2, s, sr^2\}$. ■

(12) Prove that the following groups are *not* cyclic:

(a) $Z_2 \times Z_2$
(b) $Z_2 \times \mathbb{Z}$
(c) $\mathbb{Z} \times \mathbb{Z}$

Solution.

(a) Put $Z_2 = \langle x\rangle$. We may inspect all four elements:

$$\begin{aligned} \langle(1,1)\rangle &= \{(1,1)\} \\ \langle(x,1)\rangle &= \{(1,1),(x,1)\} \\ \langle(1,x)\rangle &= \{(1,1),(1,x)\} \\ \langle(x,x)\rangle &= \{(1,1),(x,x)\} \end{aligned}$$

No subgroup has order 4, hence no subgroup generates $Z_2 \times Z_2$.

(b) If (a, b) generates $Z_2 \times \mathbb{Z}$, then it must be one of the forms $(1, \pm 1)$ or $(x, \pm 1)$, since $\langle \pm 1\rangle = \mathbb{Z}$. But $(1, \pm 1)$ generates elements whose first component is only 1. If we consider $(x, \pm 1)$, then this also doesn't generate $Z_2 \times \mathbb{Z}$ since $(1, 1) \notin \langle(x, \pm 1)\rangle$.

(c) The only candidates for generators of $\mathbb{Z} \times \mathbb{Z}$ is $(\pm 1, \pm 1)$. But any subgroup generated by $(\pm 1, \pm 1)$ contain elements that differ only in sign as $(x, y) \notin \langle(\pm 1, \pm 1)\rangle$ when $|x| \neq |y|$. ■

(13) Prove that the following pairs of groups are *not* isomorphic:

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$
(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.

Solution.

(a) $(0, x) \in \mathbb{Z} \times Z_2$ has order 2, but no element in $\mathbb{Z}$ has order 2.
(b) Same reason as above. ■

(14) Let $\sigma = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12)$. For each of the following integers a compute σ^a: $a = 13, 65, 626, 1195, -6, -81, -570$, and -1211.

Solution. Since $|\sigma| = 12$, then we know that $\langle\sigma\rangle$ has 12 distinct elements. We may then use the Division Algorithm to reduce the integers to their least residue:

$$\begin{aligned}
\sigma^{13} &= \sigma^{12+1} = \sigma \\
\sigma^{65} &= \sigma^{5(12)+5} = \sigma^5 = (1\,6\,11\,4\,9\,2\,7\,12\,5\,10\,3\,8) \\
\sigma^{626} &= \sigma^{52(12)+2} = \sigma^2 = (1\,3\,5\,7\,9\,11)(2\,4\,6\,8\,10\,12) \\
\sigma^{1195} &= \sigma^{99(12)+7} = \sigma^7 = (1\,8\,3\,10\,5\,12\,7\,2\,9\,4\,11\,6) \\
\sigma^{-6} &= \sigma^{-1(12)+6} = \sigma^6 = (1\,7)(2\,8)(3\,9)(4\,10)(5\,11)(6\,12) \\
\sigma^{-81} &= \sigma^{-7(12)+3} = \sigma^3 = (1\,4\,7\,10)(2\,5\,8\,11)(3\,6\,9\,12) \\
\sigma^{-570} &= \sigma^{-48(12)+6} = \sigma^6 \\
\sigma^{-1211} &= \sigma^{-101(12)+1} = \sigma
\end{aligned}$$

■

(15) Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Solution. If it were cyclic, then all subgroups are also cyclic, by Theorem 2.7. But $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. ■

(16) Assume $|x| = n$ and $|y| = m$. Suppose that x and y *commute*: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true of x and y do *not* commute? Give an example of commuting elements x and y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Solution. Let ℓ be the least common multiple of m and n. Then there exist $a, b \in \mathbb{Z}$ such that $\ell = am = bn$. Then

$$(xy)^\ell = x^\ell y^\ell = x^{bn} y^{am} = 1 \cdot 1 = 1$$

so that by Proposition 2.3, then $|xy|$ divides ℓ. Moreover, this is not true if x and y do not commute. If we consider $r, s \in D_8$, then $|r| = 4$ and $|s| = 2$, but $|rs| = 2$ which 4 does not divide. Lastly, consider $\mathbb{Z}/2\mathbb{Z}$. Then $|\bar{1}| = 2$, but $|\bar{1} + \bar{1}| = |\bar{0}| = 1$. ■

(17) Find a presentation for Z_n with one generator.

Solution. $Z_n = \langle x \mid x^n = 1\rangle$. ■

(18) Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x\rangle$ to h such that $x \mapsto h$.

Solution. Define the map $\varphi : Z_n \to H$ by

$$\varphi(x^k) = h^k$$

We first prove that it is well-defined. If $x^a = x^b$, then $x^{a-b} = 1$ so that $n \mid (a - b)$. Then there exists $c \in \mathbb{Z}$ such that $cn = a - b$, or $a = cn + b$. Then

$$\varphi(x^a) = h^a = h^{cn+b} = h^b = \varphi(x^b)$$

Moreover, let $x^s, x^t \in Z_n$. Then

$$\varphi(x^s x^t) = \varphi(x^{s+t}) = h^{s+t} = h^s h^t = \varphi(x^s)\varphi(x^t)$$

so that φ is a homomorphism. To show uniqueness, suppose $\psi : Z_n \to H$ is another homomorphism such that $\psi(x) = h$. It follows that we need to show $\psi(x^k) = h^k$. Proceeding by induction, we have $\psi(x) = h$ so the base case is established. Assuming it holds for some k, then

$$\psi(x^{k+1}) = \psi(x^k x) = h^k h = h^{k+1}$$

so that $\psi = \varphi$ by induction. ■

(19) Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

Solution. Define the map $\varphi : \mathbb{Z} \to H$ as

$$\varphi(n) = h^n$$

Then $\varphi(1) = h$. Moreover, for any $s, t \in \mathbb{Z}$, then

$$\varphi(s+t) = h^{s+t} = h^s h^t = \varphi(s)\varphi(t)$$

so that φ is a homomorphism. Lastly, if $\psi : \mathbb{Z} \to H$ is another homomorphism such that $\psi(1) = h$, it must satisfy $\psi(n) = \psi(n \cdot 1) = \psi(1)^n = h^n$. ■

(20) Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$, then $|x| = p^m$ for some $m \leq n$.

Solution. If $x^{p^n} = 1$, then Proposition 2.3 says that $|x|$ divides p^n. Since p is prime, then $|x|$ must also be a power of p that is at most n. ■

(21) Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$ but $(1+p)^{p^{n-2}} \not\equiv 1 \bmod p^n$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution. We proceed by induction. For $n = 1$, we have the following:

$$(1+p)^p = \sum_{k=0}^{p} \binom{p}{k} p^k = 1 + p^2 + \sum_{k=2}^{p} \binom{p}{k} p^k$$

where 1 and p^2 are for $k = 0$ and $k = 1$ respectively. Note that for $k \geq 2$, then $\binom{p}{k}$ is divisible by p because dividing by $p!$ by $(p-k)!$ results in $p(p-1)\cdots(p-k+1)$, and $k!$ must divide all other terms but p because p is prime. Then for terms $k \geq 2$, we result in $pm_k p^k$ for $k \geq 2$ where pm_k denotes the expanded binomial coefficient $\binom{p}{k}$, and p^k denotes the other term in the summation. For $k \geq 2$, this results in $p^{k+1}m_k$ so that each term contains at least p^3 and is divisible by p. Thus, $(1+p)^p \equiv 1 \bmod p$, and the base case is established. Moreover, we may write $(1+p)^p = 1 + p^2 + M_1 p^3 = 1 + p^2(1 + M_1 p)$, where $M_1 \in \mathbb{Z}$ corresponds to the rest of the summation terms with subscript 1 corresponding to $n = 1$. Now suppose it holds for some n, or that

$$(1+p)^{p^{n-1}} = 1 + p^n(1 + M_n p)$$

where $M_n \in \mathbb{Z}$ and reduces to 1 mod p^n. Then for $n+1$, we have

$$(1+p)^{p^n} = (1 + p^n(1 + M_n p))^p$$

where we set each side to the power of p. Using the Binomial Theorem, we have

$$(1 + p^n(1 + M_n p))^p = \sum_{j=0}^{p} \binom{p}{j} p^{nj}(1 + M_n p)^j = 1 + p^{n+1}(1 + M_n p) + \sum_{j=2}^{p} \binom{p}{j} p^{nj}(1 + M_n p)^j$$

Note that for $j \geq 2$, we will have terms containing at least $p^{2n} = p^{n+1}p^{n-1}$ times some constant, which reduces to 0 mod p^{n+1}. Moreover, the $j = 1$ term reduces to 0 mod p^{n+1} so that $(1+p)^{p^n} \equiv 1 \bmod p^{n+1}$ so that by the inductive hypothesis, we have $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$. If we put $n-1$, then

$$(1+p)^{p^{n-2}} = 1 + p^{n-1}(1 + M_{n-1}p) = 1 + p^{n-1} + M_{n-1}p^n$$

Taking this mod p^n, we have the left over term $1 + p^{n-1} \neq 1$. Since any element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ must have order that divide $p^{n-1}(p-1)$, we must only check powers of p, since $(1+p)^k = 1 + kp + \cdots \equiv 1 \bmod p^2$ implies that $kp \equiv 0 \bmod p^2$ so that $p \mid k$. Since p^{n-1} results in 1 and p^{n-2} doesn't, it follows that $|1+p| = p^{n-1}$. ■

(22) Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \bmod 2^n$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \bmod 2^n$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution. Like Exercise 21, we will proceed by induction, so we analyze the base case $n = 3$. We have

$$(1+2^2)^2 = 25 \equiv 1 \bmod 2^2$$

so it holds true. Suppose the relationship holds for some n. Before moving on to $n+1$, we may rewrite $(1+2^2)^{2^{n-2}}$ in a better form using the Binomial Theorem:

$$(1+2^2)^{2^{n-2}} = \sum_{k=0}^{2^{n-2}} \binom{2^{n-2}}{k} 2^{2k} = 1 + 2^n + \sum_{k=2}^{2^{n-2}} \frac{2^{n-2}(2^{n-2}-1)\cdots(2^{n-2}-k+1)}{k!} 2^{2k}$$

Evaluating the right most expression for each $k \geq 2$, we notice the following. Using the formula obtained in Section 0.2, Exercise 8, note that the largest power of 2 that $k!$ divides is $k-1$:

$$\sum_{i=1}^{\lfloor \log_2(k) \rfloor} \left\lfloor \frac{k}{2^i} \right\rfloor \leq \sum_{i=1}^{\lfloor \log_2(k) \rfloor} \frac{k}{2^i} = \frac{k}{2} + \frac{k}{4} + \cdots < k$$

Moreover, this value must be an integer. Then it must be at most $k-1$. The numerator contains at least $n-2$ 2's, as the other terms contribute at most another 2, since they are either odd (such as $2^{n-2}-1$), or even (such as $2^{n-2}-2 = 2(2^{n-3}-1)$. Therefore, there are at least $n-2$ 2's in the numerator. Coupling with the 2^{2k} term, there are $2k$ more 2's in the numerator as well. Counting all of these, we have $n-2+2k-(k-1) = n+k-1$. Since we are considering only $k \geq 2$, then $n+k-1 \geq n+2-1 = n+1 > n$ so that each term for $k \geq 2$ contains at least 2^n. We may then rewrite the binomial expansion as

$$(1+2^2)^{2^{n-2}} = 1 + M_n 2^n$$

where M_n is the associated constant for the case n after factoring out 2^n out of each term in the summation $k = 1$ onward. Then for $n+1$, we see that

$$(1+2^2)^{2^{n+1-2}} = (1+M_n 2^n)^2 = 1 + M_n 2^{n+1} + M_n^2 2^{2n} = 1 + 2^n(2M_n + 2^n M_n^2) \equiv 1 \bmod 2^n$$

so that the result holds by the inductive hypothesis. Moreover, if we put $n-1$ in the hypothesis, then

$$(1+2^2)^{2^{n-3}} = 1 + M_n 2^{n-1} \not\equiv 1 \bmod 2^n$$

Using similar reasoning as in Exercise 21, we need only check powers of 2. Moreover, we do not need to check 2^{n-1}, because $5 \equiv 1 \bmod 4$, and if $x \equiv 1 \bmod 4$, this covers half of the order of 2^{n-1}, which is 2^{n-2} (the other half is seen by some $x \equiv 3 \bmod 4$). Since 2^{n-2} results in $1 \bmod 2^n$ and 2^{n-3} does not, it follows that 5 has order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. ∎

(23) Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

Solution. By Theorem 2.7, we must have one subgroup of order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ if it were cyclic. However,

$$(2^n-1)^2 = (-1)^2 \equiv 1 \bmod 2^n$$

and

$$(2^{n-1}+1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \bmod 2^n$$

Since $n \geq 3$, then $2^n - 1 \neq 2^{n-1} + 1$ but both have order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Hence, it cannot be cyclic. ∎

(24) Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show that the elements $gx^i g^{-1}, i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Note that this cuts down some of the work in commuting normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

Solution.

(a) Since $g \in N_G(\langle x \rangle)$, then $g\langle x \rangle g^{-1} = \langle x \rangle$ so that $gxg^{-1} \in \langle x \rangle$. Then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) We first prove $gx^k g^{-1} = (gxg^{-1})^k$ for any $k \in \mathbb{Z}$. $k = 0$ and $k = 1$ is trivial, while $(gxg^{-1})^{-1} = gx^{-1}g^{-1}$ so that proving the result for positive integers will hold true for all integers. To that end, suppose $(gxg^{-1})^k = gx^k g^{-1}$. Then

$$(gxg^{-1})^{k+1} = (gxg^{-1})^k (gxg^{-1}) = gx^{k+1}g^{-1}$$

so that it holds true by induction. Now if $y \in g\langle x \rangle g^{-1}$, then there is some $m \in \mathbb{Z}$ such that $y = gx^m g^{-1} = x^{am}$ so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. Moreover, we know that conjugation is an isomorphism so that $|gxg^{-1}| = |x|$. Then $|g\langle x \rangle g^{-1}| = |\langle x \rangle|$ so that $g\langle x \rangle g^{-1} = \langle x \rangle$. ■

(25) Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem to prove that the same is true for any finite group of order n. (For such k each element has a kth root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

Solution. Fix $k \in \mathbb{Z}$ such that $(k, n) = 1$, where $|G| = n$. Then there exist $a, b \in \mathbb{Z}$ such that $ak + bn = 1$. Pick some $g \in G$, where we note that $g^n = 1$ since G is cyclic with order n. Then

$$\varphi(g^a) = g^{ak} = g^{1-bn} = g(g^n)^{-b} = g$$

so that φ is surjective. ■

(26) Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \bmod n$.

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

Solution.

(a) Suppose $\sigma_a \in \mathrm{Aut}(Z_n)$, and put $d = (n, a)$. Then there are $s, t \in \mathbb{Z}$ such that $n = ds$ and $a = dt$. If $Z_n = \langle x \rangle$, then

$$\sigma_a(x^s) = x^{as} = x^{dst} = x^{nt} = 1 = \sigma_a(1)$$

If $x^s \neq 1$, then $\sigma_a \notin \mathrm{Aut}(Z_n)$ as it would have a non-trivial kernel. It must be that $x^s = 1$, and since $|x| = n$ and $n \mid s$, then $s = n$ so that $d = 1$.

Suppose that $(a, n) = 1$. By the previous exercise, then σ_a is a surjective map. Since Z_n is finite, then σ_a is also bijective. Moreover,

$$\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$$

for some $x, y \in Z_n$. Then σ_a is also a homomorphism, hence $\sigma_a \in \mathrm{Aut}(Z_n)$.

(b) Let $Z_n = \langle x \rangle$. If $\sigma_a = \sigma_b$, then $\sigma_a(x) = \sigma_b(x)$. In particular, $x^a = x^b$, or $x^{a-b} = 1$. By Proposition 2.3, then $n \mid (a - b)$ or $a \equiv b \bmod n$.

If $a \equiv b \bmod n$, then there is some $c \in \mathbb{Z}$ such that $a = b + cn$. Then for any $x^m \in Z_n$, we have

$$\sigma_a(x^m) = x^{am} = x^{(b+cn)m} = x^{bm+cnm} = x^{bm}(x^n)^{cm} = x^{bm} = \sigma_b(x^m)$$

so that $\sigma_a = \sigma_b$.

(c) Let $Z_n = \langle x \rangle$ again, and suppose $\varphi \in \mathrm{Aut}(Z_n)$ where $\varphi(x) = x^k$ for some $k \in \mathbb{Z}$. Then for any $x^m \in Z_n$, we have

$$\varphi(x^m) = \varphi(x)^m = x^{km} = \sigma_k(x^m)$$

so that $\varphi = \sigma_k$.

(d) It is clear for any $x^m \in Z_n$ that

$$\sigma_a(\sigma_b(x^m)) = \sigma_a(x^{bm}) = x^{abm} = \sigma_{ab}(x^m)$$

so that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Part (a) shows that $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\sigma_a \in Z_n$, so we may define the map

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n) \quad \text{where} \quad \overline{a} \mapsto \sigma_a$$

Moreover, the "only if" direction in part (b) shows that ψ is well-defined, and the "if" direction shows that ψ is injective. Also, part (c) shows that ψ is surjective, hence $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(Z_n)$. ■

2.4 Subgroups Generated by Subsets of a Group

(1) Prove that if H is a subgroup of G then $\langle H\rangle = H$.

Solution. It is clear that $H \subseteq \langle H\rangle$ by definition. If $h \in \langle H\rangle$, recall that $\langle H\rangle$ is the intersection of all subgroups that contain H, and H is a subgroup that contains itself. Then $h \in H$ so that $\langle H\rangle \subseteq H$. ■

(2) Prove that if A is a subset of B then $\langle A\rangle \leq \langle B\rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A\rangle = \langle B\rangle$.

Solution. By definition, $\langle B\rangle$ is the smallest subgroup of G that contains B. Hence, it must contain A. Since $\langle A\rangle$ is the smallest subgroup of G that contains A, and $\langle B\rangle$ contains A, it follows that $\langle A\rangle \subseteq \langle B\rangle$. Moreover, take $\langle A\rangle = \{x\}$ and $B = \{x, x^2\}$ in Z_4. Then $A \subset B$, but $\langle A\rangle = \langle B\rangle = Z_4$. ■

(3) Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian.

Solution. Let $g, h \in \langle H, Z(G)\rangle$. Using Proposition 2.9, we may put them as follows:

$$g = g_1^{\epsilon_1} g_2^{\epsilon_2} \dots g_m^{\epsilon_m}, \quad h = h_1^{\delta_1} h_2^{\delta_2} \dots h_n^{\delta_n}$$

where $\epsilon_i = \delta_i = \pm 1$, and $g_i, h_i \in H \cup Z(G)$ for all i. Since both H and $Z(G)$ are abelian, then elements of H and $Z(G)$ commute with each other. Then

$$gh = g_1^{\epsilon_1} \dots g_m^{\epsilon_m} h_1^{\delta_1} \dots h_n^{\delta_n} = h_1^{\delta_1} \dots h_n^{\delta_n} g_1^{\epsilon_1} \dots g_m^{\epsilon_m} = hg$$

so that $\langle H, Z(G)\rangle$ is abelian. Moreover, put $G = D_8$ and $H = \{1, r^2\}$. Since $H \subseteq Z(D_8)$, then $C_G(D_8) = D_8$, which is not abelian. ■

(4) Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Solution. If $H = \{1\}$, then $H - \{1\}$ is empty so that $\langle H - \{1\}\rangle = \{1\}$. Suppose $|H| > 1$, and let $h \in H$ that is not the identity. Then $h^{-1} \in H$ so $1 = hh^{-1} \in \langle H - \{1\}\rangle$ so that $H \leq \langle H - \{1\}\rangle$. Moreover, $1 \in \langle H - \{1\}\rangle$ and $\langle H - \{1\}\rangle$ being the minimal set to contain $H - \{1\}$ (now equipped with 1) must also be in H. Then $H = \langle H - \{1\}\rangle$. ■

(5) Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Solution. Consider the 2-cycles (1 2) and (1 3). Then

$$\begin{aligned}(1\,2)(1\,3) &= (1\,3\,2)\\ (1\,3)(1\,2) &= (1\,2\,3)\\ (1\,3\,2)(1\,2) &= (2\,3)\end{aligned}$$

so that $\langle (1\,2), (1\,3)\rangle = S_3$. One can also do similar calculations to ensure $\langle (1\,2), (2\,3)\rangle = \langle (1\,3), (2\,3)\rangle = S_3$. ■

(6) Prove that the subgroup of S_4 generated by (1 2) and (1 2)(3 4) is a noncyclic group of order 4.

Solution. Let $a = (1\,2)$ and $b = (3\,4)$. Then $\langle a, ab\rangle = \{1, a, b, ab\}$ where $ab = ba$ since they are disjoint cycles. Moreover, $|a| = |b| = |ab| = 2$ so that it is noncyclic. ■

(7) Prove that the subgroup of S_4 generated by (1 2) and (1 3)(2 4) is isomorphic to the dihedral group of order 8.

Solution. Put $\alpha = (1\,2)$ and $\beta = (1\,3)(2\,4)$. Then $\gamma = \alpha\beta = (1\,3\,2\,4)$. Since $|\gamma| = 4$, then $\alpha\beta$ maps to $r \in D_8$. Moreover, for some $\delta \in \langle \alpha, \beta\rangle$ to map to s, it must be that $\alpha\beta\delta = \delta(\alpha\beta)^{-1} = \delta\beta\alpha$, where $\alpha\beta = \beta\alpha$ since $|\alpha| = |\beta| = 2$. By inspection, $\delta = \alpha$, hence α and γ satisfies $r^4 = s^2 = 1$. Then there is a homomorphism $\varphi : D_8 \to \langle \alpha, \beta\rangle$ given by

$$\varphi(s^i r^j) = \alpha^i (\alpha\beta)^j, \quad \text{where } i \in \{0, 1\}, j \in \{0, 1, 2, 3\}$$

Since γ, γ^2, and γ^3 are distinct elements, then φ is injective. Moreover, since $\gamma\alpha = \alpha\gamma^{-1} \in \langle \alpha, \beta\rangle$, then any product of α and β can be reduced to $\alpha^i(\alpha\beta)^j$ so that φ is surective. Since its bijective, then φ is an isomorphism, hence $D_8 = \langle \alpha, \beta\rangle$. ■

(8) Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\rangle$.

Solution. Let $A = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\rangle$ where $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (1\ 2\ 4\ 3)$. Then $\alpha\beta = (1\ 3\ 2)$, which has order 3. Then $|\langle \alpha\beta\rangle| = 3$ and is a subgroup of A so that 3 and 4 divide $|A|$. Since $A \leq S_4$, then $|A|$ divides 24 as well. Then $|A| = 12$ or 24. Note that $\alpha^2 = (1\ 3)(2\ 4)$, and we obtain $(1\ 2)$ as follows: First, note that α^2 is two disjoint 2-cycles, while β is a 4-cycle that "disrupts" the symmetry/order of powers of α. In particular, by disrupting α^2 with β, we will result in a smaller cycle, where our goal is to obtain a 2-cycle. We compute $\beta\alpha^2 = (2\ 3)$. Secondly, recall the process of conjugation. Conujugating a 2-cycle by a permutation sends the elements of the 2-cycle to the corresponding integer in the permutation, i.e., $\alpha(i\ j)\alpha^{-1} = (\alpha(i)\ \alpha(j))$, where this is verified because $(\alpha(i\ j)\alpha^{-1})(x)$ for some $x \neq i$ nor j is just the identity map. Our goal is to get $(1\ 2)$, so we need to conjugate $(2\ 3)$ by some permutation such that 2 is sent to 1, and 3 is sent to 2. Observe that the permutation that does this is $\alpha^{-1} = \alpha^3$, so that $\alpha^3(2\ 3)\alpha = (1\ 2)$, i.e., $\alpha^3\beta\alpha^2\alpha = \alpha^3\beta\alpha^3 = (1\ 2)$. Then $(1\ 2) \in \langle \alpha, \beta\rangle$ so that by the previous exercise, A has a subgroup of order 8, hence $|A| = 24$. Then $A = S_4$. ■

(9) Prove that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1 You may assume this subgroup has order 24—this will be an exercise in Section 3.2.]

Solution. Let

$$A = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \quad B = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

Since we know that $\mathrm{SL}_2(\mathbb{F}_3)$ has order 24, we need to exhibit at least 13 distinct matrices using A and B, since $\langle A, B\rangle$ divides 24. Since I, A, and B are 3 distinct matrices, we compute 10 more:

$$A^2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} \qquad B^2 = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$$
$$AB = \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix} \qquad BA = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$$
$$(AB)^2 = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} \qquad ABA^2 = \begin{pmatrix}2 & 2\\ 1 & 0\end{pmatrix}$$
$$A^2B = \begin{pmatrix}0 & 2\\ 1 & 1\end{pmatrix} \qquad B^2A = \begin{pmatrix}1 & 1\\ 2 & 0\end{pmatrix}$$
$$ABA = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} \qquad BAB = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$$

Hence $\langle A, B\rangle = 24$ so that $\langle A, B\rangle = \mathrm{SL}_2(\mathbb{F}_3)$. ■

(10) Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ and $\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]

Solution. Let

$$A = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \quad B = \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Doing some calculations, we see that $A^2 = B^2 = -I$. Moreover, letting $C = AB$, we also see that $C^2 = ABC = -I$. Moreover, I and $-I$ commute with A, B, and C. Since this satisfies the presentation given in Section 1.5, Exercise 3, then there is a surjective homomorphism $\varphi : Q_8 \to \langle A, B\rangle$ given by

$$\varphi(i) = A, \quad \varphi(j) = B, \quad \varphi(k) = AB$$

Moreover, $|\langle A, B\rangle| \leq 8$ since $|Q_8| = 8$, and $|Q_8| = |\langle A, B\rangle|$ because $I, -I, A, B, C \in \langle A, B\rangle$ are all distinct so that φ is injective. Then $Q_8 \cong \langle A, B\rangle$. ■

(11) Show that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Solution. Recall that Q_8 and S_4 both have 6 elements of order 4. However, no two elements in Q_8 can generate the entirety of $\mathrm{SL}_2(\mathbb{F}_3)$ since $|Q_8| = 8$, while $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3)\rangle$, hence they cannot be isomorphic. ■

(12) Prove that the subgroup of upper triangular matrices in $\mathrm{GL}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8. (First find the order of this subgroup.)

Solution. Let $\mathrm{UT}_3(\mathbb{F}_2)$ denote the given subgroup. Moreover, refer to each matrix in $\mathrm{UT}_3(\mathbb{F}_2)$ as (a, b, c), where these are the entries above the diagonals of 1 in the matrix (each entry on the diagonal must be 1, for otherwise we would have 0 which would mean determinant of 0, hence uninvertible). Since each of a, b, c can be 0 or 1, then there are $2^3 = 8$ elements in $\mathrm{UT}_3(\mathbb{F}_2)$.

For a matrix $A = (a, b, c) \in \mathrm{UT}_3(\mathbb{F}_2)$ to be mapped to $r \in D_8$, it must be that $A^4 = I$. Note that $A^2 = (2a, ac + 2b, 2c) = (0, ac, 0)$ so that $A^4 = (0, 2ac, 0) = I$. We must then choose a, c such that they are not 0 mod 2 after being multiplied once; the choice is $a = c = 1$, while b can be anything, so set $A = (1, 0, 1)$. Moreover, for $B = (d, e, f) \in \mathrm{UT}_3(\mathbb{F}_2)$ to map to s, it must be that $AB = BA^{-1} = BA^3$, or $(1, 0, 1)(d, e, f) = (d, e, f)(1, 1, 1)$. We find that

$$(1, 0, 1)(d, e, f) = (1 + d, e + f, 1 + f) = (1 + d, 1 + d + e, 1 + f) = (d, e, f)(1, 1, 1)$$

The only relevant equality is $e + f = 1 + d + e$, which implies $f = 1 + d$. Then d and f must be different, while e can be any element, so put $B = (1, 0, 0)$. Since $A^4 = B^2 = I$, then we have a homomorphism $\varphi : D_8 \to \mathrm{UT}_3(\mathbb{F}_2)$ given by

$$\varphi(r) = A, \quad \varphi(s) = B$$

It is easy to see that none of A, A^2, A^3 are distinct nor is equal to B, so $B \notin \langle A\rangle$ and $|\langle A\rangle| = 4$. Then $\langle A, B\rangle = \mathrm{UT}_3(\mathbb{F}_2)$ so that φ is surjective. Moreover, $|\langle A, B\rangle| = |D_8|$, hence φ is injective. Then $D_8 \cong \mathrm{UT}_3(\mathbb{F}_2)$. ■

(13) Prove that the multiplicative group of positive rational numbers is generated by the set $\{1/p \mid p \text{ is prime}\}$.

Solution. Let P denote the set in question. Note that for any $1/p \in P$, then $(1/p)^{-1} = p \in P$, and any powers are also in P. Take any $m, n \in \mathbb{Q}$ such that $(m, n) = 1$. Using the Fundamental Theorem of Arithmetic, m and n have prime factorizations so they can be written as a product of primes. Then $m/n \in \langle P\rangle$, so $\langle P\rangle = \mathbb{Q}^+$. ■

(14) A group H is called *finitely generated* if there is a finite set A such that $H = \langle A\rangle$.

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle 1/k\rangle$, where k is the product of all denominators appearing in a set of generators for H.]

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution.

(a) Any finite group G is generated by $\langle G\rangle$.

(b) $\mathbb{Z} = \langle 1\rangle$.

(c) Let $H = \langle A\rangle$, where

$$A = \left\{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n}\right\}$$

where $(p_i, q_i) = 1$ for all $1 \leq i \leq n$. Then every element $h \in H$ is of the form

$$h = \sum_{i=1}^{n} a_i \frac{p_i}{q_i}, \quad a_i \in \mathbb{Z}$$

since $\mathbb{Q}$ is abelian. Define the quantities

$$k = \prod_{i=1}^{n} q_i, \quad k_j = k/q_j$$

so that k is the product of all denominators in A, and k_j is the product of all denominators except the denominator in the j-th fraction of A. We may then rewrite h as

$$h = \frac{1}{k}\sum_{i=1}^{n} a_i p_i k_i$$

so that $h \in \langle 1/k \rangle$, which is a cyclic subgroup of $\mathbb{Q}$. Then $H \leq \langle 1/k \rangle$, hence it is cyclic.

(d) Suppose $\mathbb{Q}$ was finitely generated. Then $\mathbb{Q} = \langle p/q \rangle$ where $(p, q) = 1$, by the previous part. Let $r \in \mathbb{Z}$ such that r does not divide q. Then there is some $n \in \mathbb{Z}$ such that

$$n\frac{p}{q} = \frac{1}{r}$$

Then $q = npr$, contradicting that r doesn't divide q. ■

(15) Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Solution. By the previous exercise, such a subgroup cannot be finitely generated. Consider the set

$$A = \left\{ \frac{1}{2^k} \middle| k \in \mathbb{Z}^+ \cup \{0\} \right\}$$

where $\langle A \rangle \leq \mathbb{Q}$. Note that $\langle A \rangle < \mathbb{Q}$ since $1/3 \notin \langle A \rangle$. Moreover, if $\langle A \rangle = \langle p/q \rangle$, then $q = 2^m$ since every element of A has a power of 2. Then $2^{m+1} \notin \langle p/q \rangle$, but $2^{m+1} \in \langle A \rangle$, hence $\langle A \rangle$ cannot be cyclic. ■

(16) A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Solution.

(a) If H is maximal, then we are done. If not, there exists a subgroup $H_1 < G$ such that $H < H_1$. If H_1 is maximal, we are done, but if not, then there must be another subgroup such that $H_1 < H_2$. Continuing on, we can create a chain of subgroups H_i such that $H_i < H_{i+1}$. Since G is finite, the process of creating subgroups must terminate at some k. Then $H_k < G$ is a maximal subgroup that contains H.

(b) Note that $s \notin \langle r \rangle$ so that $\langle r \rangle$ is a proper subgroup of D_{2n}. If $\langle r \rangle$ was not maximal, there must exist some H such that $\langle r \rangle < H$ so that some reflection $sr^k \in H$ for some $1 \leq k < n$. Note that $r^{n-k} \in H$ so that $sr^k r^{n-k} = s \in H$. But then $H = D_{2n}$, contradicting that $H < D_{2n}$. It must be that $\langle r \rangle$ is maximal.

(c) Suppose H is maximal, and put $H = \langle x^k \rangle$ and $d = (n, k)$. Note that $d > 1$ for the subgroup to be proper. Let p be a prime that divides n. If $k = p$, then we are done. If $k \neq p$, consider $\langle x^p \rangle$. Then $H < \langle x^p \rangle$ since $p \mid d$. Since H is maximal, then $\langle x^p \rangle = G$. Then $(p, n) = 1$, but this contradicts that $p \mid n$. Then $k = p$.

Suppose that $H = \langle x^p \rangle$ for prime $p \mid n$. If H is not maximal, there exists $\langle x^d \rangle$ such that $d \mid p$. Since p is prime, then either $d = 1$ or p. If $d = 1$, then $\langle x^d \rangle = G$ which shows that $\langle x^d \rangle$ is not a proper subgroup of G. If $d = p$, then $\langle x^d \rangle = \langle x^p \rangle$ so that H is not a proper subgroup of $\langle x^d \rangle$. It follows that H is maximal. ■

(17) This is an exercise involving Zorn's Lemma. Prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated group, say $G = \langle g_1, g_2, \ldots, g_n \rangle$, and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let C be a chain in $\mathcal{S}$.

(a) Prove that the union H of all the subgroups in C is a subgroup of G.

(b) Prove that H is a proper subgroup.

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Solution.

(a) Let $C \subseteq \mathcal{S}$ be a chain. Put

$$H = \bigcup_{K \in C} K$$

Since at least one subgroup is in C and subgroups are nonempty, then C is nonempty. Suppose $g, h \in H$. Then $g \in K_1$ and $h \in K_2$ for some $K_1, K_2 \in C$ such that $K_1 \leq K_2$ or $K_2 \leq K_1$, or both. Without loss of generality, suppose $K_1 \leq K_2$. Then $g \in K_2$ as well so that $gh^{-1} \in K_2 \subseteq H$. Then $H \leq G$.

(b) If H was not a proper subgroup, then H must contain all generators g_i. Associate each generator with a (not necessarily distinct) subgroup K_i so that $g_i \in K_i$ for every $1 \leq i \leq n$. Since C is a chain, then we may order the subgroups such that $K_j \leq K_{j+1}$ for all $1 \leq j \leq n-1$. It follows that K_n contains every generator g_i so that $K_n = G$, contradicting that C is a chain of proper subgroups of G.

(c) Because G is nontrivial, then $\{1\} \in \mathcal{S}$ so that $\mathcal{S}$ is nonempty. Moreover, $H \in \mathcal{S}$ by the previous part, and for any $K \in C$, we have $K \leq H$ so that H is an upper bound for C. Then every chain in $\mathcal{S}$ has an upper bound, so by Zorn's Lemma, $\mathcal{S}$ must have a maximal element. ∎

(18) Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^kth roots of unity). Prove:

(a) $H_k \leq H_m$ if and only if $k \leq m$.

(b) H_k is cyclic for all k.

(c) Every proper subgroup of Z equals H_k for some k. In particular, every proper subgroup of Z is finite and cyclic.

(d) Z is not finitely generated.

Solution.

(a) Note that $|H_k| = p^k$ for any k as there are exactly p^k roots of unity. Now, if $H_k \leq H_m$, then $p^k \mid p^m$ by Lagrange's Theorem. Then $p^k \leq p^m$, or $k \leq m$ since $p > 0$.

If $k \leq m$, then $p^k \leq p^m$. In particular, $p^k \mid p^m$. Then for any $z \in H_k$, we have

$$z^{p^m} = (z^{p^k})^{p^{m-k}} = 1$$

so that $z \in H_m$. Then $H_k \leq H_m$.

(b) Let $\theta = e^{2\pi i/p^k}$. Note that $\langle\theta\rangle$ has order p^k, and $\langle\theta\rangle \subseteq H_k$. Now for some $z \in H_k$, we have $z = e^{2\pi i x/p^k}$ for some $0 \leq x < p^k$. Then $z = (e^{2\pi i/p^k})^x \in \langle\theta\rangle$ so that $\langle\theta\rangle = H_k$.

(c) Let H be a proper subgroup of Z. Note that every element in Z has order p^i for some $i \in \mathbb{Z}^+$, so elements of H will have similar orders. Define the set

$$S = \{n \in \mathbb{Z}^+ \mid |h| = p^n \text{ for some } h \in H\}$$

so that S is the set of integers n such that H contains a p^n–th root of unity. Moreover, H is trivially nonempty if we define $H_0 = \{z \in Z \mid z^{p^0} = z = 1\}$ so that the trivial proper subgroup $\{1\}$ of Z allows $1 \in H$.

Suppose now that S is infinite. For any $n \in \mathbb{Z}^+$, there exists $h \in H$ and $m \in \mathbb{Z}^+$ such that $|h| = p^m > p^n$, for otherwise it would be that every $h \in H$ has order $|h| \leq p^n$, meaning that n is an upper bound for S. Then $|h| = p^m$ so that $H_m = \langle h\rangle$, and $H_m \leq H$. Since $H_n \leq H_m$ for every $n \in \mathbb{Z}^+$, then

$$Z = \bigcup_{n \in \mathbb{Z}^+} H_n \subseteq H$$

which shows $Z \leq H$. But $H \leq Z$, hence $Z = H$, which contradicts that $Z = H$. It must be that S is finite, so it has some maximal element s. Because $s \in S$, then there is $h_0 \in H$ where $|h_0| = p^s$ so that $H_s = \langle h_0\rangle \leq H$. Suppose $h \in H$ with $|h| = p^k$ for some $k \in \mathbb{Z}^+$. Then $k \in S$ where $k \leq s$ so that $H_k \leq H_s$. Since $h \in H_k$, then $h \in H_s$ so $H \leq H_s$. Hence, $H = H_s$.

(d) Put $Z = \langle z_1, z_2, \ldots, z_n\rangle$ for some $n \in \mathbb{Z}^+$ such that $|z_i| = p^{x_i}$. Let $x = \max(x_1, x_2, \ldots, x_n)$. Then $z_i \in H_x$ for every $1 \leq i \leq n$ so that $Z \leq H_x$. But recall that Z comprises every p-power roots of unity so that $H_x \leq H_x$, contradicting part (a). It must be that Z is infinitely generated. ∎

(19) A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$.

(a) Prove that the additive group of rational numbers $\mathbb{Q}$ is divisible.

(b) Prove that no finite abelian group is divisible.

Solution.

(a) Suppose $p/q \in \mathbb{Q}$. Then $(p/qn)n = p/q$, where $p/qn \in \mathbb{Q}$.

(b) Suppose we have a finite abelian group G with $|G| = n$. Pick some nonidentity $g \in G$. Then there is no such $h \in$ where $h^n = g$, since $h^n = 1$. ■

(20) Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible.

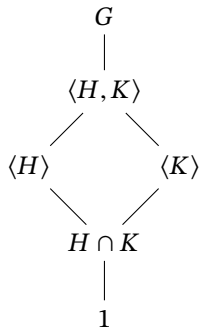
Solution. Suppose $A \times B$ is divisible, and let $a \in A, b \in B$, and $k \in \mathbb{Z}^+$. Then there exists $(c, d) \in A \times B$ such that $(c, d)^k = (c^k, d^k) = (a, b)$. But then $c^k = a$ and $d^k = b$ so that A and B are divisible.

If A and B are both divisible, pick $(a, b) \in A \times B$ and let $k \in \mathbb{Z}^+$. Then there exists $c \in A$ and $d \in B$ such that $c^k = a$ and $d^k = b$. Then $(c, d)^k = (c^k, d^k) = (a, b)$ so that $A \times B$ is divisible. ■

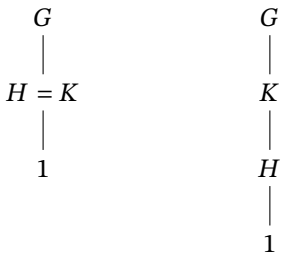
2.5 The Lattice of Subgroups of a Group

(1) Let H and K be subgroups of G. Exhibit all possible sublattices which show only $G, 1, H, K$ and their joins and intersections. What distinguishes the different drawings?

Solution. If H and K are distinct with nontrivial intersection and properly contained in their join, then we have the following lattice:



Remaining scenarios include if $H = K$ or if $H \leq K$ (or the other way), in which case $\langle H, K\rangle = H \cap K$ or $\langle H, K\rangle = H$ and $H \cap K = K$ respectively:



In further scenarios, we may have that some of the groups are trivial. ■

(2) In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.

(a) Subgroups that are contained in $\langle sr^2, r^4\rangle$

(b) Subgroups that are contained in $\langle sr^7, r^4\rangle$

(c) Subgroups that contain $\langle r^4\rangle$

(d) Subgroups that contain $\langle s\rangle$.

Solution.

(a) $\langle sr^2, r^4\rangle, \langle sr^6\rangle, \langle sr^2\rangle, \langle r^4\rangle, 1$.

(b) Note $sr^7 = sr^3$, so $\langle sr^3, r^4\rangle, \langle r^4\rangle, \langle sr^3\rangle, \langle sr^7\rangle, 1$.

(c) $\langle r^4\rangle, \langle sr^2, r^4\rangle, \langle s, r^4\rangle, \langle r^2\rangle, \langle sr^3, r^4\rangle, \langle sr^5, r^4\rangle, \langle s, r^2\rangle, \langle r\rangle, \langle sr, r^2\rangle, D_{16}$.

(d) $\langle s\rangle, \langle s, r^4\rangle, \langle s, r^2\rangle, D_{16}$. ■

(3) Show that the subgroup $\langle s, r^2\rangle$ of D_8 is isomorphic to V_4.

Solution. Note $V_4 = \{1, a, b, c\}$ and $\langle s, r^2\rangle = \{1, s, r^2, sr^2\}$, and that both groups are abelian and of order 4. Define the mapping $\varphi : \langle s, r^2\rangle \to V_4$ given by

$$\varphi(1) = 1, \quad \varphi(s) = a, \quad \varphi(r^2) = b, \quad \varphi(sr^2) = c$$

To check φ is a homomorphism, note that it is sufficient to check the squares of all elements and all pairs of elements:

$$\begin{aligned}
\varphi(s^2) = \varphi(1) = 1 = c^2 = \varphi(s)^2 \\
\varphi(sr^2) = c = ab = \varphi(s)\varphi(r^2) \\
\varphi(r^4) = \varphi(1) = 1 = b^2 = \varphi(r^2)^2 \\
\varphi(ssr^2) = \varphi(r^2) = b = ac = \varphi(s)\varphi(sr^2) \\
\varphi((sr^2)^2) = \varphi(1) = 1 = c^2 = \varphi(sr^2)^2 \\
\varphi(r^2sr^2) = \varphi(s) = a = bc = \varphi(r^2)\varphi(sr^2)
\end{aligned}$$

so that φ is indeed a homomorphism. This is necessarily bijective so that $\langle s, r^2\rangle \cong V_4$. ■

(4) Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).

Solution. Note that $D_8 = \langle s, r\rangle$. Moreover, $s \neq rs$, and $r \in \langle s, rs\rangle$ so that $\langle s, rs\rangle = D_8$. Since $r = r^3$, we also have $\langle s, r^3\rangle = D_8$. We may also replace the reflection s with sr^2, since combinations of a reflection with an

odd rotation and a reflection with an even rotation contain r and thus generates D_8. It follows that the pairs of elements that generate D_8 are:

$$\langle s, r\rangle, \langle s, r^3\rangle, \langle s, rs\rangle, \langle s, r^3s\rangle, \langle r^2s, r\rangle, \langle r^2s, r^3\rangle, \langle r^2s, rs\rangle, \langle r^2s, r^3s\rangle, \langle r, rs\rangle, \langle r^3, rs\rangle, \langle r, r^3s\rangle, \langle r^3, r^3s\rangle$$ ■

(5) Use the given lattice to find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s\rangle$ (there are 8 such elements x).

Solution. Note that $\langle r\rangle = \langle r^3\rangle = \langle r^5\rangle = \langle r^7\rangle$. We then pair each generator with an s so that we obtain just the rotation to then generate D_{16}: $x = r, r^3, r^5, r^7, sr, sr^3, sr^5, sr^7$. ■

(6) Use the given lattices to help find the centralizers of every element in the following groups:

(a) D_8

(b) Q_8

(c) S_3

(d) D_{16}.

Solution.

(a) To calculate the centralizer of an element a, start with the cyclic subgroup that contains a and see if any other elements are contained in $\langle a\rangle$. For example, to calculate $C_{D_8}(rs)$, start with $\langle rs\rangle$ in the subgroup lattice. Since $r^4, sr^5 \in C_{D_8}(rs)$, then $C_{D_8}(rs) \leq \langle sr^5, r^4\rangle$. Checking the next subgroup, it follows that $r^2 \in C_{D_8}(rs)$ so that $C_{D_8}(rs) \leq \langle rs, r^2\rangle$. Since $r \notin C_{D_8}(rs)$, then $C_{D_8}(rs) \neq D_{16}$ so that $C_{D_8}(rs) = \langle rs, r^2\rangle$. We use similar reasoning to deduce the other centralizers:

$$\begin{aligned} C_{D_8}(1) &= D_8 \\ C_{D_8}(r) &= \langle r\rangle \\ C_{D_8}(r^2) &= D_8 \\ C_{D_8}(r^3) &= \langle r\rangle \\ C_{D_8}(s) &= \langle s, r^2\rangle \\ C_{D_8}(rs) &= \langle rs, r^2\rangle \\ C_{D_8}(r^2s) &= \langle s, r^2\rangle \\ C_{D_8}(r^3s) &= \langle sr, r^2\rangle \end{aligned}$$

(b) Note that $1, -1 \in Z(Q_8)$, while none of i, j, and k commute with anything but themselves. Then:

$$\begin{aligned} C_{Q_8}(1) = C_{Q_8}(-1) &= Q_8 \\ C_{Q_8}(i) = C_{Q_8}(-i) &= \langle i\rangle \\ C_{Q_8}(j) = C_{Q_8}(-j) &= \langle j\rangle \\ C_{Q_8}(k) = C_{Q_8}(-k) &= \langle k\rangle \end{aligned}$$

(c) Since no element in S_3 commutes with each other, then $C_{S_3}(a) = \langle a\rangle$ for all $a \in S_3 - \{1\}$, where $C_{S_3}(1) = S_3$.

(d) Use similar reasoning as in part (a) to obtain the centralizers:

$$\begin{aligned} C_{D_{16}}(1) = C_{D_{16}}(r^4) &= D_{16} \\ C_{D_{16}}(r^k) &= \langle r\rangle \text{ for all } k = 1, 2, 3, 5, , 6, \\ C_{D_{16}}(s) = C_{D_{16}}(sr^4) &= \langle s, r^4\rangle \\ C_{D_{16}}(sr) = C_{D_{16}}(sr^5) &= \langle sr^5, r^4\rangle \\ C_{D_{16}}(sr^2) = C_{D_{16}}(sr^6) &= \langle sr^2, r^4\rangle \\ C_{D_{16}}(sr^3) = C_{D_{16}}(sr^7) &= \langle sr^3, r^4\rangle \end{aligned}$$ ■

(7) Find the center of D_{16}.

Solution. $Z(D_{16}) = \{1, r^4\}$ by Section 2.2, Exercise 7. ■

(8) In each of the following groups find the normalizer of each subgroup:
   (a) S_3
   (b) Q_8.

Solution.

(a) Note that every subgroup of S_3 is maximal with the exception of the trivial subgroup, so it follows that $N_{S_3}(\langle\alpha\rangle) = \langle\alpha\rangle$ or S_3 for all $\alpha \in S_3 - \{1\}$. To that end, we have $N_{S_3}(1) = S_3$. Also, for $(1\ 2) \in S_3$, then $(1\ 3)(1\ 2)(1\ 3) \neq (1\ 2)$ so that $(1\ 3) \notin N_{S_3}(\langle(1\ 2)\rangle)$. Then $N_{S_3}(\langle(1\ 2)\rangle) = \langle(1\ 2)\rangle$. Using similar reasoning with the two other 2-cycles, we conclude that $N_{S_3}(\langle\alpha\rangle) = \langle\alpha\rangle$ when α is a 2-cycle. For $\langle(1\ 2\ 3)\rangle$, note that

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2), \quad (1\ 2)(1\ 3\ 2)(1\ 2) = (1\ 2\ 3)$$

so that $(1\ 2) \in N_{S_3}(\langle(1\ 2\ 3)\rangle)$, hence $N_{S_3}(\langle(1\ 2\ 3)\rangle) = S_3$.

(b) Like S_3, the subgroups of Q_8 are maximal except for $\langle -1\rangle$ and the trivial subgroup, so $N_{Q_8}(1) = N_{Q_8}(-1) = Q_8$ since $-1 \in Z(Q_8)$. Taking i, we see that

$$ji(-j) = (-k)(-j) = -i, \quad ki(-k) = (-j)(-k) = i$$

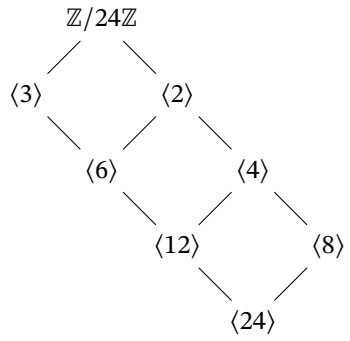
so that $j, k \in N_{Q_8}(\langle i\rangle)$. Then $N_{Q_8}(\langle i\rangle) = Q_8$. We deduce similarly that $N_{Q_8}(\langle j\rangle) = N_{Q_8}(\langle k\rangle) = Q_8$. ■

(9) Draw the lattices of subgroups of the following groups:
   (a) $\mathbb{Z}/16\mathbb{Z}$
   (b) $\mathbb{Z}/24\mathbb{Z}$
   (c) $\mathbb{Z}/48\mathbb{Z}$.

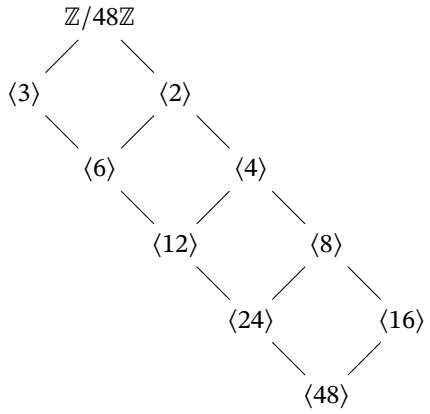
Solution.

(a) $\mathbb{Z}/16\mathbb{Z}$

(b) $\mathbb{Z}/24\mathbb{Z}$



(c) $\mathbb{Z}/48\mathbb{Z}$



■

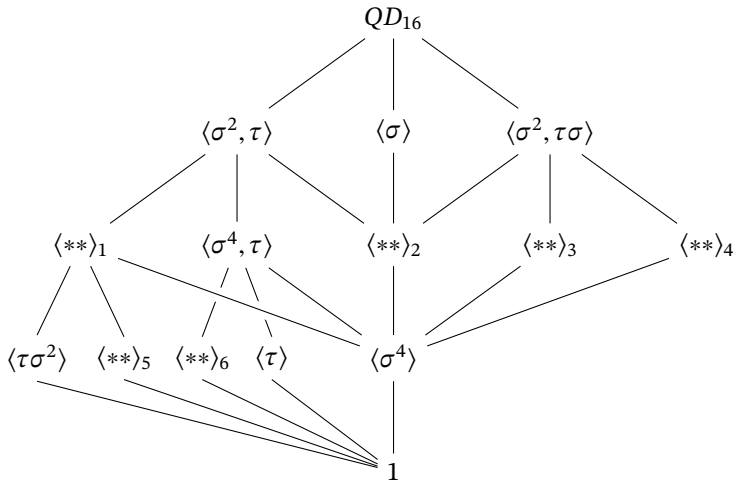
(10) Classify groups of order 4 by proving that if $|G| = 4$, then $G \cong Z_4$ or $G \cong V_4$. [See Section 1.1, Exercise 36]

Solution. Let $G = \{1, g, h, k\}$. Certainly, $G \cong Z_4$ if G contains an element of order 4 (so is then cyclic), since Theorem 2.4 says that cyclic groups of the same order are isomorphic. Suppose that G is not cyclic. It must be that $|g| = |h| = |k| = 2$. If $gh = 1$, then $h = g$ so that g and h are not distinct. If $gh = g$ or h, we may cancel to deduce either $h = 1$ or $g = 1$ respectively, contradicting the order of G. Hence, $gh = k$. We may use similar reasoning to deduce that $gk = h$ and $hk = g$ so that $G \cong V_4$. ■

(11) Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

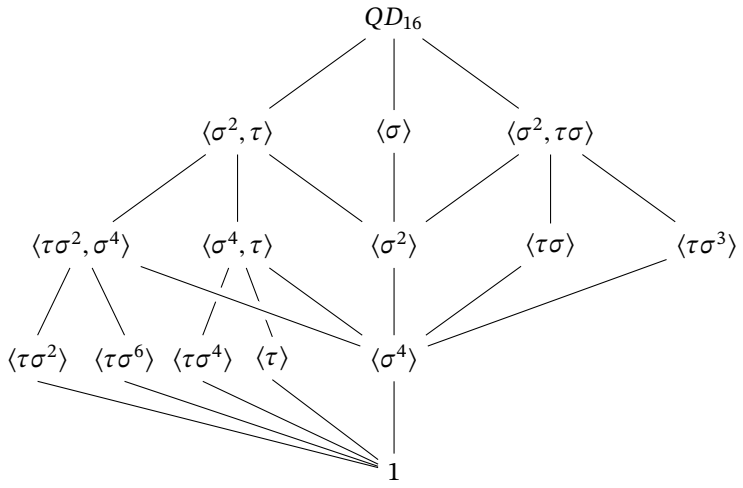
(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8, \langle \sigma \rangle \cong Z_8$, and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$, and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group, exhibiting each subgroup with at most two generators.



Solution. Note that the above has been assigned subscripts to the unknown subgroups so that we may refer to them by name in the solution. To that end, note that 2 is $\langle \sigma^2 \rangle$. To fill in the rest, we examine the cyclic subgroups for the rest of the elements. Since the structure of the subgroups generated by σ^k are clear, we must then look to elements of the form $\tau\sigma^k$. We have

$$\begin{aligned}
\langle \tau\sigma \rangle &= \{1, \tau\sigma, \sigma^4, \tau\sigma^5\} \\
\langle \tau\sigma^3 \rangle &= \{1, \tau\sigma^3, \sigma^4, \tau\sigma^7\} \\
\langle \tau\sigma^4 \rangle &= \{1, \tau\sigma^4\} \\
\langle \tau\sigma^6 \rangle &= \{1, \tau\sigma^6\}
\end{aligned}$$

It becomes clear that 6 must be $\langle \tau\sigma^4 \rangle$, since the subgroup above contains both τ and σ^4. 3 and 4 must be $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$ respectively, since $\langle \sigma^2, \tau\sigma \rangle$ both contain $\tau\sigma$ and σ^2 which multiply to $\tau\sigma^3$. Certainly, 1 cannot be $\langle \tau\sigma^6 \rangle$ as it does not contain $\langle \tau\sigma^2 \rangle$, so it must be 5. Then 1 must be $\langle \tau\sigma^2, \sigma^4 \rangle$ as it contains both subgroups. Hence, the completed diagram is



■

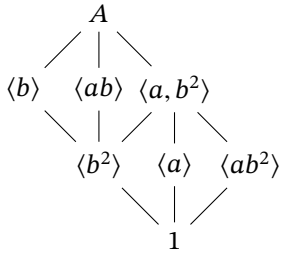
The next three examples lead to two nonisomorphic groups that have the same lattice of subgroups.

(12) The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba\rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2\rangle \cong V_4$, $\langle b\rangle \cong Z_4$, and $\langle ab\rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.

Solution. First, A is abelian, so we may write out the elements of A as

$$A = \{1, b, b^2, b^3, a, ab, ab^2, ab^3\}$$

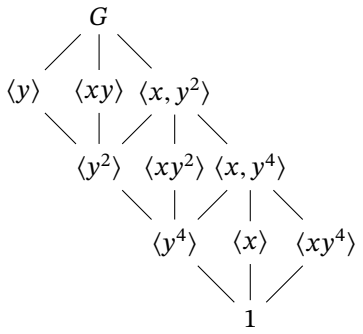
Moreover, we know that $\langle a, b^2\rangle$ must have 3 subgroups of order 2, namely $\langle a\rangle$, $\langle b^2\rangle$, and $\langle ab^2\rangle$. $\langle b\rangle$ has one subgroup of order 2, $\langle b^2\rangle$, and $\langle ab\rangle$ has one subgroup of order 2, $\langle b^2\rangle$. We may then form the lattice:



■

(13) The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx\rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2\rangle \cong Z_2 \times Z_4$, $\langle y\rangle \cong Z_8$, and $\langle xy\rangle \cong Z_8$, and every proper subgroup is contained in one of those three. Draw the lattice of all subgroups of G, giving each subgroups in terms of at most two generators (cf. Exercise 12).

Solution. Using $a = x$ and $b = y^2$ in the previous exercise, the subgroup lattice of G contains a copy of the previous lattice as well as the maximal subgroups $\langle y\rangle$ and $\langle xy\rangle$. We then have the lattice



■

(14) Let M be the group of order 16 with the following presentation:

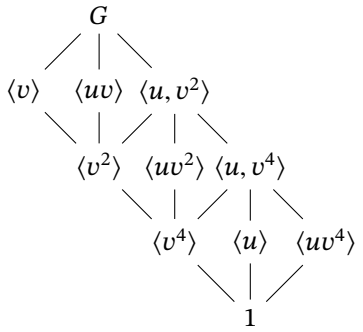
$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle, \langle v \rangle$, and $\langle uv \rangle$, and every proper subgroup is contained in one of those three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4, \langle v \rangle \cong Z_8$, and $\langle uv \rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Solution. Using the presentation for $Z_2 \times Z_4$ in Exercise 12, note that $u^2 = (v^2)^4 = 1$, and $v^2u = vuv^5 = uv^{10} = uv^2$, then $\langle u, v^2 \rangle$ is an abelian subgroup of M, and the map $\varphi : Z_2 \times Z_4 \to \langle u, v^2 \rangle$ defined by

$$\varphi(a) = u, \quad \varphi(b) = v^2$$

is a homomorphism. Moreover, φ is surjective by construction as $\langle u, v^2 \rangle = \langle \varphi(a), \varphi(b) \rangle$. Since $|Z_2 \times Z_4| = |\langle u, v^2 \rangle|$, then φ is bijective so that $Z_2 \times Z_4 \cong \langle u, v^2 \rangle$. Now, $\langle v \rangle$ and $\langle uv \rangle$ are both subgroups of order 8. Then $\langle v \rangle \cong Z_8$ and $\langle uv \rangle \cong Z_8$ since cyclic groups of the same order are isomorphic. Then the lattice of subgroups of M is the same as the lattice of $Z_2 \times Z_8$, where $x = u$ and $y = v$:



Lastly, these two subgroups are not isomorphic since M is not abelian, but $Z_2 \times Z_8$ is: if it were, then $uv = vu$, but $vu = uv^5 = uv$ would imply that $v^4 = 1$, contradicting that $|v| = 8$. ■

(15) Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

Solution. Since $|r| = 8$, then $\langle r \rangle \cong Z_8$. For the remaining subgroups, note that the lattice for D_{16} shows a striking similarity to the lattice for D_8; in fact, these subgroups *are* isomorphic to D_8 as follows:

For the subgroup $\langle s, r^2 \rangle$, observe that $(r^2)4 = s^2 = 1$, and $sr^2 = r^6s = (r^2)^{-1}s$. Then the mapping $\varphi : D_8 \to \langle s, r^2 \rangle$ given by

$$\varphi(r) = r^2, \quad \varphi(s) = s$$

extends to a homomorphism. Moreover, this mapping is surjective by construction. Since $\langle s, r^2 \rangle$ contains a subgroup of order 4 and is a subgroup of D_{16}, it must be 8 so that φ is an isomorphism, and $D_8 \cong \langle s, r^2 \rangle$.

For the subgroup $\langle sr, r^2\rangle$, we again observe that $(r^2)^4 = (sr)^2 = 1$, and $(sr)r^2 = sr^3 = r^5s = r^6r^7s = (r^2)^{-1}(sr)$. The mapping $\psi : D_8 \to \langle sr, r^2\rangle$ given by

$$\varphi(r) = r^2, \varphi(s) = sr$$

extends to a homomorphism, surjective by construction, and is an isomorphism because $\langle sr, r^2\rangle$ has order 8. Then $D_8 \cong \langle sr, r^2\rangle$. ■

(16) Use the lattice of subgroups of the quasidihedral of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2\rangle$ (cf. Exercise 11).

Solution. Every element of order 2 generates a cyclic subgroup of order 2. Using the lattice, $\langle \tau, \sigma^2\rangle$ properly contains all cyclic subgroups, except $\langle \tau\sigma\rangle$ and $\langle \tau\sigma^3\rangle$, both of which are order 4. Then $\langle \tau, \sigma^2\rangle$ contains all cyclic subgroups of order 2, hence contain all elements of order 2. ■

(17) Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 14).

Solution. Using the lattice in Exercise 14, we see that we have 3 candidates to be isomorphic to V_4, namely $\langle v^2\rangle, \langle uv^2\rangle$, and $\langle u, v^4\rangle$. The first and second subgroups are cyclic, while $\langle u, v^4\rangle = \{1, u, v^4, uv^4\}$. Since it is not generated by one element, each of these elements are of order 2, and $v^4u = v^3uv^5 = \cdots = uv^{20} = uv^4$ so that it is abelian, then $\langle u, v^4\rangle \cong V_4$. ■

(18) Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 11).

Solution. Note that $\sigma^4\tau = \sigma^3\tau\sigma^3 = \cdots = \tau\sigma^{12} = \tau\sigma^4$ so that $\sigma^4 \in Z(QD_{16})$ as σ^4 already commutes with powers of σ. Moreover, any power of σ does not commute with τ except for σ^4. The elements $\tau\sigma$ and $\tau\sigma^3$ do not commute with σ^2 as $(\tau\sigma)\sigma^2 = \tau\sigma^3 = \sigma\tau \neq \sigma^2(\tau\sigma) = \tau\sigma^2$, and $(\tau\sigma^3)\sigma^2 = \sigma^7\tau \neq \sigma^3\tau = \sigma^2(\tau\sigma^3)$. Next, $(\tau\sigma^2)\sigma^2 = \tau\sigma^4 \neq \tau = \sigma^2(\tau\sigma^2)$ so that σ^2 does not commute with $\tau\sigma^2$. Moreover, $(\tau\sigma^6)(\tau\sigma^2) = \tau\sigma^2\sigma^4\tau\sigma^2 = (\tau\sigma^2)(\tau\sigma^6)$ so that $\tau\sigma^2$ commutes with $\tau\sigma^6$, but $\sigma^2\tau\sigma^6 = \tau\sigma^4 \neq \tau = (\tau\sigma^6)\sigma^2$ so σ^2 does not commute with $\tau\sigma^6$. Lastly, $\sigma^2(\tau\sigma^4) = \tau\sigma^2 \neq (\tau\sigma^4)\sigma^2$, and $\sigma^2\tau = \tau\sigma^6 \neq \tau\sigma^2$ so that σ^2 does not commute with $\tau\sigma^4$ nor with τ. It follows that the centralizers of the elements of QD_{16} are

$$\begin{aligned}
C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) &= QD_{16}\\
C_{QD_{16}}(\langle\sigma^k\rangle) &= \langle\sigma\rangle \text{ for } k = 1, 2, 3, 5, 6, 7\\
C_{QD_{16}}(\langle\tau\sigma\rangle) = C_{QD_{16}}(\langle\tau\sigma^5\rangle) &= \langle\tau\sigma\rangle\\
C_{QD_{16}}(\langle\tau\sigma^3\rangle) = C_{QD_{16}}(\langle\tau\sigma^7\rangle) &= \langle\tau\sigma^3\rangle\\
C_{QD_{16}}(\langle\tau\rangle) = C_{QD_{16}}(\langle\tau\sigma^4\rangle) &= \langle\sigma^4, \tau\rangle\\
C_{QD_{16}}(\langle\tau\sigma^2\rangle) = C_{QD_{16}}(\langle\tau\sigma^6\rangle) &= \langle\tau\sigma^2, \sigma^4\rangle
\end{aligned}$$

■

(19) Use the lattice to help find $N_{D_{16}}(\langle s, r^4\rangle)$.

Solution. Based on the placement of $\langle s, r^4\rangle$, its normalizer may be itself, $\langle s, r^2\rangle$, or D_{16}. Note that $\langle s, r^4\rangle = \{1, s, r^4, sr^4\}$, and taking r^2 and $(r^2)^{-1} = r^6$, we have

$$r^2\langle s, r^4\rangle r^6 = \{1, sr^4, r^4, s\} = \langle s, r^4\rangle$$

so that $r^2 \in N_{D_{16}}(\langle s, r^4\rangle)$, and $\langle s, r^2\rangle \leq N_{D_{16}}(\langle s, r^4\rangle)$. Since $rsr^{-1} = r^2s \neq r$, then $r \notin N_{D_{16}}(\langle s, r^4\rangle)$ so that $N_{D_{16}}(\langle s, r^4\rangle) = \langle s, r^2\rangle$. ■

(20) Use the lattice of subgroups of QD_{16} (cf. Exercise 11) to help find the normalizers

(a) $N_{QD_{16}}(\langle\tau\sigma\rangle)$

(b) $N_{QD_{16}}(\langle\tau, \sigma^4\rangle)$.

Solution.

(a) Note that $\langle\tau\sigma\rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\}$. Moreover, $(\sigma^2)^{-1} = \sigma^6$ so that

$$\sigma^2\langle\tau\sigma\rangle\sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\sigma\} = \langle\tau\sigma\rangle$$

and $\sigma(\tau\sigma)\sigma^7 = \tau\sigma^3 \neq \tau\sigma$ so that $\sigma \notin N_{QD_{16}}(\langle\tau\sigma\rangle)$ so that $N_{QD_{16}}(\langle\tau\sigma\rangle) = \langle\sigma^2, \tau\sigma\rangle$.

(b) $\langle\tau, \sigma^4\rangle = \{1, \tau, \sigma^4, \tau\sigma^4\}$, and

$$z\sigma^2\langle\tau, \sigma^4\rangle\sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\}$$

while $\sigma\tau\sigma^7 = \tau\sigma^2 \neq \tau$ so that $\sigma \notin N_{QD_{16}}(\langle\tau, \sigma^4\rangle)$. Then $N_{QD_{16}}(\langle\tau, \sigma^4\rangle) = \langle\sigma^2, \tau\rangle$. ■

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Let G and H be groups.

(1) Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker(\varphi) \trianglelefteq G$.

Solution. Since $E \leq H$, then $1_H \in E$. Since $\varphi(1_G) = 1_H \in E$, then $1_G \in \varphi^{-1}(E)$ so that it is nonempty. Suppose $x, y \in \varphi^{-1}(E)$. Then $\varphi(x), \varphi(y) \in E$ so that $\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in E$. Then $xy^{-1} \in \varphi^{-1}(E)$, hence $\varphi^{-1}(E) \leq G$.

If $E \trianglelefteq H$, then $heh^{-1} \in E$ for every $e \in E$ and $h \in H$. Let $x \in \varphi^{-1}(E)$ and $g \in G$. Note that $\varphi(g) \in H$. Then

$$\varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(gxg^{-1}) \in E$$

so that $gxg^{-1} \in \varphi^{-1}(E)$. Then $\varphi^{-1}(E) \trianglelefteq G$, and since $\ker(\varphi) = \varphi^{-1}(1_H)$, then $\ker(\varphi) \trianglelefteq G$ as well. ■

(2) Let $\phi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \phi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \phi^{-1}(a)$, $Y = \phi^{-1}(b)$. Fix an element $u \in X$ (so $\phi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

Solution. To show that $v = u^{-1}w \in Y$, then

$$\varphi(v) = \varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}(ab) = b \in Y$$ ■

(3) Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Solution. Let $aB, a'B \in A/B$. Then

$$(aB)(a'B) = (aa')B = (a'a)B = (a'B)(aB)$$

so that A/B is abelian.

To produce an abelian quotient group from a non-abelian group, a good thought is to consider the centers of non-abelian groups. In this case, we may choose $G = D_8$ with $Z(D_8) = \langle r^2 \rangle \trianglelefteq D_8$. Since $D_8/\langle r^2 \rangle \cong V_4$, then the quotient group is abelian. ■

(4) Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Solution. Note that $(gN)^0 = 1N = g^0N$, and $(gN)^{-1} = g^{-1}N$ by Proposition 3.5. It suffices to show that the relationship holds for $\alpha \in \mathbb{Z}^+$. To that end, note that $\alpha = 1$ holds. Supposing it holds for some α, then

$$(gN)^{\alpha+1} = (gN)^\alpha(gN) = (g^\alpha N)(gN) = g^{\alpha+1}N$$

so that the result is true by induction. ■

(5) Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Solution. Let $gN \in G/N$. If possible, let $n \in \mathbb{Z}^+$ be the smallest integer such that $g^n \in N$. Then $g^nN = (gN)^n = 1N$ so that $|gN| \leq n$. Moreover, if $m \in \mathbb{Z}^+$ is an integer such that $(gN)^m = 1N$, then $g^mN = 1N$ so that $g^m \in N$. By minimality of n, then $|gN| \geq n$ so that $|gN| = n$.

If there is no such n, then $g^k \notin N$ for every $k \in \mathbb{Z}^+$. Suppose for contradiction that gN has infinite order x. Then $(gN)^x = g^xN = 1N$, or that $g^x \in N$, contradicting our previous assumption. It follows that gN has infinite order. Moreover, let G be a nontrivial group with nonidentity $g \in G$. Noting that $G \trianglelefteq G$, then $gG \in G/N$ has order 1, but $|g| > 1$. ■

(6) Define $\phi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\phi(x)$ be x divided by the absolute value of x. Describe the fibers of ϕ and prove that ϕ is a homomorphism.

Solution. The fibers of φ are as follows: the positive reals map to 1, and the negative reals map to -1. Moreover, for any $x, y \in \mathbb{R}^\times$, then

$$\varphi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \varphi(x)\varphi(y)$$ ■

(7) Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

Solution. Let $(x, y), (a, b) \in \mathbb{R}^2$. Then

$$\begin{aligned}\pi((x, y) + (a, b)) &= \pi((x + a, y + b)) \\ &= (x + a) + (y + b) \\ &= (x + y) + (a + b) \\ &= \pi((x, y)) + \pi((a, b))\end{aligned}$$

so that π is a homomorphism. Moreover, for any $a \in \mathbb{R}$, then $\pi((a, 0)) = a$ so that π is surjective. $\ker(\pi)$ is the diagonal line in $\mathbb{R}$ with equation $y = -x$, and the fiber $\varphi^{-1}(a)$ for any $a \in \mathbb{R}$ is the diagonal line $y = -x + a$, or just a vertical translation of the kernel. ■

(8) Let $\phi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that ϕ is a homomorphism and find the image of ϕ. Describe the kernel and the fibers of ϕ.

Solution. Let $x, y \in \mathbb{R}^\times$. Then

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\pi(y)$$

so that φ is a homomorphism. Moreover, $\varphi(\pm a) = a$ for any $a \in \mathbb{R}^+$ so that $\text{im}(\varphi)$ is the positive reals. $\ker(\varphi) = \{1, -1\}$ since no other real number has an absolute value of 1, and the fiber of φ over a is the pair of reals $\{a, -a\}$. ■

(9) Define $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\phi(a + bi) = a^2 + b^2$. Prove that ϕ is a homomorphism and find the image of ϕ. Describe the kernel and the fibers of ϕ geometrically (as subsets of the plane).

Solution. Let $a + bi, c + di \in \mathbb{C}^\times$. Then

$$\begin{aligned}\varphi((a + bi)(c + di)) &= \varphi((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= c^2(a^2 + b^2) + d^2(a^2 + b^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= \varphi(a + bi)\varphi(c + di)\end{aligned}$$

and φ is a homomorphism. Note that $a^2 + b^2 > 0$ for any a, b where at least one of them is nonzero, so $\text{im}(\varphi) \subseteq \mathbb{R}^+$. Also, $\varphi(\sqrt{a} + 0i) = a$ for any $a \in \mathbb{R}^+$, so $\text{im}(\varphi) = \mathbb{R}^+$. $\ker(\varphi) = \{a + bi \in \mathbb{C}^\times \mid a^2 + b^2 = 1\}$ is simply the circle of radius 1, and the fiber of φ over some $a \in \mathbb{R}^\times$ is the circle with radius $\sqrt{a}$. ■

(10) Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. Show that this is a well defined, surjective homomorphism and describe its fibers and kernel explicitly (showing that φ is well defined involves the fact that $\overline{a}$ has a different meaning in the domain and range of φ).

Solution. Suppose $\overline{a} = \overline{b}$ for $\overline{a}, \overline{b} \in \mathbb{Z}/8\mathbb{Z}$. Then $a = b + 8k$ for $k \in \mathbb{Z}$, and

$$\varphi(\overline{a}) = \overline{a} = \overline{b + 8k} = \overline{b + 4(2k)} = \overline{b} = \varphi(\overline{b})$$

Moreover, this is a homomorphism as

$$\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = \overline{a + b} = \overline{a} + \overline{b} = \varphi(\overline{a}) + \varphi(\overline{b})$$

and is clearly surjective as $\varphi(\bar{a}) = \bar{a}$ for any $\bar{a} \in \mathbb{Z}/4\mathbb{Z}$. The fibers are the following, noting that $\ker(\varphi) = \varphi^{-1}(\bar{0})$:

$$\begin{aligned}\varphi^{-1}(\bar{0}) &= \{\bar{0}, \bar{4}\}\\ \varphi^{-1}(\bar{1}) &= \{\bar{1}, \bar{5}\}\\ \varphi^{-1}(\bar{2}) &= \{\bar{2}, \bar{6}\}\\ \varphi^{-1}(\bar{3}) &= \{\bar{3}, \bar{7}\}\end{aligned}$$

■

(11) Let F be a field and let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in F, ac \neq 0 \right\} \leq \mathrm{GL}_2(F)$$

(a) Prove that the map

$$\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

is a surjective homomorphism from G onto $F^\times$ (recall that $F^\times$ is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ.

(b) Prove that the map

$$\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

(c) Let

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in F \right\}$$

Prove that H is isomorphic to the additive group F.

Solution.

(a) Note that

$$\varphi\left(\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}\right) = a$$

so that φ is surjective. Moreover, for any $a, b, c, d, e, f \in F$ with $ac \neq 0$ and $df \neq 0$, we have

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}\right) = ad = \varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right)\varphi\left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right)$$

and φ is then a homomorphism. The fiber of $a \in F^\times$ over φ is

$$\varphi^{-1}(a) = \left\{ \begin{pmatrix} a & s \\ 0 & t \end{pmatrix} \;\middle|\; s, t \in F, t \neq 0 \right\}$$

with $\ker(\varphi) = \varphi^{-1}(1)$.

(b) Showing that ψ is a surjective homomorphism is very similar to the previous part. The fiber of any $(a, c) \in F^\times \times F^\times$ is

$$\psi^{-1}((a, c)) = \left\{ \begin{pmatrix} a & s \\ 0 & c \end{pmatrix} \;\middle|\; s \in F \right\}$$

with $\ker(\psi) = \psi^{-1}((1, 1))$.

(c) Define the mapping $\pi : H \to F$ given by

$$\pi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = b$$

Then its inverse $\pi^{-1} : F \to H$ given by

$$\pi^{-1}(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

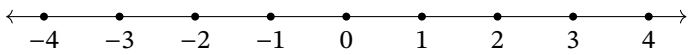
is a two-sided inverse of π so that π is a bijection. Moreover, for $b, c \in F$, then

$$\pi\left(\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}\right) = \pi\left(\begin{pmatrix}1 & b+c\\ 0 & 1\end{pmatrix}\right) = b + c = \pi\left(\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\right) + \pi\left(\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}\right)$$

so that π is a homomorphism. Then π is an isomorphism, and $H \cong F$. ■

(12) Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\phi : G \to H$ be the homomorphism $\phi : r \mapsto e^{2\pi ir}$. Draw the points on a real line which lie in the kernel of ϕ. Describe similarly the elements in the fibers of ϕ above the points -1, i, and $e^{4\pi i/3}$ of H.

Solution. Since $e^{2\pi ir} = 1$ if and only if r is an integer, then $\ker(\varphi) = \mathbb{Z}$. On a number line, this is shown as



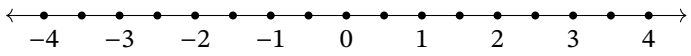
Moreover, note that $-1 = e^{-2\pi i/2}$ and $i = e^{2\pi i/4}$. Then the fibers of these elements are just the integral differences of $1/2, 1/4$, and $2/3$ respectively, since $4\pi i/3 = 2/3(2\pi i)$:

$$\begin{aligned}\varphi^{-1}(-1) &= \frac{1}{2} + \mathbb{Z} = \left\{\frac{1}{2} + n \;\middle|\; n \in \mathbb{Z}\right\}\\ \varphi^{-1}(i) &= \frac{1}{4} + \mathbb{Z} = \left\{\frac{1}{4} + n \;\middle|\; n \in \mathbb{Z}\right\}\\ \varphi^{-1}(e^{4\pi i/3}) &= \frac{2}{3} + \mathbb{Z} = \left\{\frac{2}{3} + n \;\middle|\; n \in \mathbb{Z}\right\}\end{aligned}$$

■

(13) Repeat the preceding exercise with the map ϕ replaced by the map $\phi : r \mapsto e^{4\pi ir}$.

Solution. The kernel of φ is $\frac{1}{2}\mathbb{Z}$, or



Moreover, the fibers are just all halved, so

$$\begin{aligned}\varphi^{-1}(-1) &= \frac{1}{4} + \frac{1}{2}\mathbb{Z} = \left\{\frac{1}{4} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z}\right\}\\ \varphi^{-1}(-i) &= \frac{1}{8} + \frac{1}{2}\mathbb{Z} = \left\{\frac{1}{8} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z}\right\}\\ \varphi^{-1}(e^{4\pi i/3}) &= \frac{1}{3} + \frac{1}{2}\mathbb{Z} = \left\{\frac{1}{3} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z}\right\}\end{aligned}$$

■

(14) Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \le q < 1$.

(b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of roots of unity in $\mathbb{C}^\times$.

Solution.

(a) Suppose $t \in \mathbb{Q}$, and put $t = a/b$ in lowest terms. Then there exists unique q, r such that $a = bq + r$, or that $t = q + r/b$, where $0 \le r < 1$. Then $t + \mathbb{Z} = q + r/b + \mathbb{Z} = r/b + \mathbb{Z}$. Since r is unique, then r/b is the representative of $t + \mathbb{Z}$ such that $0 \le r < 1$.

(b) Suppose $t = p/q \in \mathbb{Q}$. Then $|t + \mathbb{Z}| \le q$, since $q(t + \mathbb{Z}) = qt + \mathbb{Z} = \mathbb{Z}$ so that $t + \mathbb{Z}$ has finite order. Moreover, $1/k + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has order k, but because $k \in \mathbb{Z}$ can be made arbitrarily large, then $1/k + \mathbb{Z}$ has arbitrarily large order.

(c) Note that $\mathbb{Q}/\mathbb{Z} \subseteq \mathrm{Tor}(\mathbb{R}/\mathbb{Z})$ by the previous exercise, so it remains to show that cosets with irrational representatives do not have finite order. If $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ with finite order n, and $x \in \mathbb{R} - \mathbb{Q}$, then $n(x + \mathbb{Z}) = nx + \mathbb{Z} = \mathbb{Z}$ implies that $nx \in \mathbb{Z}$. But since $n \in \mathbb{Z}^+$, this implies that $x \in \mathbb{Z}$, contradicting that it was irrational. Hence, $\mathrm{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

(d) By Exercise 3.1.12, we have $\mathbb{R}/\mathbb{Z} \cong S^1$. Note that $\mathrm{Tor}(S^1)$ consists of $z \in \mathbb{C}^\times$ such that $z^n = 1$, which is precisely the set of roots of unity. Since $\mathrm{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, then $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the set of roots of unity. ■

(15) Prove that a quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible (cf. Exercise 2.4.19).

Solution. Let A be a divisible abelian group, and let B be a proper subgroup of A. Pick $aB \in A/B$. Since A is divisible, there exists $x \in A$ such that $x^n = a$ for $x \in A$ and $n \in \mathbb{Z}$. Then $(xB)^n = x^nB = aB$ so that A/B is divisible. Since $\mathbb{Q}$ is divisible, and $\mathbb{Z} < \mathbb{Q}$ is proper, then $\mathbb{Q}/\mathbb{Z}$ is also divisible. ■

(16) Let G be a group, let N be a normal subgroup of G, and let $\overline{G} = G/N$. Prove that if $G = \langle x, y\rangle$ then $\overline{G} = \langle \overline{x}, \overline{y}\rangle$. Prove more generally that if $G = \langle S\rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S}\rangle$.

Solution. If $G = \langle S\rangle$, then for every $g \in G$, we have

$$g = s_1 s_2 \dots s_n \quad \text{where } s_i \in S \text{ for } 1 \le i \le n$$

Let $\overline{S} = \{sN \mid s \in S\}$. Then for any $\overline{g} \in \overline{G}$, we have

$$gN = (s_1 s_2 \dots s_n)N = (s_1N)(s_2N)\dots(s_nN)$$

so that $\overline{g} \in \overline{S}$. Hence, $\overline{G} = \langle \overline{S}\rangle$. The case where $\overline{G} = \langle \overline{x}, \overline{y}\rangle$ is similar, where every element $g \in G$ is of the form $g = w(x, y)$, where $w(x, y)$ denotes a word in $\langle x, y\rangle$. ■

(17) Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5): $G = \langle r, s \mid r^8 = s^2 = 1,\ rs = sr^{-1}\rangle$, and let $\overline{G} = G/\langle r^4\rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\bar{s}^a\bar{r}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\bar{s}^a\bar{r}^b$, for some integers a and b as in (b): $\overline{rs}$, $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.

(e) Prove that $\overline{H} = \langle \bar{s}, \bar{r}^2\rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.

(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

Solution.

(a) Since $\langle r^4\rangle = \{1, r^4\}$, each coset in $\overline{G}$ has 2 elements and partitions G into 8 sets. Hence, $|\overline{G}| = 8$.

(b) The elements of $\overline{G}$ are

$$\begin{aligned} \bar{1} &= \{1, r^4\}, & \bar{s} &= \{s, sr^4\} \\ \bar{r} &= \{r, r^5\}, & \overline{sr} &= \{sr, sr^5\} \\ \bar{r}^2 &= \{r^2, r^6\}, & \overline{sr^2} &= \{sr^2, sr^6\} \\ \bar{r}^3 &= \{r^3, r^7\}, & \overline{sr^3} &= \{sr^3, sr^7\} \end{aligned}$$

(c) The orders of the elements of $\overline{G}$ are

$\bar{x}$	$\bar{1}$	$\bar{r}$	$\bar{r}^2$	$\bar{r}^3$	$\bar{s}$	$\overline{sr}$	$\overline{sr^2}$	$\overline{sr^3}$
$\lvert x\rvert$	1	4	2	4	2	2	2	2

(d) $\overline{rs} = \overline{sr^3}, \overline{sr^{-2}s} = \bar{r}^2, \overline{s^{-1}r^{-1}sr} = \bar{r}^2$.

(e) We first note that $\overline{H} = \{1, \bar{r}^2, \bar{s}, \overline{sr^2}\}$. To show that $\overline{H} \trianglelefteq \overline{G}$, we simplify the process by noting that elements of $\overline{G}$ are of the form $\bar{r}^k$ or $\overline{sr^k}$. If an element is of the former, we have

$$\overline{r^k r^2 r^{-k}} = \bar{r}^2 \in \overline{H}$$
$$\overline{r^k s r^{-k}} = \overline{s(r^2)^{-k}} \in \overline{H}$$

If it is of the latter, then

$$\overline{(sr^k)r^2(r^{-k}s)} = \overline{r^{-2}} \in H$$
$$\overline{(sr^k)s(r^{-k}s)} = \overline{s(r^2)^k} \in H$$

where $\overline{sr^k}^{-1} = \overline{r^{-k}s}$. The above calculations show that for every $\bar{g} \in \overline{G}$, then $\overline{gr^2g^{-1}}, \overline{gsg^{-1}} \in H$ so that $\overline{gHg^{-1}} = \overline{H}$, hence $\overline{H} \trianglelefteq \overline{G}$. Moreover, it is easy to see that every element of $\overline{H}$ is of order 2 so that $\overline{H} \cong V_4$.

Let $\pi : G \to \overline{G}$ be the natural projection of G onto $\overline{G}$. Then $\pi^{-1}(\overline{H})$ is the complete preimage of $\overline{H}$, or the set of elements that map to a coset in $\overline{H}$. Using part (b), we see that

$$\pi^{-1}(\overline{H}) = \{1, r^2, r^4, r^6, s, sr^2, sr^4, sr^6\}$$

Note that $|\pi^{-1}(\overline{H})| = 8$, and the elements of $\overline{H}$ satisfy the relations $(r^2)^4 = s^2 = 1$. Then the mapping $\varphi : D_8 \to \pi^{-1}(\overline{H})$ given by $\varphi(r) = r^2$ and $\varphi(s) = s$ extends to a homomorphism that is clearly surjective. Then φ is an isomorphism, and $\pi^{-1}(\overline{H}) \cong D_8$.

(f) From the previous exercise, we have that $\overline{G} = \langle \bar{r}, \bar{s} \rangle$. Since $\bar{r}^2$ commutes with both $\bar{r}$ and $\bar{s}$, then $\bar{r}^2 \in Z(\overline{G})$. However, $\overline{rs} \neq \overline{sr}$ and $\overline{r^3 s} \neq \overline{sr^3}$. Additionally, none of $\overline{sr}, \overline{sr^2}$, nor $\overline{sr^3}$ commute with $\bar{r}$ so that $Z(\overline{G}) = \{\bar{1}, \bar{r}^2\}$. The elements of $\widehat{G} = \overline{G}/Z(\overline{G})$ are as follows:

$$\hat{1} = \{\bar{1}, \bar{r}^2\} \qquad \hat{s} = \{\bar{s}, \overline{sr^2}\}$$
$$\hat{r} = \{\bar{r}, \bar{r}^3\} \qquad \widehat{sr} = \{\overline{sr}, \overline{sr^3}\}$$

One can see that each nonidentity element of $\widehat{G}$ has order 2 so that $\widehat{G} \cong V_4$. ■

(18) Let G be the quasidihedral group of order 16 (whose lattice was computed in Exercise 11 of Section 2.5): $G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle$, and let $\overline{G} = G/\langle \sigma^4 \rangle$ be the quotient of G by the subgroup generated by σ^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{\tau}^a \overline{\sigma}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{\tau}^a \overline{\sigma}^b$, for some integers a and b as in (b): $\overline{\sigma\tau}$, $\overline{\tau\sigma^{-2}\tau}, \overline{\tau^{-1}\sigma^{-1}\tau\sigma}$.

(e) Prove that $\overline{G} \cong D_8$.

Solution.

(a) $\langle \sigma^4 \rangle$ has 2 elements, so each coset has 2 elements which subsequently split G into 8 cosets. Hence, $|\overline{G}| = 8$.

(b) The elements are

$$\overline{1} = \{1, \sigma^4\} \qquad \overline{\tau} = \{\tau, \tau\sigma^4\}$$
$$\overline{\sigma} = \{\sigma, \sigma^5\} \qquad \overline{\tau\sigma} = \{\tau\sigma, \tau\sigma^5\}$$
$$\overline{\sigma}^2 = \{\sigma^2, \sigma^6\} \qquad \overline{\tau\sigma^2} = \{\tau\sigma^2, \tau\sigma^6\}$$
$$\overline{\sigma}^3 = \{\sigma^3, \sigma^7\} \qquad \overline{\tau\sigma^3} = \{\tau\sigma^3, \tau\sigma^7\}$$

(c) The orders are

$\bar{x}$	$\bar{1}$	$\bar{\sigma}$	$\bar{\sigma}^2$	$\bar{\sigma}^3$	$\bar{\tau}$	$\overline{\tau\sigma}$	$\overline{\tau\sigma^2}$	$\overline{\tau\sigma^3}$
$\lvert\bar{x}\rvert$	1	4	2	4	2	2	2	2

(d) $\overline{\sigma\tau} = \overline{\tau\sigma^3}, \overline{\tau\sigma^{-2}\tau} = \bar{\sigma}^2, \overline{\tau^{-1}\sigma^{-1}\tau\sigma} = \bar{\sigma}^2$.

(e) Note that $\bar{\sigma}^4 = \bar{\tau}^2 = \bar{1}$, and $\overline{\sigma\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^7} = \overline{\tau\sigma}$ so that $\bar{G}$ satisfies the same relations in D_8. Then the mapping $\varphi : \bar{G} \to D_8$ given by $\varphi(\bar{\sigma}) = r$ and $\varphi(\bar{\tau}) = s$ extends to a surjective homomorphism, hence $\bar{G} \cong D_8$. ■

(19) Let G be the modular group of order 16 (whose lattice was computed in Exercise 14 of Section 2.5): $G = \langle u, v \mid u^2 = v^8 = 1,\ vu = uv^5\rangle$, and let $\bar{G} = G/\langle v^4\rangle$ be the quotient of G by the subgroup generated by v^4 (this subgroup is contained in the center of G, hence is normal).

(a) Show that the order of $\bar{G}$ is 8.

(b) Exhibit each element of $\bar{G}$ in the form $\bar{u}^a\bar{v}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\bar{G}$ exhibited in (b).

(d) Write each of the following elements of $\bar{G}$ in the form $\bar{u}^a\bar{v}^b$, for some integers a and b as in (b): $\overline{vu}$, $\overline{uv^{-2}u}$, $\overline{u^{-1}v^{-1}uv}$.

(e) Prove that $\bar{G}$ is abelian and is isomorphic to $Z_2 \times Z_4$.

Solution.

(a) $\langle v^4\rangle$ has 2 elements, so each coset has 2 elements. Then G is split into 8 cosets, hence $|\bar{G}| = 8$.

(b) The elements are

$$\bar{1} = \{1, v^4\} \qquad \bar{u} = \{u, uv^4\}$$
$$\bar{v} = \{v, v^5\} \qquad \overline{uv} = \{uv, uv^5\}$$
$$\bar{v}^2 = \{v^2, v^6\} \qquad \overline{uv^2} = \{uv^2, uv^6\}$$
$$\bar{v}^3 = \{v^3, v^7\} \qquad \overline{uv^3} = \{uv^3, uv^7\}$$

(c) The orders are

$\bar{x}$	$\bar{1}$	$\bar{v}$	$\bar{v}^2$	$\bar{v}^3$	$\bar{u}$	$\overline{uv}$	$\overline{uv^2}$	$\overline{uv^3}$
$\lvert\bar{x}\rvert$	1	4	2	4	2	2	2	2

(d) $\overline{vu} = \overline{uv^5}, \overline{uv^{-2}u} = \bar{u}^2, \overline{u^{-1}v^{-1}uv} = \bar{1}$.

(e) Since $\overline{vu} = \overline{uv^5} = \overline{uv}$, $\bar{G}$ is abelian. Moreover, using the presentation of $Z_2 \times Z_4$ in Section 2.5, Exercise 12, we see that $\bar{u}^2 = \bar{v}^4 = 1$ so that $\bar{G}$ satisfies the same relations. Then $\varphi : \bar{G} \to Z_2 \times Z_4$ given by $\varphi(\bar{u}) = a$ and $\varphi(\bar{v}) = b$ is a surjective homomorphism, hence $\bar{G} \cong Z_2 \times Z_4$. ■

(20) Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\widetilde{G} = G/\langle\overline{12}\rangle$, where for each integer a we simplify notation by writing $\widetilde{\bar{a}}$ as $\widetilde{a}$.

(a) Show that $\widetilde{G} = \{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{11}\}$.

(b) Find the order of each element of $\widetilde{G}$.

(c) Prove that $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$ (thus $(\mathbb{Z}/24\mathbb{Z})/(12\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, just as if we inverted and canceled the $24\mathbb{Z}$'s).

Solution.

(a) Note that for some $\widetilde{x} \in \widetilde{G}$, we have $\widetilde{x} = \bar{x}\langle 12\rangle = \{\bar{x}, \overline{x+12}\}$. It follows that $x = 0, 1, 2, \ldots, 11$ produces distinct cosets.

(b) The orders are

$\widetilde{x}$	$\widetilde{0}$	$\widetilde{1}$	$\widetilde{2}$	$\widetilde{3}$	$\widetilde{4}$	$\widetilde{5}$	$\widetilde{6}$	$\widetilde{7}$	$\widetilde{8}$	$\widetilde{9}$	$\widetilde{10}$	$\widetilde{11}$
$\lvert\widetilde{x}\rvert$	1	12	6	4	3	12	2	12	3	4	6	12

(c) Define the mapping $\varphi : \widetilde{G} \to \mathbb{Z}/12\mathbb{Z}$ given by $\varphi(\widetilde{x}) = \bar{x}$. This map is trivially a bijection, and for any $\widetilde{x}, \widetilde{y} \in \widetilde{G}$, then

$$\varphi(\widetilde{x} + \widetilde{y}) = \varphi(\widetilde{x+y}) = \overline{x+y} = \bar{x} + \bar{y} = \varphi(\widetilde{x}) + \varphi(\widetilde{y})$$

so that φ is a homomorphism. Then $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. ■

(21) Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx \rangle$$

Let $\overline{G} = G/\langle x^2y^2 \rangle$ (note that every subgroup of the abelian group G is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\bar{x}^a\bar{y}^b$ for some integers a and b.

(c) Find the order of each elements of $\overline{G}$ exhibited in (b).

(d) Prove that $\overline{G} \cong Z_4 \times Z_2$.

Solution.

(a) Note that $(x^2y^2)^2 = x^4y^4 = 1$ so that $\langle x^2y^2 \rangle = \{1, x^2y^2\}$. Then each coset of $\overline{G}$ has 2 elements, hence its order is 8.

(b) Noting that $\bar{x}^2\bar{y}^2 = \bar{1}$ in $\overline{G}$, we have $\bar{x}^2 = \bar{y}^2$. Then we have the elements

$$\begin{aligned} \bar{1} &= \{1, x^2y^2\} & \bar{y} &= \{y, x^2y^3\} \\ \bar{x} &= \{x, x^3y^2\} & \overline{xy} &= \{xy, x^3y^3\} \\ \bar{x}^2 &= \{x^2, y^2\} & \overline{x^2y} &= \{x^2y, y^3\} \\ \bar{x}^3 &= \{x^3, xy^2\} & \overline{x^3y} &= \{x^3y, xy^3\} \end{aligned}$$

(c) The orders are

$\bar{g}$	$\bar{1}$	$\bar{x}$	$\bar{x}^2$	$\bar{x}^3$	$\bar{y}$	$\overline{xy}$	$\overline{x^2y}$	$\overline{x^3y}$
$\lvert\bar{g}\rvert$	1	4	2	4	4	2	4	2

(d) Using the presentation of $Z_2 \times Z_4$ in Section 2.5, Exercise 12, and noting that $\overline{xy}^2 = \bar{x}^4 = 1$ then the mapping $\varphi : Z_2 \times Z_4 \to \overline{G}$ given by

$$\varphi(a) = \overline{xy}, \quad \varphi(b) = \bar{x}$$

extends to a unique homomorphism. Now suppose $\varphi(a^sb^t) = \varphi(a^ub^v)$. Then $\overline{xy}^s\bar{x}^t = \overline{xy}^u\bar{x}^v$. Since $\langle \overline{xy} \rangle \cap \langle \bar{x} \rangle$ is trivial, then $\overline{xy}^{s-u} = \bar{x}^{v-t}$ imply that both quantities must be one. Then $\overline{xy}^s = \overline{xy}^u$ and $\bar{x}^v = \bar{x}^t$. Then $s \equiv u \bmod 2$ and $v \equiv t \bmod 4$, so that $a^sb^t = a^ub^t$ since $|a| = 2$ and $|b| = 4$. Then φ is injective. Because $|Z_2 \times Z_4| = |\overline{G}| = 8$, then φ is an isomorphism, hence $\overline{G} \cong Z_2 \times Z_4 \cong Z_4 \times Z_2$. ■

(22) (a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

(b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Solution.

(a) Observe that $H \cap K \leq G$ since $H \leq G$ and $K \leq G$. Let $g \in G$ and $x \in H \cap K$. Since $H \trianglelefteq G$ and $K \trianglelefteq G$, then $gxg^{-1} \in H$ and $gxg^{-1} \in K$, hence $gxg^{-1} \in H \cap K$. Then $g(H \cap K)g^{-1} \subseteq H \cap K$. By Theorem 3.6, then $H \cap K \trianglelefteq G$.

(b) Let G be a group and I be a nonempty set of indices, possibly not countable. Consider the collection of subgroups $\{N_i \mid i \in I\}$ of G, where $N_i \trianglelefteq G$ for every $i \in I$. Consider their intersection

$$N = \bigcap_{i \in I} N_i$$

Since $N \leq G$, what remains to be shown is that $gNg^{-1} \subseteq N$ for some $g \in G$. To that end, let $n \in N$. Then $gng^{-1} \in N_i$ for each $i \in I$ because $N_i \trianglelefteq G$. It follows that $gng^{-1} \in N$ so that $gNg^{-1} \subseteq N$. ■

(23) Prove that the join (cf. Section 2.5) of any nonempty collection of normal subgroups of a group is a normal subgroup.

Solution. Let G be a group and I be a nonempty set of indices. Let $\{N_i \mid i \in I\}$ be a collection of normal subgroups of G, and let $N = \langle N_i \mid i \in I\rangle$ be the join of the collection. Let $g \in G$ and $n \in N$. Then

$$n = n_1 n_2 \dots n_k \quad \text{where } n_i \in N_i \text{ for some } i \in I$$

Since $N_i \trianglelefteq G$, then $gn_ig^{-1} \in N_i$ for each $1 \leq i \leq k$. Then

$$gng^{-1} = g(n_1 n_2 \dots n_k)g^{-1} = (gn_1g^{-1})(gn_2g^{-1}) \cdots (gn_kg^{-1})$$

Because gng^{-1} is written as a product of elements where each one belongs to some N_i, it follows that it is in the join N, hence $gNg^{-1} \subseteq N$. Then $N \trianglelefteq G$. ■

(24) Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Solution. We know $N \cap H \leq G$, so pick $h \in H$ and $x \in N \cap H$. Since $N \trianglelefteq G$, then $hxh^{-1} \in N$. Since $H \leq G$, then $hxh^{-1} \in H$ so that $hxh^{-1} \in N \cap H$. Then $N \cap H \trianglelefteq H$. ■

(25) (a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

(b) Let $G = \mathrm{GL}_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries $2, 1$. Show that $gNg^{-1} \subseteq N$ but g does not normalize N.

Solution.

(a) ($\Rightarrow$) If $N \trianglelefteq G$, then $gNg^{-1} \subseteq N$ holds true for all $g \in G$.

($\Leftarrow$) Suppose $gNg^{-1} \subseteq N$ for every $g \in G$, and let $n \in N$. To show that $N \subseteq gNg^{-1}$, note for some $g \in G$, then $g^{-1}Ng \subseteq N$ so that $g^{-1}ng \in N$. It follows that $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$ so that $N = gNg^{-1}$, hence $N \trianglelefteq G$.

(b) Let

$$n = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$$

where $x \in \mathbb{Z}$. Then

$$gng^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix} \in N$$

since $2x \in \mathbb{Z}$. Notice that the upper right entry of gng^{-1} for any $n \in N$ will be even, so any matrix with an odd integer in the upper right entry will have no such $n \in N$ such that gng^{-1} is that matrix. ■

(26) Let $a, b \in G$.

(a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conjugate of b. Prove that the order of a and the order of any conjugate of a are the same.

(b) Prove that the conjugate of a^{-1} is the inverse of the conjugate of a.

(c) Let $N = \langle S\rangle$ for some subset S of G. Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.

(d) Deduce that if N is the cyclic group $\langle x\rangle$, then N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

(e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G.

Solution.

(a) Note that $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$. The second result follows by Exercise 1.1.22.

(b) For any $g \in G$, then

$$(ga^{-1}g^{-1})(gag^{-1}) = ga^{-1}(g^{-1}g)ag^{-1} = g(a^{-1}a)g^{-1} = gg^{-1} = 1$$

so that $(gag^{-1})^{-1} = ga^{-1}g^{-1}$.

(c) If S is empty, then N is trivial, so the result follows. Suppose S is not empty, and pick $n \in N$. Because $N = \langle S \rangle$, then we have $n = s_1 s_2 \dots s_k$, where $s_i \in S$ for each $i = 1, 2, \dots, k$. Since

$$gng^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_kg^{-1})$$

for every $g \in G$, and $gSg^{-1} \subseteq N$, then the right hand side is also in N, hence $gNg^{-1} \subseteq N$ so that $N \trianglelefteq G$.

(d) ($\Rightarrow$) Immediate from the definition of a normal subgroup.
($\Leftarrow$) Put $S = \{x\}$ and use the previous part.

(e) Let $S = \{g \in G \mid |g| = n\}$, and put $N = \langle S \rangle$. If S is empty, then N is trivial, hence is normal. If S is nonempty, note that part (a) shows that for any $g \in G$ and $s \in S$, then $|gsg^{-1}| = |s| = n$ so that $gsg^{-1} \in S \subseteq N$. Then $gSg^{-1} \subseteq N$, hence $N \trianglelefteq G$ by part (c). ■

(27) Let N be a *finite* subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Solution. ($\Rightarrow$) Suppose $gNg^{-1} \subseteq N$. For any $g \in G$, define a mapping $\varphi : N \to gNg^{-1}$ given by $\varphi(n) = gng^{-1}$. If $\varphi(m) = \varphi(n)$, then $gmg^{-1} = gng^{-1}$ so that φ is injective by cancellation. Moreover, if $m \in gNg^{-1}$, there exists $n \in N$ such that $m = gng^{-1} = \varphi(n)$ so that φ is surjective. It follows that φ is a bijection, and $|N| = |gNg^{-1}|$. Since $gNg^{-1} \subseteq N$, and N is finite, it follows that $gNg^{-1} = N$.
($\Leftarrow$) Immediate.

Note that $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$. We may replace the condition that $gNg^{-1} = N$ with $gNg^{-1} \subseteq N$ by the implication showed above. ■

(28) Let N be a *finite* subgroup of a group G and assume $N = \langle S \rangle$ for some subset S of G. Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.

Solution. ($\Rightarrow$) Immediate, since $gSg^{-1} \subseteq gNg^{-1} = N$ because $g \in N_G(N)$.
($\Leftarrow$) If S is empty, then N is trivial hence the conclusion follows. Suppose S is not empty, and pick $n \in N$. Then $n = s_1 s_2 \dots s_k$, where $s_i \in S$ for every $i = 1, 2, \dots, k$. Then $gng^{-1} = gs_1g^{-1}gs_2g^{-1} \dots gs_kg^{-1} \in N$ because $gs_ig^{-1} \in gSg^{-1} \subseteq N$. Then $gNg^{-1} \subseteq N$, and by the previous exercise, $g \in N_G(N)$. ■

(29) Let N be a *finite* subgroup of G and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subsets S and T of G. Prove that N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.

Solution. ($\Rightarrow$) Immediate, since $gNg^{-1} = N$ for every $g \in G$, so $tSt^{-1} \subseteq N$.
($\Leftarrow$) Suppose S and T are nonempty subsets of G, and let $g \in G$. Since $g \in \langle T \rangle$, then $g = t_1 t_2 \dots t_k$, where $t_i \in T$ for each $i = 1, 2, \dots, k$. Since we need to show this for every $g \in G$, we must proceed by inducting on the word length of $g \in \langle T \rangle$. To that end, $t_1 S t_1^{-1} \subseteq N$, so the base case is satisfied. Assume now that $gSg^{-1} \subseteq N$ when g is some k-length word made up of elements from T. Consider the $k+1$-length word $g = t_1 t_2 \dots t_k t_{k+1}$, where $t_i \in T$ for each $i = 1, 2, \dots, k+1$. For notation, set $\hat{t} = t_1 t_2 \dots t_k$ so that $g = \hat{t} t_{k+1}$. The induction assumption shows that $\hat{t} S \hat{t}^{-1} \subseteq N$. For any $s \in S$, then

$$gsg^{-1} = \hat{t} t_{k+1} s t_{k+1}^{-1} h^{-1} = \hat{t}(t_{k+1} s t_{k+1}^{-1})\hat{t}^{-1}$$

where $t_{k+1} s t_{k+1}^{-1} \in N$ because $tSt^{-1} \subseteq N$ for every $t \in T$. Since $N = \langle S \rangle$, then we may set $t_{k+1} s t_{k+1}^{-1} = s_1 s_2 \dots s_m$, where $s_i \in S$ for every $i = 1, 2, \dots, m$. Then

$$\hat{t}(t_{k+1} s t_{k+1}^{-1})\hat{t}^{-1} = (\hat{t} s_1 \hat{t}^{-1})(\hat{t} s_2 \hat{t}^{-1}) \cdots (\hat{t} s_m \hat{t}^{-1}) \in N$$

Hence, $gsg^{-1} \in N$ so that $gSg^{-1} \subseteq N$. Induction shows that this is true for every $g \in G$, and by finiteness of N, we use the result from the previous exercise to conclude that $N \trianglelefteq G$. ■

(30) Let $N \leq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

Solution. ($\Rightarrow$) Suppose $gN = Ng$. For some $n \in N$, there exists $n' \in N$ such that $ng = gn'$, or $n = gn'g^{-1}$. Then $n \in gNg^{-1}$ so that $N \subseteq gNg^{-1}$. Moreover, if $n \in N$, then for some $n' \in N$ we have $gn = n'g$ so that $gng^{-1} = n'$, hence $gNg^{-1} \subseteq N$, hence $g \in N_G(N)$.
($\Leftarrow$) Suppose $g \in N_G(N)$ and $n \in N$. Since $n \in gNg^{-1}$, there exists $n' \in N$ such that $n = gn'g^{-1}$ so that $ng = gn'$, hence $n \in gN$, and $Ng \subseteq gN$. By symmetry, we have $gN \subseteq Ng$, hence $gN = Ng$. ■

(31) Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e. is the join of all subgroups H for which $N \trianglelefteq H$).

Solution. If $h \in H$, then $hNh^{-1} = N$ because $N \trianglelefteq H$, hence $h \in N_G(N)$. Because $N_G(N) \leq G$, then $H \subseteq N_G(N)$ implies $H \leq N_G(N)$. Moreover, since every subgroup such that N is normal in is a subgroup of $N_G(N)$, then $N_G(N)$ is the largest subgroup in which N is normal. ■

(32) Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for Q_8 in Section 2.5.]

Solution. By the lattice, the subgroups of Q_8 are 1, $\langle -1\rangle$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, and Q_8. It is clear that $Q_8/1 \cong Q_8$, and $Q_8/Q_8 \cong 1$. Now, the lattice shows that $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$ are all maximal subgroups, so their normalizers must either be themselves, or Q_8. Since $j\langle i\rangle(-j) = \langle i\rangle$, then $j \in N_{Q_8}(\langle i\rangle)$ so that $N_{Q_8}(\langle i\rangle) = Q_8$. We may similarly argue that $N_{Q_8}(\langle j\rangle) = N_{Q_8}(\langle k\rangle) = Q_8$. Moreover, $Z(Q_8) = \langle -1\rangle$, and every center of a group is normal. It follows that every subgroup of Q_8 is normal.

Let us first examine $Q_8/\langle -1\rangle = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$. Since $\bar{i}^2 = \overline{-1} = \bar{1}$, then $|\bar{i}| = 2$. We can argue that $|\bar{j}| = |\bar{k}| = 2$ so that $Q_8/\langle -1\rangle \cong V_4$. The quotient group $Q_8/\langle i\rangle = \{\bar{1}, \bar{j}\}$ has order 2 so $Q_8/\langle i\rangle \cong Z_2$. By symmetry, $Q_8/\langle j\rangle \cong Q_8/\langle k\rangle \cong Z_2$. ■

(33) Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for D_8 in Section 2.5.]

Solution. Again, $D_8/1 \cong D_8$ and $D_8/D_8 \cong 1$. Examining the three maximal subgroups $\langle s, r^2\rangle$, $\langle r\rangle$, and $\langle rs, r^2\rangle$. observe the following:

$$\begin{aligned} r\langle s, r^2\rangle r^{-1} &= \{1, sr^2.r^2, s\} = \langle s, r^2\rangle \\ s\langle r\rangle s^{-1} &= \{1, r^3, r^2, r\} = \langle r\rangle \\ r\langle rs, r^2\rangle r^{-1} &= \{1, sr, r^2, sr^3\} = \langle rs, r^2\rangle \end{aligned}$$

then the normalizers of each subgroup contain r and s, hence $N_{D_8}(\langle s, r^2\rangle) = N_{D_8}(\langle r\rangle) = N_{D_8}(\langle rs, r^2\rangle) = Q_8$. Moreover, each of these maximal subgroups are of order 4, which means their corresponding quotient groups will have order 2, hence $Q_8/\langle s, r^2\rangle \cong Q_8/\langle r\rangle \cong Q_8/\langle rs, r^2\rangle \cong Z_2$.

Now we examine $\langle r^2\rangle = Z(D_8)$ so it is clearly normal. Then $D_8/\langle r^2\rangle = \{\bar{1}, \bar{r}, \bar{s}, \overline{sr}\}$. Note that the nonidentity elements have order 2, and so $D_8/\langle r^2\rangle \cong V_4$.

For the remaining subgroups of order 2, observe that

$$\begin{aligned} r\langle s\rangle r^{-1} &= \{1, sr^2\} \neq \langle s\rangle \\ r\langle sr\rangle r^{-1} &= \{1, rs\} \neq \langle sr\rangle \\ r\langle sr^2\rangle r^{-1} &= \{1, s\} \neq \langle sr^2\rangle \\ r\langle sr^3\rangle r^{-1} &= \{1, sr\} \neq \langle sr^3\rangle \end{aligned}$$

so that none of the subgroups of order 2 contain r, hence none of them are normal. ■

(34) Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1}\rangle$ be the usual presentation of the dihedral group of order $2n$ and let k be a positive integer dividing n.

(a) Prove that $\langle r^k\rangle$ is a normal subgroup of D_{2n}.

(b) Prove that $D_{2n}/\langle r^k\rangle \cong D_{2k}$.

Solution.

(a) Observe that $\langle r^k\rangle = \{1, r^k, r^{2k}, \ldots, r^{n-k}\}$. It is clear that $r\langle r^k\rangle r^{-1} = \langle r^k\rangle$, and observe that $sr^k s^{-1} = r^{-k} = r^{n-k}$ so that $s\langle r^k\rangle s^{-1} = \langle r^k\rangle$. Since $r, s \in N_{D_{2n}}(\langle r^k\rangle)$, then $\langle r^k\rangle \trianglelefteq D_{2n}$.

(b) Consider $D_{2n}/\langle r^k\rangle$. Since $k \mid n$, then the order of $\langle r^k\rangle$ is n/k, and the number of cosets in the quotient group is $2n/(n/k) = 2k$. Now consider the cosets $\bar{r}$ and $\bar{s}$:

$$\bar{r} = \{r, r^{k+1}, r^{2k+1}, \ldots, r^{n-k+1}\} \quad \text{and} \quad \bar{s} = \{s, sr^k, sr^{2k}, \ldots, sr^{n-k}\}$$

It is clear that $\bar{s} \neq \bar{1}$, and $\bar{s}^2 = \bar{1}$ so that $|\bar{s}| = 2$. Moreover, $\bar{r}^k = \bar{1}$, hence $|\bar{r}| \leq k$. However, note that $\bar{r}^i = \bar{1}$ when $i \mid k$ so that $|\bar{r}| = k$. This clearly satisfies the relations for D_{2k}, hence $D_{2n}/\langle r^k\rangle \cong D_{2k}$. ■

(35) Prove that $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$ and describe the isomorphism type of the quotient group (cf. Exercise 9, Section 2.1).

Solution. We know that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$, so we just need to show that $A\,\mathrm{SL}_n(F)A^{-1} = \mathrm{SL}_n(F)$ for all $A \in \mathrm{GL}_n(F)$. To that end, note that for any $S \in \mathrm{SL}_n(F)$ and $X \in \mathrm{GL}_n(F)$, then we have $\det(XSX^{-1}) = \det(X)\det(S)\det(X^{-1}) = 1$, hence $X\,\mathrm{SL}_n(F)X^{-1} \subseteq \mathrm{SL}_n(F)$, and $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$.

Recall that when a subgroup is normal, it is actually the kernel of some homomorphism. Observe that every element of $\mathrm{SL}_n(F)$ has determinant 1, so if we consider the mapping $A \mapsto \det(A)$ for some $A \in \mathrm{GL}_n(F)$, then the kernel of this homomorphism is clearly $\mathrm{SL}_n(F)$. We may then consider the mapping $\varphi : \mathrm{GL}_n(F)/\mathrm{SL}_n(F) \to F^\times$ given by $\varphi(\overline{X}) = \det(X)$.

We now show that this mapping is well defined. Suppose $\overline{A} = \overline{B}$ for some $\overline{A}, \overline{B} \in \mathrm{GL}_n(F)/\mathrm{SL}_n(F)$. Recall that the elements of $\overline{A}$ are of the form AS for $A \in \mathrm{GL}_n(F)$ and some $S \in \mathrm{SL}_n(F)$. Since $\overline{A} = \overline{B}$, then for $AS \in \overline{A}$ there exists $S' \in \mathrm{SL}_n(F)$ such that $AS = BS_0$. Then

$$\varphi(\overline{A}) = \det(A) = \det(AS) = \det(BS') = \det(B) = \varphi(\overline{B})$$

so that φ is well defined.

To show that φ is injective, suppose $\varphi(\overline{A}) = \varphi(\overline{B})$. Then $\det(A) = \det(B)$. Pick some $AS \in \overline{A}$, where $S \in \mathrm{SL}_n(F)$. Note that $B^{-1}AS \in \mathrm{SL}_n(F)$, since $\det(B^{-1}AS) = \det(B^{-1})\det(A)\det(S) = \det(A)^{-1}\det(A)\det(S) = 1$, hence $B^{-1}AS = S'$ for some $S' \in \mathrm{SL}_n(F)$. Then $AS = BS'$, and $AS \in \overline{B}$ so that $\overline{A} \subseteq \overline{B}$. A similar argument shows that $\overline{B} \subseteq \overline{A}$ so that $\overline{A} = \overline{B}$, and φ is injective. Moreover, for some $f \in F^\times$, then $\det(fI_n) = f\det(I_n) = f$ so that φ is surjective. Lastly, for $\overline{A}, \overline{B} \in \mathrm{SL}_n(F)$, then

$$\varphi(\overline{AB}) = \det(AB) = \det(A)\det(B) = \varphi(\overline{A})\varphi(\overline{B})$$

so that φ is a homomorphism. Then φ is a bijective homomorphism, and $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$. ∎

(36) Prove that if $G/Z(G)$ is cyclic then G is abelian. [If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]

Solution. Suppose $G/Z(G) = \langle xZ(G)\rangle$ for some $x \in G$. Then cosets are of the form $x^aZ(G)$ for some $a \in \mathbb{Z}$. Suppose $g, h \in G$. Since both g and h belong to some coset in $G/Z(G)$, then $g = x^m z$ and $h = x^n z'$ for some $m, n \in \mathbb{Z}$ and $z, z' \in Z(G)$. Then

$$ab = (x^m z)(x^n z') = (x^n z')(x^m z) = ba$$

so that G is abelian. ∎

(37) Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Solution. Let C be the the given set. It is clear that $C \leq A \times B$. Suppose $(a, b) \in A \times B$. Then for any $(a', 1) \in C$, we have

$$(a, b)(a', 1)(a, b)^{-1} = (aa'a^{-1}, b1b^{-1}) = (aa'a^{-1}, 1) \in C$$

so that $C \trianglelefteq A \times B$.

Consider the mapping $\varphi : A \times B/C \to B$ given by $\varphi(\overline{(a, b)}) = b$. To show that this is well-defined, suppose $\overline{(a, b)} = \overline{(a', b')}$. Then $(a, b)C = (a', b')C$, which implies that $C = (a^{-1}, b^{-1})(a', b')C$, or that $(a^{-1}a', b^{-1}b') \in C$. Then $b^{-1}b' = 1$, or $b = b'$ so that φ is well-defined.

Now suppose $\varphi(\overline{(a, b)}) = \varphi(\overline{(a', b')})$. Then $b = b'$ so that $(a, b)C = (a', b')C$, hence φ is injective. Moreover, $\varphi(\overline{(1, b)}) = b$ so that φ is surjective. Lastly, for $\overline{(a, b)}, \overline{(a', b')} \in A \times B/C$, then

$$\varphi(\overline{(a, b)(a', b')}) = \varphi(\overline{(aa', bb')}) = bb' = \varphi(\overline{(a, b)})\varphi(\overline{(a', b')})$$

so that φ is a bijective homomorphism. Hence, $A \times B/C \cong B$. ∎

(38) Let A be an abelian group and let D be the (diagonal) subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

Solution. Since A is abelian, then $A \times A$ is abelian, hence any subgroup is normal so that $D \trianglelefteq A \times A$.

Now consider two cosets $\overline{(a_1, a_2)}, \overline{(a_3, a_4)} \in (A \times A)/D$. Then $\overline{(a_1, a_2)} = \overline{(a_3, a_4)}$ when $(a_1, a_2)^{-1}(a_3, a_4) \in D$, which implies that $a_1^{-1}a_3 = a_2^{-1}a_4$, or $a_3 a_4^{-1} = a_1 a_2^{-1}$. We can construct a well-defined, injective homomorphism $\varphi : (A \times A)/D \to A$ given by $\varphi(\overline{(a, b)}) = ab^{-1}$. Moreover, this is surective, since $\varphi(\overline{(a, 1)}) = a$ for any $a \in A$. Lastly, it is a homomorphism, because

$$\begin{aligned}\varphi(\overline{(a_1, b_1)(a_2, b_2)}) &= \varphi(\overline{(a_1 a_2, b_1 b_2)}) \\ &= (a_1 a_2)(b_1 b_2)^{-1} \\ &= (a_1 b_1^{-1})(a_2 b_2^{-1}) \\ &= \varphi(\overline{(a_1, b_1)})\varphi(\overline{(a_2, b_2)})\end{aligned}$$

Hence, φ is a bijective homomorphism, and $(A \times A)/D \cong A$. ∎

(39) Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.

Solution. Let $\alpha, \beta \in S_3$, where $\alpha = 1$ and $\beta = (1\ 2\ 3)$ so that $\alpha^{-1} = \alpha$ and $\beta^{-1} \neq \beta$. For $\gamma = (1\ 2) \in S_3$, consider $\alpha\gamma\alpha^{-1}$ and $\beta\gamma\beta^{-1}$. Observe that $\alpha\gamma\alpha^{-1} = \gamma$, while $\beta\gamma\beta^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \neq (1\ 2) = \gamma$. Then $(\alpha, \beta)(\gamma, \gamma)(\alpha^{-1}, \beta^{-1}) = (\gamma, (2\ 3))$, hence D is not a normal subgroup of $S_3 \times S_3$. ∎

(40) Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$.)

Solution. ($\Rightarrow$) Suppose $\overline{xy} = \overline{yx}$. Then $xyN = yxN$. Then there exists $n, n' \in N$ such that $xyn = yxn'$, or $x^{-1}y^{-1}xy = n'n^{-1}$ so that $x^{-1}y^{-1}xy \in N$.
($\Leftarrow$) Suppose $x^{-1}y^{-1}xy \in N$. Then there is $n \in N$ such that $x^{-1}y^{-1}xy = n$, or $xy = yxn$. Then $a \in xyN$ if and only if $a = xyn'$ for some $n' \in N$ if and only if $a = yxnn'$ if and only if $a \in yxN$. Hence, $\overline{xy} = \overline{yx}$. ∎

(41) Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator* subgroup of G).

Solution. Let $g \in G$ and $x^{-1}y^{-1}xy \in N$. Then

$$g(x^{-1}y^{-1}xy)g^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \in N$$

so that $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}] \in N$. Then $gNg^{-1} \subseteq N$, hence $N \trianglelefteq G$.

G/N is abelian, since the previous exercise shows that $\overline{x}$ and $\overline{y}$ in G/N commute when $[x, y] \in N$. ∎

(42) Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show $x^{-1}y^{-1}xy \in H \cap K$.]

Solution. Let $x \in H$ and $y \in K$. Since $H \trianglelefteq G$, then $y^{-1}xy \in H$, hence $[x, y] \in H$. Since $K \trianglelefteq G$, then $x^{-1}y^{-1}x \in K$, hence $[x, y] \in K$. Then $[x, y] \in H \cap K = 1$ so that $[x, y] = 1$. It follows that $x^{-1}y^{-1}xy = 1$, or $xy = yx$. ∎

(43) Assume $\mathcal{P} = \{A_i \mid i \in I\}$ is any partition of G with the property that $\mathcal{P}$ is a group under the "quotient operation" defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and any element a_j of A_j and let A_iA_j be the element of $\mathcal{P}$ containing a_ia_j (this operation is assumed to be well defined). Prove that the element of $\mathcal{P}$ that contains the identity of G is a normal subgroup of G and the elements of $\mathcal{P}$ are the cosets of this subgroup (so $\mathcal{P}$ is just a quotient group of G in the usual sense).

Solution. For any $g \in G$, let $\overline{g} \in \mathcal{P}$ be the element such that $g \in \overline{g}$. Now, $\overline{1} \in \mathcal{P}$ is the set such that $1 \in \overline{1}$ so that $\overline{1}$ is nonempty. Moreover, for any $g, h \in \overline{1}$, we have $\overline{gh} = \overline{g} \cdot \overline{h} = \overline{1} \cdot \overline{1} = \overline{1}$ so that $\overline{1}$ is closed under the operation. Lastly, we have that $\overline{g^{-1}} = \overline{g^{-1}} \cdot \overline{1} = \overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1}g} = \overline{1}$ so that $\overline{1}$ is closed under inverses, hence $\overline{1} \leq G$.

To show that $\overline{1} \trianglelefteq G$, let $g \in G$ and $x \in \overline{1}$. Then $\overline{gxg^{-1}} = \overline{g} \cdot \overline{x} \cdot \overline{g^{-1}} = \overline{g} \cdot \overline{1} \cdot \overline{g^{-1}} = \overline{gg^{-1}} = \overline{1}$, hence $gxg^{-1} \in \overline{1}$ so that $\overline{1} \trianglelefteq G$.

Consider some $g\overline{1} \in G/\overline{1}$, and let $\overline{g} \in \mathcal{P}$. For some $gy \in g\overline{1}$ where $y \in \overline{1}$, then $\overline{gy} = \overline{g} \cdot \overline{y} = \overline{g} \cdot \overline{1} = \overline{g}$ so that $gy \in \overline{g}$, hence $g\overline{1} \subseteq \overline{g}$. If $x \in \overline{g}$, then $\overline{x} = \overline{g}$ so that $\overline{g^{-1}x} = \overline{g^{-1}g} = \overline{1}$, hence $g^{-1}x \in \overline{1}$. Then $x = gg^{-1}x = g(g^{-1}x) \in g\overline{1}$, hence $\overline{g} \subseteq g\overline{1}$. It follows that $\overline{g} = g\overline{1}$. ∎

3.2 More on Cosets and Lagrange's Theorem

Let G be a group.

(1) Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.

Solution. Only 1, 2, 5, 9, 15, and 60 are permissible orders for subgroups of a group of order 120. The corresponding indices are 120, 60, 24, 12, 8, and 2, respectively. ■

(2) Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).

Solution. Since $|S_3| = 6$, then Lagrange's Theorem shows that non-trivial subgroups are of order 2 and 3. Clearly, none of the cyclic subgroups of order 2 can be contained in $\langle(1\ 2\ 3)\rangle$ since it has order 3. Moreover, $\langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle$, hence all cyclic subgroups are accounted for, and the containment is correct.

To prove that the subgroups of S_3 are only the cyclic subgroups in the lattice, suppose S_3 has a non-cyclic subgroup H of order 3, and suppose $H = \langle\sigma, \tau\rangle$ for some $\sigma, \tau \in S_3$. We then have $H = \{1, \sigma, \tau\}$. Since $|\sigma|$ divides $|H|$, it must be that $|\sigma| = 3$, hence σ and σ^2 are distinct elements so that $\tau = \sigma^2$. Then $H = \langle\sigma\rangle$, contradicting it was non-cyclic. Hence, all proper subgroups of S_3 are cyclic, and the lattice is correct. ■

(3) Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

Solution. Lagrange's Theorem shows that the possible orders of subgroups of Q_8 are 1, 2, 4, and 8. The only possible subgroup of order 2 is $\langle -1\rangle$ since it is the only element of order 2 in Q_8. The only subgroups of order 4 are $\langle i\rangle, \langle j\rangle$, ad $\langle k\rangle$ since every other nonidentity element has order 4 and are contained in one of these subgroups.

Since $\langle -1\rangle$ is contained in each of $\langle i\rangle, \langle j\rangle$, and $\langle k\rangle$, and the subgroups of order 4 are maximal via Lagrange's, then the lattice is correct. ■

(4) Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 3.1.36.]

Solution. If G is abelian, then we are done. Suppose G is not abelian. It follows that $Z(G)$ is a proper subgroup of G, and by Lagrange's Theorem, the order of $Z(G)$ must be either 1, p, or q. Assume $Z(G)$ is not trivial, and without loss of generality, assume $|Z(G)| = p$. Since $Z(G) \trianglelefteq G$ as $Z(G)$ is abelian, then we may Lagrange's again to obtain $|G/Z(G)| = |G|/|Z(G)| = q$, which is prime. Then $G/Z(G)$ is cyclic, so by Exercise 3.1.36, G is abelian, a contradiction. Hence, $Z(G) = 1$. ■

(5) Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

Solution.

(a) Since $1 \in H$, then $g1g^{-1} = 1 \in gHg^{-1}$ so that gHg^{-1} is nonempty. Now suppose $gxg^{-1}, gyg^{-1} \in gHg^{-1}$ for some $x, y \in H$. Then

$$(gxg^{-1})(gyg^{-1})^{-1} = gxg^{-1}gy^{-1}g^{-1} = gxy^{-1}g^{-1} \in gHg^{-1}$$

since $xy^{-1} \in H$. Hence, $gHg^{-1} \leq G$.

Define a map $\varphi : H \to gHg^{-1}$ by $\varphi(h) = ghg^{-1}$. To show that this is a bijection, suppose $\varphi(h_1) = \varphi(h_2)$. Then $gh_1g^{-1} = gh_2g^{-1}$, hence $h_1 = h_2$ so that φ is injective. Moreover, for any $ghg^{-1} \in gHg^{-1}$, then $\varphi(h) = ghg^{-1}$ so that φ is surjective. Hence, $|gHg^{-1}| = |H|$.

(b) Let $g \in G$. Since H is the unique subgroup of G of order n, then by part (a), gHg^{-1} is a subgroup of G of order n, hence $gHg^{-1} = H$. It follows that $H \trianglelefteq G$. ■

(6) Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

Solution. Suppose $Hg = g'H$ for some $g' \in G$. Note that $g \in Hg$ so that $g \in g'H$. Then $Hg = g'H = gH$, hence $Hg = gH$, and $g \in N_G(H)$. ■

(7) Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

Solution. Let $h \in H$. Since $h^{-1}h = 1 \in H$, then $h \sim h$ so that $\sim$ is reflexive. Suppose $g, h \in H$ such that $g \sim h$. Then $h^{-1}g \in H$, hence $g^{-1}h = (h^{-1}g)^{-1} \in H$ so that $h \sim g$ and $\sim$ is symmetric. Lastly, suppose $g, h, k \in G$ such that $g \sim h$ and $h \sim k$. Then $h^{-1}g \in H$ and $k^{-1}h \in H$, hence $(k^{-1}h)(h^{-1}g) = k^{-1}g \in H$ so that $g \sim k$ and $\sim$ is transitive. It follows that $\sim$ is an equivalence relation.

The equivalence class of some $a \in G$ is given by $\{b \in G \mid b^{-1}a \in H\}$. Note that b is in the equivalence class of a when $b^{-1}a = h$ for some $h \in H$, hence $b = ah^{-1}$. The set becomes $\{ah^{-1} \mid h \in H\}$, which is the left coset of H containing a. Since the equivalence classes partition G, then the left cosets of H partition G, by Proposition 0.2, then the left cosets of H in G form a partition of G, proving Proposition 4. ■

(8) Prove that if H and K are finite subgroups of G whose orders are relatively prime then $|H \cap K| = 1$.

Solution. Let $|H| = m$ and $|K| = n$ such that $(m, n) = 1$. Let $\ell = |H \cap K|$. Since $H \cap K \leq H$ and $H \cap K \leq K$, then by Lagrange's Theorem, $\ell \mid m$ and $\ell \mid n$. It follows that $\ell \mid (m, n) = 1$, hence $\ell = 1$. ■

(9) This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66 (1959), p. 119). Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}$$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Define the relation $\sim$ on S by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is *prime*). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p.

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element $x \in G$ with $x^p = 1$, i.e., G contains an element of order p. [Show $p \mid k$ and so $k > 1$.]

Solution.

(a) Consider the $(p-1)$-tuples of elements of G, and call this set $\mathcal{S}'$. Clearly, $\mathcal{S}'$ has $|G|^{p-1}$ elements. Define the map $\varphi : \mathcal{S}' \to \mathcal{S}$ by $\varphi(x_1, x_2, \ldots, x_{p-1}) = (x_1, x_2, \ldots, x_{p-1}, (x_1 x_2 \cdots x_{p-1})^{-1})$. Now suppose $\varphi(x_1, \ldots, x_{p-1}) = \varphi(y_1, \ldots, y_{p-1})$. Then we have $x_i = y_i$ for all $1 \leq i \leq p-1$, and the last inverse term must imply $x_1 x_2 \cdots x_{p-1} = y_1 y_2 \cdots y_{p-1}$ since inverses are unique in a group. Hence φ is injective. Moreover, this mapping is clearly surjective. It follows that $|\mathcal{S}| = |\mathcal{S}'| = |G|^{p-1}$.

(b) Let $\alpha = (x_1, x_2, \ldots, x_p) \in \mathcal{S}$. A cyclic permutation of α is some $\beta = (x_k, x_{k+1}, \ldots, x_p, x_1, x_2, \ldots, x_{k-1})$ for some $1 \leq k \leq p$ where the indices are taken modulo p. Observe that these consist of the same elements as α, just in a different order, hence $x_k x_{k+1} \cdots x_p x_1 x_2 \cdots x_{k-1} = x_1 x_2 \cdots x_p = 1$, so that $\beta \in \mathcal{S}$.

(c) Let $\alpha, \beta, \gamma \in \mathcal{S}$. $\sim$ is clearly reflexive since α is a cyclic permutation of itself.

Suppose $\alpha \sim \beta$. Then β is a cyclic permutation of α, hence α is a cyclic permutation of β, so that $\beta \sim \alpha$ and $\sim$ is symmetric.

Lastly, suppose $\alpha \sim \beta$ and $\beta \sim \gamma$. Then β is a cyclic permutation of α, and γ is a cyclic permutation of β, hence γ is a cyclic permutation of α by taking the composition of the permutations, so that $\alpha \sim \gamma$ and $\sim$ is transitive. It follows that $\sim$ is an equivalence relation on $\mathcal{S}$.

(d) ($\Rightarrow$) Let $[\alpha]$ denote the equivalence class that contains α. If $[\alpha]$ contains a single element, then it must be that all cyclic permutations of α are equal, hence $\alpha = (x, x, \ldots, x)$ for some $x \in G$. Since $\alpha \in \mathcal{S}$, then $x^p = 1$.

($\Leftarrow$) Suppose $\alpha = (x, x, \ldots, x)$ for some $x \in G$ such that $x^p = 1$. Then any cyclic permutation of α is equal to α, hence $[\alpha]$ contains a single element.

(e) Let $\alpha = (x_1, x_2, \ldots, x_p) \in \mathcal{S}$ where the x_i need not be distinct, and let $[\alpha]$ be the equivalence class containing α. Suppose $[\alpha]$ has n elements, and note that $x_i = x_j$ whenever $i + kn \equiv j \bmod p$ for some $k \in \mathbb{Z}$ that represents the amount of cyclic shifts.

There are two cases to discuss, either $n = p$ or $1 \leq n < p$. If $n = p$, then we are done. Suppose $1 \leq n < p$. Since p is prime, then $(n, p) = 1$, hence there exists some $k \in \mathbb{Z}$ such that $kn \equiv 1 \bmod p$. In particular, $i + kn \equiv i + 1 \equiv j \bmod p$ implies $x_{i+1} = x_j$. It follows that $x_i = x_j$ for all $1 \leq i, j \leq p$, hence $\alpha = (x, x, \ldots, x)$ for some $x \in G$. By part (c), $[\alpha]$ contains a single element.

Since the equivalence classes partition $\mathcal{S}$, let k be the number of classes of size 1 and d be the number of classes of size p. Then $|\mathcal{S}| = k + pd$, as desired.

(f) Because p divides $|G|$, then it divides $|\mathcal{S}| = |G|^{p-1}$. From part (d), we have $|G|^{p-1} = k + pd$, hence $p \mid k$ so that $k > 1$. Then there is at least one equivalence class of size 1 that is not $\{(1, 1, \ldots, 1)\}$. By part (c), this equivalence class is of the form $(x, x, \ldots, x)$ for some nonidentity $x \in G$ such that $x^p = 1$. It follows that G contains an element of order p. ∎

(10) Suppose H and K are subgroups of finite index in the (possibly infinite) group G with $|G : H| = m$ and $|G : K| = n$. Prove that $\operatorname{lcm}(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

Solution. Let $|G : H \cap K| = \ell$. Consider the cosets gH, gK, and $g(H \cap K)$ for some $g \in G$. We wish to identify $g(H \cap K)$ in terms of gH and gK. Note that $x \in g(H \cap K)$ implies that $g^{-1}x \in H \cap K$, hence $g^{-1}x \in H$ and $g^{-1}x \in K$, so that $x \in gH$ and $x \in gK$. It follows that $g(H \cap K) \subseteq gH \cap gK$. Now suppose $x \in gH \cap gK$. Then $x \in gH$ and $x \in gK$, hence $g^{-1}x \in H$ and $g^{-1}x \in K$, so that $g^{-1}x \in H \cap K$. It follows that $x \in g(H \cap K)$, hence $gH \cap gK \subseteq g(H \cap K)$. We conclude that $g(H \cap K) = gH \cap gK$.

Note that the set of cosets of $H \cap K$ in G partitions G into ℓ parts, and each coset is the intersection of a coset of H with a coset of K. Since there are m cosets of H and n cosets of K, then there are at most mn distinct intersections, hence $\ell \leq mn$.

We now show that ℓ is a multiple of m (a similar argument can be done to show that it is a multiple of n). Let $x \in G$. Since the cosets of H in G partition G, then there exists a unique $g \in G$ such that $x \in gH$. Moreover, because $H \cap K \leq H$, then the cosets of $H \cap K$ in H partition H so that there exists a unique $h \in H$ such that $x \in gh(H \cap K)$. Pick another coset $h' \neq h$ of $H \cap K$ in H. Then $gh(H \cap K) \neq gh'(H \cap K)$ since if they were equal, then $(gh)^{-1}(gh') = h^{-1}h' \in H \cap K$, contradicting that h and h' are distinct cosets. It follows that for each coset of H in G, there are $|H : H \cap K|$ distinct cosets of $H \cap K$ in G. Since there are m cosets of H in G, then $\ell = m|H : H \cap K|$, hence $m \mid \ell$. Similarly, $n \mid \ell$. Since ℓ is a multiple of both m and n, then $\operatorname{lcm}(m, n) \mid \ell$, hence $\operatorname{lcm}(m, n) \leq \ell$, and we have the desired inequality $\operatorname{lcm}(m, n) \leq \ell \leq mn$.

Lastly, if $(m, n) = 1$, then $\operatorname{lcm}(m, n) = mn$ so that $\ell = mn$. ∎

(11) Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$.

Solution. Note that cosets of H are contained in cosets of K. If H has infinite index in K or if K has infinite index in G, then H has infinite index in G. The finite case follows in the proof of Exercise 3.2.10, where we showed that each coset of K contains $|K : H|$ distinct cosets of H. Since there are $|G : K|$ distinct cosets of K in G, then there are $|G : K| \cdot |K : H|$ distinct cosets of H in G, hence $|G : H| = |G : K| \cdot |K : H|$. ∎

(12) Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left cosets and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets).

Solution. Let L be the set of left cosets of H in G and R be the set of right cosets of H in G. Define the map $\varphi : L \to R$ be given by $\varphi(xH) = Hx^{-1}$. Firstly, this map is well-defined: suppose $xH = yH$. Then $yx^{-1} \in H$, hence $(yx^{-1})^{-1} = xy^{-1} \in H$, so that $Hx^{-1} = Hy^{-1}$. Note that the map $\psi : R \to L$ given by $\psi(Hx) = x^{-1}H$ is well-defined by a similar argument. It is clear that $\varphi \circ \psi = 1$ and $\psi \circ \varphi = 1$, hence $\psi = \varphi^{-1}$ so that φ is a bijection. It follows that $|L| = |R|$. ∎

(13) Fix any labelling of the vertices of a square and use this to identify D_8 as a subgroup of S_4. Prove that the elements of D_8 and $\langle(123)\rangle$ do not commute in S_4.

Solution. Let $D_8 = \{1, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (2\,4), (1\,2)(3\,4), (1\,3), (1\,4)(2\,3)\}$ be the subgroup of S_4, where a square is labelled clockwise from 1 to 4. Note that D_8 is generated by $r = (1\,2\,3\,4)$ and $s = (2\,4)$. Then

$(1\,2\,3)(1\,2\,3\,4) = (1\,3\,4\,2) \neq (1\,4\,3\,2) = (1\,2\,3\,4)(1\,2\,3)$, and $(1\,2\,3)(2\,4) = (1\,4\,3) \neq (1\,3\,4) = (2\,4)(1\,2\,3)$, so that the generators of D_8 do not commute with the generator of $\langle(1\,2\,3)\rangle$. It follows that the elements of D_8 and $\langle(1\,2\,3)\rangle$ do not commute in S_4. ■

(14) Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

Solution. Suppose S_4 has a normal subgroup N of order 8. By Lagrange's then N cannot contain any 3-cycle. Then elements of N are comprised of at least the identity, 2-cycles, a product of 2 disjoint 2-cycles, or 4-cycles. Observe that N cannot contain all 6 2-cycles of S_4 for otherwise $(1\,2)(1\,3) = (1\,3\,2) \in N$, a contradiction. It must be that there is some 2-cycle $\sigma \in S_4$ that is not in N. Since $N \trianglelefteq S_4$, then $N\langle\sigma\rangle \leq S_4$. Since $\sigma \notin S_4$, then $N \cap \langle\sigma\rangle = 1$, hence $|N\langle\sigma\rangle| = 16$. This contradicts Lagrange's Theorem, hence N cannot exist.

If S_4 has a normal subgroup M of order 3, then $M \cong Z_3$ which is cyclic. Since S_4 contains 4 distinct 3-cycles, we may pick another $\tau \in S_4$ such that $\tau \notin M$, hence $M \cap \langle\tau\rangle = 1$. Because $M \trianglelefteq S_4$, we have $|M\langle\tau\rangle| = 9$, contradicting Lagrange's Theorem, hence M cannot exist. ■

(15) Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

Solution. Observe that the elements of G_i consists of permutations on the $\{1, 2, \ldots, n\} - \{i\}$ which has $n-1$ elements. Then $G_i \cong S_{n-1}$. ■

(16) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$.

Solution. Let p be a prime. Note that $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$. For any $a \in \mathbb{Z}$, then we either have $a \mid p$ or $a \nmid p$. If $a \mid p$, then $a \equiv 0 \bmod p$, hence $a^p \equiv 0 \equiv a \bmod p$. If $a \nmid p$, then $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's Theorem and Corollary 3.9, $|\bar{a}|$ divides $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, hence $\bar{a}^{p-1} = \bar{1}$. Then $a^{p-1} \equiv 1 \bmod p$, or $a^p \equiv a \bmod p$. ■

(17) Let p be a prime and let n be a positive integer. Find the order of $\bar{p}$ in $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and deduce that $n \mid \varphi(p^n-1)$ (here φ is Euler's function).

Solution. Since $p^n \equiv 1 \bmod (p^n-1)$, then $|\bar{p}| \leq n$. Suppose $d < n$ such that $p^d \equiv 1 \bmod (p^n-1)$. Then $p^n - 1 \mid p^d - 1$ so that $p^n - 1 \leq p^d - 1$, a contradiction. It follows that $|\bar{p}| = n$. By Lagrange's Theorem, $|\bar{p}| = n$ divides $|(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times| = \varphi(p^n-1)$. ■

(18) Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G:N|$ are relatively prime then $H \leq N$.

Solution. Since $N \trianglelefteq G$, then $HN \leq G$. Moreover, $H \cap N \leq H$ so that $|H \cap N|$ divides $|H|$. Then we have that $|G| = m|HN|$ and $|H| = n|H \cap N|$ for some $m, n \in \mathbb{Z}$. By Corollary 13, we have that

$$|HN| = \frac{|H||N|}{|H \cap N|} \implies m|HN| = m\frac{n|H \cap N||N|}{|H \cap N|} \implies \frac{|G|}{|N|} = |G:N| = mn$$

Since $(|H|, |G:N|) = 1$, then $n = 1$ so that $|H| = |H \cap N|$. It follows that $H = H \cap N$, hence $H \leq N$. ■

(19) Prove that if N is a normal subgroup of the finite group G and $(|N|, |G:N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Solution. Let M be a subgroup of G with order $|N|$. By the previous exercise, we have $M \leq N$, and since they have the same order, then $M = N$. ■

(20) If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.

Solution. Suppose $y = abxb^{-1}a^{-1} \in ab(A \cap B)b^{-1}a^{-1}$ for some $x \in A \cap B$. Since $A \trianglelefteq G$, then $bxb^{-1} \in A$ so that $y = a(bxb^{-1})a^{-1} = bxb^{-1} \in A$. Moreover, $bxb^{-1} \in B$ since $x \in B$, hence $y \in A \cap B$. It follows that $ab(A \cap B)b^{-1}a^{-1} \subseteq A \cap B$, so that $A \cap B \trianglelefteq AB$. ■

(21) Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index. [Recall Exercise 1.6.21 and Exercise 3.1.15.]

Solution. Suppose $\mathbb{Q}$ has a proper subgroup H such that $|\mathbb{Q} : H|$ is some finite n. Recalling that $\mathbb{Q}$ is divisible by Exercise 2.4.19, then $\mathbb{Q}/H$ is also divisible by Exercise 3.1.15. However, $\mathbb{Q}/H$ is a finite group of order n, hence it cannot be divisible unless it is trivial. It follows that $H = \mathbb{Q}$, a contradiction. Therefore, $\mathbb{Q}$ has no proper subgroups of finite index. Moreover, $\mathbb{Q}/\mathbb{Z}$ has no proper subgroup of finite index for the same reasoning. ■

(22) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\phi(n)} \equiv 1 \bmod n$ for every integer a relatively prime to n, where ϕ denotes Euler's ϕ-function.

Solution. Recall $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Since $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $|\overline{a}|$ divides $\varphi(n)$, hence $a^{\varphi(n)} \equiv 1 \bmod n$. ■

(23) Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \bmod \varphi(100)$ and use the previous exercise.]

Solution. Note that $100 = 2^2 \cdot 5^2$, then $\varphi(100) = 2^1(2-1)5^1(5-1) = 40$. Since $3^4 \bmod 40 = 81 \bmod 40 \equiv 1 \bmod 40$, then $3^{100} \bmod 40 \equiv 1 \bmod 40$. It follows that $3^{100} = 1 + 40k = 1 + \varphi(100)k$ for some $k \in \mathbb{Z}$, hence

$$3^{3^{100}} = 3^{1+\varphi(100)k} = 3 \cdot 3^{\varphi(100)^k} \equiv 3 \cdot 1^k \bmod 100 = 3 \bmod 100$$

so that the last two digits of $3^{3^{100}}$ are 03. ■

3.3 The Isomorphism Theorems

Let G be a group.

(1) Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|\mathrm{GL}_N(F) : \mathrm{SL}_n(F)| = q - 1$. [See Exercise 3.1.35.]

Solution. In Exercise 3.1.35, we showed that $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$ and that $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$. Since F is a finite field of order q, then $|F^\times| = q - 1$. We then have that $|\mathrm{GL}_n(F) : \mathrm{SL}_n(F)| = |F^\times| = q - 1$. ■

(2) Prove all parts of the Lattice Isomorphism Theorem.

Solution. Let $\mathcal{A} = \{A \leq G \mid N \subseteq A\}$ and $\overline{\mathcal{A}} = \{\overline{A} \leq \overline{G}\}$. Define the map $\varphi : \mathcal{A} \to \overline{\mathcal{A}}$ by $\varphi(A) = \overline{A} = A/N$. Note that $\varphi(A) \leq \overline{G}$ as follows: since $\overline{1} \in \overline{A}$, then $\overline{A}$ is nonempty. Moreover, for any $\overline{a}, \overline{b} \in \overline{A}$ where $a, b \in A$, then $ab^{-1} \in A$ implies $\overline{a}\overline{b}^{-1} = \overline{ab^{-1}} \in \overline{A}$, hence $\overline{A} \leq \overline{G}$. This also implies that φ is surjective, since for any $\overline{A} \in \overline{\mathcal{A}}$, we know that the preimage of $\overline{A}$ under the natural projection homomorphism from G to G/N is some subgroup A of G containing N such that $\varphi(A) = \overline{A}$. Lastly, suppose $\varphi(A) = \varphi(B)$ for some $A, B \in \mathcal{A}$. Then $\overline{A} = \overline{B}$ implies that for some $a \in A$, there is some $b \in B$ such that $\overline{a} = \overline{b}$, hence $aN = bN$ so that $b^{-1}a \in N \subseteq B$. It follows that $a = b(b^{-1}a) \in B$, hence $A \subseteq B$. A similar argument shows that $B \subseteq A$, hence $A = B$ so that φ is injective. Therefore, φ is a bijection.

1. ($\Rightarrow$) Suppose $A \leq B$ for $A, B \in \mathcal{A}$, and suppose $\overline{a} \in \overline{A}$ for some $a \in A$. Since $A \leq B$, then $a \in B$ so that $\overline{a} \in \overline{B}$, hence $\overline{A} \leq \overline{B}$.
   ($\Leftarrow$) Suppose $\overline{A} \leq \overline{B}$ for $A, B \in \mathcal{A}$, and suppose $a \in A$ for some $a \in A$. Then $\overline{a} \in \overline{A}$ so that $\overline{a} \in \overline{B}$, hence there is some $b \in B$ such that $\overline{a} = \overline{b}$. It follows that $aN = bN$ so that $b^{-1}a \in N \subseteq B$, hence $a = b(b^{-1}a) \in B$. Therefore, $A \leq B$.
2. Consider a mapping $\psi : B/A \to \overline{B}/\overline{A}$ given by $\psi(bA) = \overline{b}\overline{A}$ for $b \in B$. To show ψ is well-defined, suppose $b_1A = b_2A$ for some $b_1, b_2 \in B$. Then $b_2^{-1}b_1 \in A$, hence $\overline{b_2^{-1}b_1} \in \overline{A}$ so that $\overline{b}_1\overline{A} = \overline{b}_2\overline{A}$, hence $\psi(b_1A) = \psi(b_2A)$. It is clear that ψ is a homomorphism, and it is surjective since for any $\overline{b}\overline{A} \in \overline{B}/\overline{A}$, there is some $b \in B$ such that $\psi(bA) = \overline{b}\overline{A}$. Finally, if $bA \in \ker\psi$, then $\psi(bA) = \overline{A}$ so that $\overline{b} \in \overline{A}$, hence $bN \in A/N$ or that $b \in A$. It follows that $\ker\psi = A/A = 1$, hence ψ is an isomorphism. Therefore, $|B : A| = |B/A| = |\overline{B}/\overline{A}| = |\overline{B} : \overline{A}|$.
3. $\overline{x} \in \overline{\langle A, B\rangle}$ if and only if $x = x_1x_2\ldots x_n$ where $x_i \in A \cup B$ for each $1 \leq i \leq n$ if and only if $\overline{x} = \overline{x_1x_2}\ldots\overline{x_n}$ where $\overline{x_i} \in \overline{A} \cup \overline{B}$ for each $1 \leq i \leq n$ if and only if $\overline{x} \in \langle\overline{A}, \overline{B}\rangle$, hence $\overline{\langle A, B\rangle} = \langle\overline{A}, \overline{B}\rangle$.
4. $\overline{x} \in \overline{A \cap B}$ if and only if $x \in A \cap B$ if and only if $x \in A$ and $x \in B$ if and only if $\overline{x} \in \overline{A}$ and $\overline{x} \in \overline{B}$ if and only if $\overline{x} \in \overline{A} \cap \overline{B}$, hence $\overline{A \cap B} = \overline{A} \cap \overline{B}$.
5. ($\Rightarrow$) Suppose $A \trianglelefteq G$, and let $gN \in \overline{G}$. Then for any $\overline{a} \in \overline{A}$ where $a \in A$, we have that $gag^{-1} \in A$ so that $gNg^{-1} = gag^{-1}N \in \overline{A}$, hence $\overline{A} \trianglelefteq \overline{G}$.
   ($\Leftarrow$) Suppose $\overline{A} \trianglelefteq \overline{G}$, and let $g \in G$. Then for any $a \in A$, we have that $\overline{g}\overline{a}\overline{g}^{-1} \in \overline{A}$ so that $gag^{-1}N \in A/N$, hence $gag^{-1} \in A$, thus $A \trianglelefteq G$. ■

(3) Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either
   (i) $K \leq H$ or
   (ii) $G = HK$ and $|K : K \cap H| = p$.

Solution. Since $H \trianglelefteq G$, then $N_G(H) = G$. Then $K \leq N_G(H)$, hence $KH \leq G$ by the Second Isomorphism Theorem. By Proposition 3.14, then $KH = HK$. Since we have $H \leq HK \leq G$, we may use Exercise 3.2.11 to conclude that $|G : H| = |G : HK| \cdot |HK : H|$. Since $|G : H| = p$ is prime, we have that $|G : HK|$ is either 1 or p. If the former is true, then $G = HK$. If the latter is true, then $HK = H$, hence $K \leq H$. In particular, if the former is true, then $|HK : H| = p$, and we may use the Second Isomorphism Theorem to conclude that $HK/H \cong K/(K \cap H)$ so that $|K : K \cap H| = |HK : H| = p$. ■

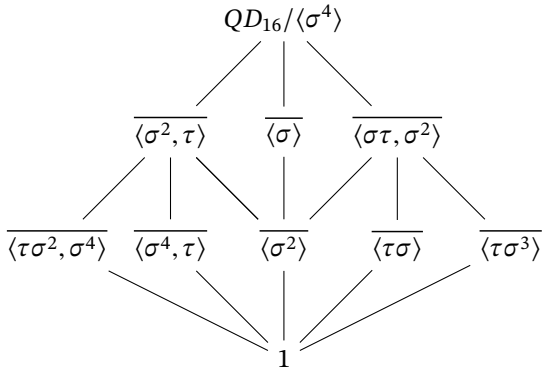
(4) Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

Solution. Consider the map $\varphi : A \times B \to (A/C) \times (B/D)$ given by $\varphi(a, b) = (aC, bD)$. This map is clearly well-defined and a homomorphism. Now suppose $\varphi((a, b)) = (C, D)$. Then $aC = C$ and $bD = D$, hence $a \in C$ and $b \in D$, so that $(a, b) \in C \times D$, hence $\ker\varphi \subseteq C \times D$. If $(c, d) \in C \times D$, then $\varphi((c, d)) = (cC, dD) = (C, D)$, so that $C \times D \subseteq \ker\varphi$. It follows that $\ker\varphi = C \times D$, hence $C \times D \trianglelefteq A \times B$. Lastly, φ is clearly surjective since

for any $(aC, bD) \in (A/C) \times (B/D)$, we have $\varphi((a,b)) = (aC, bD)$. By the First Isomorphism Theorem, we have $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$. ■

(5) Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group of order 16 in Exercise 2.5.11. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for QD_{16} to decide the isomorphism type of this group.

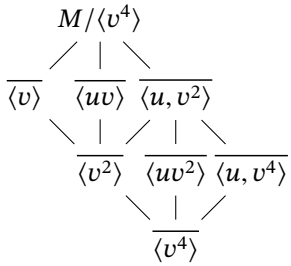
Solution. Note that $\tau\sigma^4\tau = \tau\tau\sigma^{12} = \sigma^4$, hence $\langle \sigma^4 \rangle \trianglelefteq QD_{16}$. By the Lattice Isomorphism Theorem, we may draw the following diagram:



Moreover, $\overline{\sigma^4} = \overline{\tau^2} = \bar{1}$ and $\overline{\tau\sigma} = \overline{\sigma^3\tau} = \overline{\sigma^{-1}\tau}$, then the generators $\bar{\sigma}$ and $\bar{\tau}$ satisfy the relations as r and s do in D_8, hence $QD_{16}/\langle \sigma^4 \rangle \cong D_8$. ■

(6) Let $M = \langle u, v \rangle$ be the modular group of order 16 in Exercise 2.5.14. Prove that $\langle v^4 \rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/\langle v^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for M to decide the isomorphism type of this group.

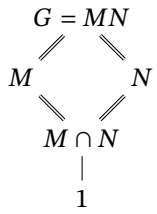
Solution. Note that $uv^4u = uuv^{20} = v^4$, hence $\langle v^4 \rangle \trianglelefteq M$. By the Lattice Isomorphism Theorem, we may draw the following diagram:



Moreover, $\overline{v^4} = \overline{u^2} = \bar{1}$ and $\overline{vu} = \overline{uv^5} = \overline{uv}$ so that the generators of $M/\langle v^4 \rangle$ satisfy the relations as a and b do in $Z_2 \times Z_4$, whose presentation is given in Exercise 2.5.12. Then $M/\langle v^4 \rangle \cong Z_2 \times Z_4$. ■

(7) Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$. [Draw the lattice.]

Solution. The lattice is given as the following, where double lines represent the quotient group $G/(M \cap N)$:



Now consider the mapping $\varphi : G \to (G/M) \times (G/N)$ given by $\varphi(g) = (gM, gN)$. This is clearly a homomorphism with $\ker\varphi = M \cap N$. Now let $(gM, hN) \in (G/M) \times (G/N)$. Since $G = MN$, there exist $m, m' \in M$ and $n, n' \in N$ such that $g = mn$ and $h = m'n'$. Then $\varphi(mn') = (mnM, mn'N) = (gM, hN)$, hence φ is surjective. By the First Isomorphism Theorem, we have $G/(M \cap N) \cong \varphi(G) = (G/M) \times (G/N)$. ■

(8) Let p be a prime and let G be the group of p-power roots of 1 in $\mathbb{C}$ (cf. Exercise 2.4.18). Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.

Solution. Let $\varphi(z) = z^p$ be the map. For any $z, w \in G$, then $\varphi(zw) = (zw)^p = z^p w^p = \varphi(z)\varphi(w)$, hence φ is a homomorphism. Moreover, for any $y \in G$, there is some $n \in \mathbb{Z}^+$ such that $y^{p^n} = 1$. Then let $z = y^{p^{n-1}}$, so that $z^p = y^{p^n} = 1$, hence $z \in G$ and $\varphi(z) = y$. It follows that φ is surjective. By the First Isomorphism Theorem, we have $G/\ker\varphi \cong G$. Since $\ker\varphi$ contains all p-power roots of unity of order dividing p, then $\ker\varphi$ is nontrivial, hence G is isomorphic to a proper quotient of itself. ■

(9) Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup with a normal subgroup N is a Sylow p-subgroup of N.)

Solution. Since $P \cap N \leq P$, Lagrange's Theorem concludes that $|P \cap N| = p^c$ for some $c \leq a$. Moreover, $c \leq b$ since $P \cap N \leq N$ where $|N| = p^b n$ where $p \nmid n$. Since $N \trianglelefteq G$, then $P \leq N_G(N) = G$ so that by the Second Isomorphism Theorem, we have $PN \leq G$, and $PN/N \cong P/(P \cap N)$. It now follows that $|PN/N| = |P/P \cap N| = p^{a-k}$.

Now note that $|G/N| = |G|/|N| = p^{a-b}m/n$, where $p \nmid m$ and $p \nmid n$. Since $PN/N \leq G/N$, then we may use Lagrange's Theorem again to conclude that $p^{a-k} \mid p^{a-b}$, hence $a - k \leq a - b$, or $k \geq b$. Since we showed previously that $k \leq b$, it follows that $k = b$, hence $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. ■

(10) Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Solution. It follows by the Second Isomorphism Theorem that $HN \leq G$ and $HN/N \cong H/(H \cap N)$. Note that

$$|HN| = \frac{|H||N|}{|H \cap N|} \quad \text{must divide} \quad |G| = |H||G : H|$$

Hence, $|N|/|H \cap N|$ divides $|G : H|$. Since $(|G : H|, |H|) = 1$, and $|N|/|H \cap N|$ divides $|G : H|$, it follows that $(|N|/|H \cap N|, |H|) = 1$, hence $(|N : H \cap N|, |H \cap N|) = 1$. Then $H \cap N$ is a Hall subgroup of N.

Now, observe that $|G/N : HN/N| = |G|/|HN| = |G : H|/|HN : H|$. Moreover, $|HN/N| = |H|/|H \cap N|$. Then $(|G/N : HN/N|, |HN/N|) = 1$ follows because $(|G : H|, |H|) = 1$, hence HN/N is a Hall subgroup of G/N. ■

3.4 Composition Series and the Hölder Program

(1) Prove that if G is an abelian simple group then $G \cong \mathbb{Z}_p$ for some prime p (do not assume G is a finite group).

Solution. Since G is simple, then its only subgroups are 1 and G. Since G is abelian, then all of its subgroups are normal. If G is trivial, then $G \cong Z_1$, which we exclude from this statement.

Consider now some nonidentity $g \in G$. Then $\langle g \rangle \leq G$. Since $g \neq 1$, and G is simple, it must be that $\langle g \rangle = G$, hence G is cyclic.

Now consider $|g| = n$. If $n = \infty$, then $\langle g^k \rangle$ is a proper nontrivial subgroup of G for any $k \in \mathbb{Z}^+$, contradicting that G is simple. Then n must be finite. If $n = ab$ for $a, b \in \mathbb{Z}^+$ where $1 < a, b < n$, then $\langle g^a \rangle$ is a proper nontrivial subgroup of G, again contradicting that G is simple. It follows that n is prime, hence $G \cong Z_n$ for some prime n. ■

(2) Exhibit all 3 composition series for Q_8 and all 7 composition series for D_8. List the composition factors in each case.

Solution. The composition series for Q_8 are as follows:

$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle i \rangle \trianglelefteq Q_8$$
$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle j \rangle \trianglelefteq Q_8$$
$$1 \trianglelefteq \langle -1 \rangle \trianglelefteq \langle k \rangle \trianglelefteq Q_8$$

The composition factors for each series are isomorphic to Z_2.

The composition series for D_8 are as follows:

$$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle rs \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^3 s \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$

with each composition factor isomorphic to Z_2. ■

(3) Find a composition series for the quasidihedral group of order 16 (cf. Exercise 2.5.11). Deduce that QD_{16} is solvable.

Solution. A clear composition series is $1 \trianglelefteq \langle \sigma^4 \rangle \trianglelefteq \langle \sigma^2 \rangle \trianglelefteq \langle \sigma \rangle \trianglelefteq QD_{16}$, with each composition factor isomorphic to Z_2. Since all composition factors are abelian, then QD_{16} is solvable. ■

(4) Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.

Solution. Let $|G| = m$. If $m = 1$, the result is trivial. If m is prime, then the result is trivial by Cauchy's Theorem.

Suppose the result is true for all groups with order less than m, and let $n \in \mathbb{Z}^+$ where $n \mid m$. If n is prime, then there exists $g \in G$ where $|g| = n$ by Cauchy's Theorem. Then $|g| \leq G$ is a subgroup of order n, and the result is true. Suppose now n is not prime. Then $n = kp$ for some prime divisor p of n. Since $p \mid m$, there exists an element $h \in G$ where $|h| = p$ by Cauchy's Theorem. Then $\langle h \rangle$ has order p, and $G/\langle h \rangle$ is a finite abelian group of order $m/p < m$. Since $k \mid m/p$, by the inductive hypothesis, there exists a subgroup $\overline{H}$ of $G/\langle h \rangle$ where $|\overline{H}| = k$. By the Lattice Isomorphism Theorem, there exists a subgroup H of G containing $\langle h \rangle$ such that $H/\langle h \rangle = \overline{H}$. Then $|H| = |\overline{H}||\langle h \rangle| = kp = n$, hence H is a subgroup of G of order n. By induction, the result holds for all finite abelian groups. ■

(5) Prove that subgroups and quotient groups of a solvable group are solvable.

Solution. Let G be a solvable group, and let $H \leq G$. Then there exists a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_{i+1}/G_i is abelian for each $0 \leq i \leq n-1$. Consider the set of subgroups $H_i = H \cap G_i$ for each $0 \leq i \leq n$. Note that $H_0 = H \cap G_0 = 1$ and $H_n = H \cap G_n = H$ since $H \leq G$. It is clear that $H_i \leq H_{i+1}$ for each $0 \leq i \leq n-1$. Moreover, let $g \in H_{i+1}$ and $x \in H_i$. Then $g \in G_{i+1}$ and $x \in G_i$. Since $G_i \trianglelefteq G_{i+1}$, then $gxg^{-1} \in G_i$. Moreover, $g, x \in H$ so that $gxg^{-1} \in H$, hence $gxg^{-1} \in H_i$. It follows that $H_i \trianglelefteq H_{i+1}$ for each $0 \leq i \leq n-1$. Note that $H_i = G_i \cap H = (G_i \cap G_{i+1}) \cap H = G_i \cap H_{i+1}$ so that by the Second Isomorphism Theorem, we have $H_{i+1}/H_i = H_{i+1}/(H_{i+1} \cap G_i) \cong H_{i+1}G_i/G_i \leq G_{i+1}/G_i$. Since G_{i+1}/G_i is abelian, then so is H_{i+1}/H_i. Therefore, H is solvable with the chain

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H$$

Now let $N \trianglelefteq G$. Consider the subgroups $N_i = G_iN$. Since it is clear that $N_i \leq N_{i+1}$, we need to show that $N_i \trianglelefteq N_{i+1}$. To that end, let $gn \in N_{i+1}$ and $hn' \in N_i$ for some $g \in G_{i+1}$, $h \in G_i$, and $n, n' \in N$. We now consider the element $gnhn'n^{-1}g^{-1} \in gnN_i(gn)^{-1}$. Since $h \in G_i \leq G$, then $nh = hn''$ for some $n'' \in N$, hence $gnhn'n^{-1}g^{-1} = ghn''n'n^{-1}g^{-1}$. Moreover, $(n''n'n^{-1})g^{-1} = g^{-1}n'''$ for $n''' \in N$ so we obtain $ghg^{-1}n''' \in N_i$ since $ghg^{-1} \in G_i$ because $G_i \trianglelefteq G_{i+1}$. It follows that $N_i \trianglelefteq N_{i+1}$. By the Lattice Isomorphism Theorem, then $N_i/N \trianglelefteq N_{i+1}/N$, and the Third Isomorphism Theorem concludes that $(N_{i+1}/N)/(N_i/N) \cong N_{i+1}/N_i$.

We now show N_{i+1}/N_i is abelian. Let $g_1n_1N_i, g_2n_2N_i \in N_{i+1}/N_i$ for some $g_1, g_2 \in G_{i+1}$ and $n_1, n_2 \in N$, and consider the product $(g_1n_1N_i)(g_2n_2N_i) = g_1g_2N_i$, where $g_1n_1g_2n_2 = g_1g_2n_3$ for some $n_3 \in N$ since $N \trianglelefteq G$. Since G_{i+1}/G_i is abelian, then $(g_1G_i)(g_2G_i) = (g_2G_i)(g_1G_i)$, which implies $g_1g_2g_1 = g_2g_1h$ for some $h \in G_i \leq N_i$. Hence, $g_1g_2N_i = g_2g_1hN_i = g_2g_1N_i$ so that N_{i+1}/N_i is abelian. Therefore, G/N is solvable with the chain

$$1 = N_0/N \trianglelefteq N_1/N \trianglelefteq \cdots \trianglelefteq N_n/N = G/N$$ ■

(6) Prove part (1) of the Jordan–Hölder Theorem by induction on $|G|$.

Solution. Let G be a finite group. If $G = 1$, then the result is trivial. Suppose now G is nontrivial and that the result holds for all groups of order less than $|G|$. If G is simple, then the composition series is $1 \trianglelefteq G$. Suppose now G is not simple, and let N be a maximal, normal subgroup of G. Since $|N| < |G|$, we may conclude by the inductive hypothesis that there exists a composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N$$

for some $k \in \mathbb{Z}^+$. Since $N \trianglelefteq G$ and G/N is simple, then the chain

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N \trianglelefteq G$$

is a composition series for G. By induction, the result holds for all finite groups. ■

(7) If G is a finite group and $H \trianglelefteq G$, prove that there is a composition series of G, one of whose terms is H.

Solution. If $H = G$, then the result follows trivially, since the last term in the composition series must be H. Now suppose H is a proper, normal subgroup of G. If $|G| = 1$, the result is trivial. Suppose $|G| > 1$, and assume the result is true for all groups with order less than $|G|$.

Since H is proper, then $|H| < |G|$, hence we have a composition series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H$$

by the inductive hypothesis. Now consider the quotient group G/H. Since $|G/H| < |G|$, then by the inductive hypothesis, there exists a composition series

$$1 = K_0/H \trianglelefteq K_1/H \trianglelefteq \cdots \trianglelefteq K_n/H = G/H$$

for some $n \in \mathbb{Z}^+$. By the Lattice Isomorphism Theorem, we have $H = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = G$. Since each $K_{i+1}/K_i \cong (K_{i+1}/H)/(K_i/H)$ is simple, then the chain

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = G$$

is a composition series for G with one of its terms equal to H. By induction, the result holds for all finite groups. ■

(8) Let G be a *finite* group. Prove that the following are equivalent:
(i) G is solvable.
(ii) G has a chain of subgroups
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$$
such that H_{i+1}/H_i is cyclic, $0 \leq i \leq s-1$.
(iii) All composition factors of G are of prime order.
(iv) G has a chain of subgroups
$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$$
such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t-1$.
[For (iv), prove that a minimal nontrivial normal subgroup M of G is necessarily abelian and then use induction. To see that M is abelian, let $N \trianglelefteq M$ be of prime index (by (iii)) and show that $x^{-1}y^{-1}xy \in N$ for all $x, y \in M$ (cf. Exercise 3.1.40). Apply the same argument to gNg^{-1} to show that $x^{-1}y^{-1}xy$ lies in the intersection of all G-conjugates of N, and use the minimality of M to conclude that $x^{-1}y^{-1}xy = 1$.]

Solution. **(i) (⇒) (ii)**: Suppose G is solvable, and consider the chain of subgroups
$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$
where G_{i+1}/G_i is abelian. We prove the following lemma: if A is a finite abelian group, then there exists a chain of subgroups
$$1 = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_k = A$$
such that A_{j+1}/A_j is cyclic. We prove this lemma by induction on $|A|$. If $|A| = 1$, the result is trivial. Suppose $|A| > 1$ and that the result holds for all abelian groups of order less than $|A|$. Since A is finite abelian, there exists some nonidentity $a \in A$ such that $\langle a \rangle \trianglelefteq A$. Then $|\langle a \rangle| < |A|$, hence by the inductive hypothesis, there exists a chain of subgroups
$$1 = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_m = \langle a \rangle$$
such that B_{j+1}/B_j is cyclic. Now consider the quotient group $A/\langle a \rangle$. Since $|A/\langle a \rangle| < |A|$, then by the inductive hypothesis, there exists a chain of subgroups
$$1 = C_0/\langle a \rangle \trianglelefteq C_1/\langle a \rangle \trianglelefteq \cdots \trianglelefteq C_\ell/\langle a \rangle = A/\langle a \rangle$$
for some $\ell \in \mathbb{Z}^+$. By the Lattice Isomorphism Theorem, we have $\langle a \rangle = C_0 \trianglelefteq C_1 \trianglelefteq \cdots \trianglelefteq C_\ell = A$. Since each $C_{i+1}/C_i \cong (C_{i+1}/\langle a \rangle)/(C_i/\langle a \rangle)$ is cyclic, then the chain
$$1 = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_m = \langle a \rangle = C_0 \trianglelefteq C_1 \trianglelefteq \cdots \trianglelefteq C_\ell = A$$
satisfies the lemma. By induction, the lemma holds for all finite abelian groups.

Applying this lemma to each abelian quotient G_{i+1}/G_i in the original chain, we obtain a chain of subgroups
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$$
such that H_{i+1}/H_i is cyclic, hence (ii) holds.

(ii) (⇒) (iii): Suppose G has a chain of subgroups
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$$
such that H_{i+1}/H_i is cyclic. We prove that each composition factor of G is of prime order. We prove this by induction on $|G|$. If $|G| = 1$, the result is trivial. Suppose $|G| > 1$ and that the result holds for all groups of order less than $|G|$. Since $H_{s-1} \trianglelefteq G$ and G/H_{s-1} is cyclic, then $G/H_{s-1} \cong Z_n$ for some $n \in \mathbb{Z}^+$. If n is prime, then the composition factors of G/H_{s-1} are of prime order. Since $|H_{s-1}| < |G|$, then by the inductive hypothesis, the composition factors of H_{s-1} are also of prime order, hence all composition factors of G are of prime order. Suppose now n is not prime, so that $n = km$ for some $k, m \in \mathbb{Z}^+$ where $1 < k, m < n$. Then Z_n has a proper, nontrivial subgroup $\langle a^m \rangle$ of order k. Let $\pi : G \to G/H_{s-1}$ be the natural projection, and let $K = \pi^{-1}(\langle a^m \rangle)$. Then $H_{s-1} \trianglelefteq K \trianglelefteq G$ so that by the Lattice Isomorphism Theorem, $K/H_{s-1} \cong \langle a^m \rangle$ is a proper, nontrivial subgroup of G/H_{s-1}, contradicting that H_{s-1} is maximal normal in G. It follows that n must

be prime, hence all composition factors of G are of prime order. By induction, the result holds for all finite groups.

(iii) (⇒) (iv): Suppose all composition factors of G are of prime order. We prove that G has a chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$$

such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian. Let M be a minimal, nontrivial normal subgroup of G, and suppose $N \trianglelefteq M$ have prime index. Then for any $x, y \in M$, we have $x^{-1}y^{-1}xy \in N$ since M/N is abelian. Now for any $g \in G$, consider $gNg^{-1} \trianglelefteq gMg^{-1} = M$. By the same argument, we have $x^{-1}y^{-1}xy \in gNg^{-1}$ for all $x, y \in M$. It follows that $x^{-1}y^{-1}xy$ lies in the intersection of all G-conjugates of N. Since M is minimal normal in G, then this intersection is either 1 or M. If it were M, then M would be abelian, contradicting that M/N is nontrivial. Hence, $x^{-1}y^{-1}xy = 1$ for all $x, y \in M$, so that M is abelian.

(iv) (⇒) (i): This implication is immediate from the definition of solvable groups. ■

(9) Prove the following special case of part (2) of the Jordan–Hölder Theorem: assume the finite group G has two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G \quad \text{and} \quad 1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G.$$

Show that $r = 2$ and that the list of composition factors is the same. [Use the Second Isomorphism Theorem.]

Solution. Consider $H = N_{r-1} \cap M_1$. Then $H \trianglelefteq M_1$. Since $M_1/1 \cong M_1$ is simple, then either $H = 1$ or $H = M_1$. If $H = M_1$, then $N_{r-1} \trianglelefteq M_1$. By simplicity of M_1, it must be that $N_{r-1} = M_1$ so that $r = 2$. Both composition series are then the same, so we now suppose $H = 1$.

Noting that $M_1 \trianglelefteq G$ and $N_{r-1} \trianglelefteq G$, we may use the Second Isomorphism Theorem to conclude that $N_{r-1}M_1/M_1 \cong N_{r-1}/(N_{r-1} \cap M_1) = N_{r-1}/1 \cong N_{r-1}$. Observe now that $M_1 \leq N_{r-1}M_1 \leq G$, hence $N_{r-1}M_1/M_1 \trianglelefteq G/M_1$. By simplicity of G/M_1, it must be that $N_{r-1}M_1 = 1$ or $N_{r-1}M_1 = G$. Since N_{r-1} is not trivial, it must be that $N_{r-1}M_1 = G$. Now, N_{r-1} is simple, hence $N_{r-2} = 1 = N_0$, and we may conclude that $r = 2$. Moreover, the composition factors are isomorphic:

$$G/N_{r-1} \cong M_1/(N_{r-1} \cap M_1) \cong M_1 \quad \text{and} \quad N_{r-1}/1 \cong N_{r-1} \cong G/M_1 \qquad \blacksquare$$

(10) Prove part (2) of the Jordan–Hölder Theorem by induction on $\min\{r, s\}$. [Apply the inductive hypothesis to $H = N_{r-1} \cap M_{s-1}$ and use the preceding exercises.]

Solution. Suppose G has two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G \tag{♣}$$

and

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_s = G. \tag{♠}$$

We induct on $\min\{r, s\}$. By the previous exercise, we may assume that $\min\{r, s\} > 2$. Suppose the statement is true for $\min\{r, s\} < k$ for some $k > 2$, and let $\min\{r, s\} = k$. Let $H = N_{r-1} \cap M_{s-1}$. If $N_{r-1} \leq M_{s-1}$ is proper, then by simplicity of M_{s-1}, it must be that $N_{r-1} = 1$, contradicting that N_{r-1} is nontrivial. Hence, $N_{r-1} \trianglelefteq M_{s-1}$. By a similar argument, we have $M_{s-1} \trianglelefteq N_{r-1}$. If we have $M_{s-1} = N_{r-1}$, then by the previous exercise, the composition factors of both series are the same, so we now suppose $M_{s-1} \neq N_{r-1}$ and they are not contained in one another. They are then proper normal subgroups of $M_{s-1}N_{r-1}$. If $M_{s-1}N_{r-1} \neq G$, then $M_{s-1}N_{r-1} \trianglelefteq G$ is proper, so by simplicity of G/N_{r-1}, it must be that $M_{s-1}N_{r-1} = N_{r-1}$, contradicting that $M_{s-1} \trianglelefteq N_{r-1}$. Hence, $M_{s-1}N_{r-1} = G$. We may use the Second Isomorphism Theorem to conclude that

$$M_{s-1}/H \cong M_{s-1}N_{r-1}/N_{r-1} = G/N_{r-1} \tag{♡}$$

and

$$N_{r-1}/H \cong M_{s-1}N_{r-1}/M_{s-1} = G/M_{s-1}. \tag{♢}$$

which shows that both M_{s-1}/H and N_{r-1}/H are simple. Consider now the composition series for H:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t = H. \tag{★}$$

It is clear that appending N_{r-1} to the series (★) gives a composition series for N_{r-1}. Similarly, we get a composition series for M_{s-1}. Moreover, there are $r-2$ factors for the series for N_{r-1} and $s-2$ factors for the series for M_{s-1}. Since $\min\{r-1, s-1\} = k-1 < k$, then by the inductive hypothesis, both series have the same number of factors and the same composition factors up to isomorphism. Therefore, $r-2 = s-2$ so that $r = s$. In (♣) and (♠), both series have $r-2$ factors isomorphic to (★) up to some order, and the last 2 factors in (♡) and (♢) are isomorphic to G/N_{r-1} and G/M_{s-1} respectively. The result then follows by induction. ■

(11) Prove that if H is a nontrivial normal subgroup of the solvable group G then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.

Solution. Since G is solvable, we have the sequence

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

where G_{i+1}/G_i is abelian. Let $H_i = H \cap G_i$ for each $0 \leq i \leq n$. Since H is nontrivial, consider the set of indices $I = \{i \in \mathbb{Z}^+ \mid G_i \cap H \neq 1\}$. Since $H_n = H$, then I is nonempty. By the Well Ordering Property, there exist some minimal index k such that $H_k = G_k \cap H \neq 1$ but $H_{k-1} = G_{k-1} \cap H = 1$. Note that $H_k \trianglelefteq G$ since $H \trianglelefteq G$ and $G_k \trianglelefteq G$. Moreover, by the Second Isomorphism Theorem, we have

$$H_k \cong H_k/1 = H_k/(H_k \cap G_{k-1}) \cong H_k G_{k-1}/G_{k-1} \leq G_k/G_{k-1}$$

Since G_k/G_{k-1} is abelian, then so is H_k. Therefore, $A = H_k$ is a nontrivial, abelian normal subgroup of G contained in H. ■

(12) Prove (without using the Feit–Thompson Theorem) that the following are equivalent:
(i) Every group of odd order is solvable.
(ii) The only simple groups of odd order are those of prime order.

Solution. **(i) (⇒) (ii)** Suppose every group of odd order is solvable. Let G be a simple group of odd order. Since G is solvable, then by the characterization of solvable groups, all composition factors of G are of prime order. Since G is simple, then its only composition series is $1 \trianglelefteq G$, hence G is of prime order.
(ii) (⇒) (i) Suppose the only simple groups of odd order are those of prime order. Let G be a group of odd order. We want to show that G is solvable. Consider a composition series of G:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

Each composition factor G_{i+1}/G_i is simple and of odd order, so by assumption, each is of prime order and hence abelian. Therefore, G is solvable. ■

3.5 Transpositions and the Alternating Group

(1) In Exercise 1.3.1 and Exercise 1.3.2 you were asked to find the cycle decomposition of some permutations. Write each of these permutations as a product of transpositions. Determine which of these is an even permutation and which is an odd permutation.

Solution. For Exercise 1.3.1, odd permutations are σ, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$, while even permutations are τ and σ^2. For Exercise 1.3.2, odd permutations are τ, $\tau\sigma$, and $\tau^2\sigma$, while even permutations are σ, σ^2, and $\sigma\tau$. ■

(2) Prove that σ^2 is an even permutation for every permutation σ.

Solution. Let σ be a permutation with a transposition product $\tau_1\tau_2\cdots\tau_k$. Then σ^2 has $2k$ transpositions in its product, hence is even. ■

(3) Prove that S_n is generated by $\{(i\ i+1) \mid 1 \le i \le n-1\}$. [Consider conjugates, viz. $(2\ 3)(1\ 2)(2\ 3)^{-1}$.]

Solution. Inducting on n, note that the base case is trivial. Let $T_n = \langle (i\ i+1) \mid 1 \le i \le n-1\rangle$. Suppose that $S_n = T_n$ for some $n \ge 1$, and consider some $\sigma \in S_{n+1}$. Write σ as a product of transpositions, and let $(j\ k)$ be a transposition in σ.

There are 2 cases to consider. If $1 \le j < k \le n$, then $(j\ k) \in S_n = T_n$ by the inductive hypothesis. If $k = n+1$ and $j = n$, then $(j\ k) \in T_{n+1}$ by definition. Suppose now that $1 \le j < k = n+1$ where $j < n$. Note that

$$(j\ n+1) = (n\ n+1)(j\ n)(n\ n+1)$$

where each transposition on the right-hand side is in T_{n+1} (in particular, $(j\ n) \in S_n = T_n$ by the inductive hypothesis). It follows that $(j\ k) \in T_{n+1}$ for all transpositions in σ, hence $\sigma \in T_{n+1}$. By induction, the result holds for all $n \ge 1$. ■

(4) Show that $S_n = \langle (1\ 2), (1\ 2\ 3\ldots n)\rangle$ for all $n \ge 2$.

Solution. Note that $(1\ 2\ 3\ldots n)(1\ 2)(1\ 2\ 3\ldots n)^{-1} = (2\ 3)$. We may conjugate $(2\ 3)$ by the n-cycle again to get $(3\ 4)$, and so on until an arbitrary $(i\ i+1) = (1\ 2\ 3\ldots n)^{i-1}(1\ 2)(1\ 2\ 3\ldots n)^{-(i-1)}$ is obtained for each $1 \le i < n$. By the previous exercise, then $S_n = \langle (1\ 2), (1\ 2\ 3\ldots n)\rangle$. ■

(5) Show that if p is prime, $S_p = \langle \sigma, \tau\rangle$ where σ is any transposition and τ is any p-cycle.

Solution. It is clear that the set of all transpositions is equal to S_n, since any permutation in S_n can be written as a product of transpositions. Let $\sigma = (i\ j)$ and τ be a p-cycle. Note that there exists some power k such that $\tau^k(i) = 1$. Then $\sigma' = \tau^k\sigma\tau^{-k} = (1\ \tau^k(j))$ is a transposition in $\langle \sigma, \tau\rangle$. We claim that every transposition of the form $(1\ k) \in \langle \sigma, \tau\rangle$ for $2 \le k \le p$, and we proceed by induction. The base case of $(1\ \tau^k(j))$ is done. Suppose $(1\ m) \in \langle \sigma, \tau\rangle$ for some $2 \le m < p$. Note that there must exist some power n such that $\tau^n(1) = m$. Then $\tau^n(1\ \tau^k(j))\tau^{-n} = (m\ \tau^{n+k}(j))$ lies in $\langle \sigma, \tau\rangle$. Then $(1\ \tau^{n+k}(j)) = (1\ m)(m\ \tau^{n+k}(j))(1\ m) \in \langle \sigma, \tau\rangle$. By induction, every transposition of the form $(1\ k)$ is in $\langle \sigma, \tau\rangle$. Then for any transposition $(a\ b)$, we have $(a\ b) = (1\ a)(1\ b)(1\ a) \in \langle \sigma, \tau\rangle$. It follows that all transpositions are in $\langle \sigma, \tau\rangle$, hence $S_p = \langle \sigma, \tau\rangle$. ■

(6) Show that $\langle (1\ 3), (1\ 2\ 3\ 4)\rangle$ is a proper subgroup of S_4. What is the isomorphism type of this subgroup?

Solution. Put $\tau = (1\ 3)$ and $\sigma = (1\ 2\ 3\ 4)$. Then $\sigma^4 = \tau^2 = 1$. Moreover, $\sigma\tau = (1\ 2\ 3\ 4)(1\ 3) = (1\ 4)(2\ 3)$, and $\tau\sigma^{-1} = (1\ 3)(4\ 3\ 2\ 1) = (1\ 4)(2\ 3)$, so that $\sigma\tau = \tau\sigma^{-1}$. This satisfies the same relations in S_4 as r and s do in D_8. We then define a surjective homomorphism $\varphi : D_8 \to \langle \sigma, \tau\rangle$ by $\varphi(r) = \sigma$ and $\varphi(s) = \tau$. Then $\langle \sigma, \tau\rangle$ has at most 8 elements, showing that it is a proper subgroup of S_4. It is easy to see that φ maps to distinct elements in $\langle \sigma, \tau\rangle$, hence $|\langle \sigma, \tau\rangle| = 8$ and φ is an isomorphism. Therefore, $\langle \sigma, \tau\rangle \cong D_8$. ■

(7) Prove that the group of rigid motions of a tetrahedron is isomorphic to A_4. [Recall Exercise 1.7.20.]

Solution. By Exercise 1.7.20, we know that the group of rigid motions is isomorphic to a subgroup of S_4. Moreover, Exercise 1.2.9 shows that this group has order 12. We claim that the subgroup of S_4 that this group is isomorphic to is A_4.

The group of rigid motions of a tetrahedron consists of the following elements: the identity, 8 rotations about axes through a vertex and the center of the opposite face (by 120° or 240°), and 3 rotations about axes

through the midpoints of opposite edges (by 180°). The identity is even, the 8 rotations about vertices are even (since they correspond to 3-cycles in S_4), and the 3 rotations about midpoints of edges are also even (since they correspond to products of two disjoint transpositions in S_4). Therefore, all 12 elements of the group of rigid motions are even permutations, so the group is isomorphic to a subgroup of A_4. Since both groups have order 12, it follows that the group of rigid motions of a tetrahedron is isomorphic to A_4. ■

(8) Prove the lattice of subgroups of A_4 given in the text is correct. (By the preceding exercise and the comments following Lagrange's Theorem, A_4 has no subgroup of order 6.)

Solution. The previous exercise shows that A_4 is isomorphic to the group of rigid motions of a tetrahedron, where the text shows that this group cannot have a subgroup of order 6.

We know that a subgroup of A_4 with order 4 must be isomorphic to either Z_4 or V_4. Since the symmetries of A_4 have either order 1 (the identity), order 2 (the 180° rotations about midpoints of opposite edges), or order 3 (the 120° and 240° rotations about vertices), there are no elements of order 4 in A_4. Therefore, the unique subgroup of order 4 in A_4 must be isomorphic to V_4, namely $\langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle$. Moreover, this is the only subgroup of order 4 in A_4 since any other subgroup of order 4 would necessarily contain different elements of order 2, which there are none of besides in this subgroup.

The remaining potential subgroup orders of A_4 are 2 or 3, both of which are cyclic. Since the lattice shows 4 cyclic subgroups of order 3 that contain all 8 elements of order 3 in A_4, and 3 cyclic subgroups of order 2 that contain all 3 elements of order 2 in A_4, the lattice is correct. ■

(9) Prove that the (unique) subgroup of order 4 in A_4 is normal and is isomorphic to V_4.

Solution. The above discussion shows that A_4 is isomorphic to V_4. Moreover, this subgroup is generated by all elements of order 2 in A_4. By Exercise 3.1.26, this subgroup is normal in A_4. ■

(10) Find a composition series for A_4. Deduce that A_4 is solvable.

Solution. Since the subgroup lattice is correct, we know that the subgroup of order 4 is maximal and normal in A_4. Moreover, it is abelian. Therefore, we have the composition series

$$1 \trianglelefteq \langle (1\,2)(3\,4)\rangle \trianglelefteq \langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle \trianglelefteq A_4$$

where each composition factor is of prime order. By the characterization of solvable groups, A_4 is solvable. ■

(11) Prove that S_4 has no subgroup isomorphic to Q_8.

Solution. If such a subgroup H of S_4 existed, then it would contain all elements of order 4 in S_4 (of which there are 6) since Q_8 has 6 elements of order 4. However, this implies that $(1\,2\,3\,4)^2 = (1\,3)(2\,4) \in H$ and $(1\,4\,3\,2)^2 = (1\,4)(2\,3) \in H$. Along with the identity, this shows that H contains more than 8 elements, a contradiction. Therefore, no such subgroup exists. ■

(12) Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.

Solution. Recall that A_n contains only even permutations, while S_{n-2} contain both even and odd permutations. Our homomorphism must then mapp odd permutations of S_{n-2} to even permutations of A_n, while ensuring that the original action of the permutation in S_{n-2} is preserved. Hence, we "add" on a transposition to odd permutations in S_{n-2} to make them even in A_n. We then define the map $\varphi : S_{n-2} \to A_n$ by

$$\varphi(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even,} \\ \sigma \circ (n-1\ n) & \text{if } \sigma \text{ is odd.} \end{cases}$$

Now suppose $\sigma, \tau \in S_{n-2}$. There are 3 cases to consider:
1. If both σ and τ are even, then $\varphi(\sigma\tau) = \sigma\tau = \varphi(\sigma)\varphi(\tau)$.
2. If both σ and τ are odd, then $\varphi(\sigma\tau) = \sigma \circ (n-1\ n)\tau \circ (n-1\ n) = \varphi(\sigma)\varphi(\tau)$.
3. Without loss of generality, assume σ is even and τ is odd. Then $\varphi(\sigma\tau) = \sigma\tau \circ (n-1\ n) = \varphi(\sigma)\varphi(\tau)$.

In all cases, $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$, so φ is a homomorphism. It is clear that φ is injective, since if $\varphi(\sigma) = \varphi(\tau)$, then either both σ and τ are even or both are odd, so that $\sigma = \tau$. Therefore, φ is an injective homomorphism from S_{n-2} to A_n, showing that A_n contains a subgroup isomorphic to S_{n-2}. ■

(13) Prove that every element of order 2 in A_n is the square of an element of order 4 in S_n. [An element of order 2 in A_n is a product of $2k$ commuting transpositions.]

Solution. By the hint, every element of order 2 in A_n contains a pair of cycles of the form $(a\ b)(c\ d)$. Note that $(a\ c\ b\ d)^2 = (a\ b)(c\ d)$, and $(a\ c\ b\ d)$ is of order 4 in S_n. Then any element of order 2 in A_n can be written as the square of an element of order 4 in S_n by grouping its transpositions into pairs and applying this construction to each pair. ■

(14) Prove that the subgroup of A_4 generated by any element of order 2 and any element of order 3 is all of A_4.

Solution. Observing the lattice was proven correct in Exercise 3.5.8, we see that any subgroup generated by an element σ of order 2 and an element τ of order 3. Then $\langle\sigma\rangle$ is a proper subgroup of $\langle\sigma,\tau\rangle$, but the lattice shows that $\langle\sigma\rangle$ is maximal in A_4. Therefore, $\langle\sigma,\tau\rangle = A_4$. ■

(15) Prove that if x and y are distinct 3-cycles in S_4 with $x \neq y^{-1}$, then the subgroup of S_4 generated by x and y is A_4.

Solution. Using the same argument in the previous exercise, we note that $\langle x\rangle$ and $\langle y\rangle$ are distinct, proper subgroups of $\langle x,y\rangle$. Since both are maximal in A_4, it follows that $\langle x,y\rangle = A_4$. ■

(16) Let x and y be distinct 3-cycles in S_5 with $x \neq y^{-1}$.

(a) Prove that if x and y fix a common element of $\{1,\dots,5\}$, then $\langle x,y\rangle \cong A_4$.

(b) Prove that if x and y do not fix a common element of $\{1,\dots,5\}$, then $\langle x,y\rangle = A_5$.

Solution.

(a) Consider $X = \{1,2,3,4,5\} - \{i\}$, where $i \in \{1,2,3,4,5\}$ is the common element being fixed by both x and y. Then x and y act only on X. Define the map $\varphi : \langle x,y\rangle \to S_4$ given by $\varphi(\sigma) = \sigma|_X$. It is clear that φ is a homomorphism.

Now suppose $\sigma \in \ker\varphi$. Then σ fixes all elements in X as well as i, so that σ is the identity. Therefore, φ is injective. We now look at $\varphi(\langle x,y\rangle) = \langle\varphi(x),\varphi(y)\rangle$. Since φ is injective, it follows that $\varphi(x) \neq \varphi(y)$ and $\varphi(x) \neq \varphi(y)^{-1}$ if $x \neq y$ and $x \neq y^{-1}$. By the previous exercise, we have distinct 3-cycles in S_4 such that one is not equal to the other's inverse, so that $\langle\varphi(x),\varphi(y)\rangle = A_4$. Therefore, $\langle x,y\rangle \cong A_4$.

(b) Put $x = (a\ b\ c)$ and $y = (a\ d\ e)$ for distinct $a,b,c,d,e \in \{1,2,3,4,5\}$. Then $xy = (a\ d\ e\ b\ c)$ is a 5-cycle, hence $\langle x,y\rangle$ contains a subgroup of order 5. Moreover, $yxy^{-1} = (b\ c\ d)$ and $xyx^{-1} = (b\ d\ e)$, both of which are distinct 3-cycles not equal to each other's inverses. Hence, $\langle x,y\rangle$ contains a subgroup isomorphic to A_4, which has order 12. By Langrange's Theorem then $\langle x,y\rangle$ must have order of at least 60, hence $\langle x,y\rangle = A_5$. ■

(17) If x and y are 3-cycles in S_n, prove that $\langle x,y\rangle$ is isomorphic to $\mathbb{Z}_3$, A_4, A_5, or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Solution. There are 4 cases to consider:

1. If x and y act on the same 3 elements, they are either the same cycle or inverses of each other. In this case, $\langle x,y\rangle = \langle x\rangle \cong Z_3$.
2. If x and y act on 4 elements, they must fix a common element, hence $\langle x,y\rangle \cong A_4$ by part (a) of the previous exercise.
3. If x and y act on 5 elements and do not fix a common element, then $\langle x,y\rangle = A_5$ by part (b) of the previous exercise.
4. If x and y act on 6 elements, then they are disjoint and commute. We show that $\langle x,y\rangle \cong Z_3 \times Z_3$. Let $z \in Z_3$ such that $\langle z\rangle = Z_3$, and define the map $\varphi : \langle x,y\rangle \to Z_3 \times Z_3$ by $\varphi(x^a y^b) = (z^a, z^b)$ for $a,b \in \{0,1,2\}$. It is clear that φ is a homomorphism. Suppose $\varphi(x^a y^b) = (1,1)$. Then $z^a = 1$ and $z^b = 1$, so that $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$. Therefore, $x^a y^b = 1$, showing that φ is injective. It is clear that $|\langle x,y\rangle| = 9 = |Z_3 \times Z_3|$, since there are 3 choices for both a and b. Hence, φ is an isomorphism, and $\langle x,y\rangle \cong Z_3 \times Z_3$. ■

4 Group Actions

4.1 Group Actions and Permutation Representations

Let G be a group and let A be a nonempty set.

(1) Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is

$$\bigcap_{g \in G} gG_ag^{-1}.$$

Solution. Suppose $h \in G_b$. We want to show that $h \in gG_ag^{-1}$. Since $h \in G_b$, we have $h \cdot b = b$. But $b = g \cdot a$, so $h \cdot (g \cdot a) = g \cdot a$. Applying g^{-1} to both sides, we get $g^{-1}hg \cdot a = a$. This means that $g^{-1}hg \in G_a$, so $h \in gG_ag^{-1}$. Thus, we have shown that $G_b \subseteq gG_ag^{-1}$. For the other direction, suppose $h \in gG_ag^{-1}$. Then there exists some $k \in G_a$ such that $h = gkg^{-1}$. We want to show that $h \in G_b$. We have $h \cdot b = (gkg^{-1}) \cdot (g \cdot a) = g \cdot (k \cdot a) = g \cdot a = b$, since $k \in G_a$ implies $k \cdot a = a$. Thus, $h \in G_b$. Therefore, we have shown that $gG_ag^{-1} \subseteq G_b$. Combining both inclusions, we conclude that $G_b = gG_ag^{-1}$.

Now, if G acts transitively on A, then for any $b \in A$, there exists some $g \in G$ such that $b = g \cdot a$. From the first part, we have $G_b = gG_ag^{-1}$. The kernel of the action is the intersection of all stabilizers G_b for $b \in A$. Therefore, the kernel is

$$\bigcap_{b \in A} G_b = \bigcap_{g \in G} gG_ag^{-1}. \qquad \blacksquare$$

(2) Let G be a permutation group on the set A (i.e., $G \leq S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1.$$

Solution. Suppose $\tau \in \sigma G_a \sigma^{-1}$. We want to show that $\tau \in G_{\sigma(a)}$. Since $\tau \in \sigma G_a \sigma^{-1}$, there exists some $\rho \in G_a$ such that $\tau = \sigma\rho\sigma^{-1}$. We have $\tau \cdot \sigma(a) = (\sigma\rho\sigma^{-1}) \cdot \sigma(a) = \sigma \cdot (\rho \cdot a) = \sigma(a)$, since $\rho \in G_a$ implies $\rho \cdot a = a$. Thus, $\tau \in G_{\sigma(a)}$. Therefore, we have shown that $\sigma G_a \sigma^{-1} \subseteq G_{\sigma(a)}$. For the other direction, suppose $\tau \in G_{\sigma(a)}$. We want to show that $\tau \in \sigma G_a \sigma^{-1}$. We have $\tau \cdot \sigma(a) = \sigma(a)$. Applying σ^{-1} to both sides, we get $\sigma^{-1}\tau\sigma \cdot a = a$. This means that $\sigma^{-1}\tau\sigma \in G_a$, so $\tau \in \sigma G_a \sigma^{-1}$. Thus, we have shown that $G_{\sigma(a)} \subseteq \sigma G_a \sigma^{-1}$. Combining both inclusions, we conclude that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$.

Now, if G acts transitively on A, then for any $b \in A$, there exists some $\sigma \in G$ such that $b = \sigma(a)$. From the first part, we have $\sigma G_a \sigma^{-1} = G_b$. The kernel of the action is the intersection of all stabilizers G_b for $b \in A$. Therefore, the kernel is

$$\bigcap_{b \in A} G_b = \bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1. \qquad \blacksquare$$

(3) Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. [Use the preceding exercise.]

Solution. Since G is abelian, then the conjugate of G_a is trivial, i.e., $\sigma G_a \sigma^{-1} = G_a$ for all $\sigma \in G$. From the previous exercise, we know that the kernel of this action is trivial. However, the intersection of all $\sigma G_a \sigma^{-1}$ is just G_a so that $G_a = 1$. Then G_a is trivial for every $a \in A$, hence $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. It follows by Proposition 4.2 that $|G|/|G_a| = |A|$, hence $|G| = |A|$ because G_a is trivial. $\blacksquare$

(4) Let S_3 act on the set Ω of ordered pairs $\{(i, j) \mid 1 \leq i, j \leq 3\}$ by $\sigma((i, j)) = (\sigma(i), \sigma(j))$. Find the orbits of S_3 on Ω. For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9—first fix a labeling of these nine ordered pairs). For each orbit O of S_3 acting on these nine points, pick some $a \in O$ and find the stabilizer of a in S_3.

Solution. Note that in Ω, there are two types of ordered pairs: those with identical elements and those with distinct elements. In the former case, it is clear that any $\sigma \in S_3$ will map such a pair to another pair with identical elements. In the latter case, it is easy to find some $\sigma \in S_3$ that maps any ordered pair with distinct elements to any other such pair. We now label the elements of Ω accordingly:

- $1 = (1,1)$
- $2 = (2,2)$
- $3 = (3,3)$
- $4 = (1,2)$
- $5 = (2,1)$
- $6 = (1,3)$
- $7 = (3,1)$
- $8 = (2,3)$
- $9 = (3,2)$

We then have the two orbits

$$O_1 = \{(i,i) \mid i \in \{1,2,3\}\} \quad \text{and} \quad O_2 = \{(i,j) \mid i \neq j\}$$

of S_3 acting on Ω. Note that $|O_1| = 3$ and $|O_2| = 6$. Now for each $\sigma \in S_3$, we find its cycle decomposition as an element of S_9. We describe how to compute one such cycle decomposition, and the rest follow similarly. Consider $\sigma = (123) \in S_3$. Then we have the following mappings:
- $(1,1) \mapsto (2,2) \mapsto (3,3) \mapsto (1,1)$, which corresponds to the cycle (1 2 3) in S_9.
- $(1,2) \mapsto (2,3) \mapsto (3,1) \mapsto (1,2)$, which corresponds to the cycle (4 8 7) in S_9.
- $(2,1) \mapsto (3,2) \mapsto (1,3) \mapsto (2,1)$, which corresponds to the cycle (5 9 6) in S_9.

Combining these cycles, we find that the cycle decomposition of $\sigma = (123)$ in S_9 is (1 2 3)(4 8 7)(5 9 6). The cycle decompositions for all elements of S_3 acting on Ω are as follows:
- $1 \in S_3$ is the same as $1 \in S_9$.
- (12): (1 2)(4 5)(6 7)(8 9)
- (13): (1 3)(4 6)(5 7)(8 9)
- (23): (1 2)(2 3)(5 6)(7 8)
- (123): (1 2 3)(4 8 7)(5 9 6)
- (132): (1 3 2)(4 7 8)(5 6 9)

For O_1, we pick $a = (1,1)$. The only $\sigma \in S_3$ that fixes $(1,1)$ is the identity permutation and (2 3), so the stabilizer of $(1,1)$ in S_3 is $\langle(2\ 3)\rangle$. Moreover, we have $|G_a||O_1| = 2 \cdot 3 = 6 = |S_3|$ as expected. For O_2, we pick $a = (1,2)$. The only $\sigma \in S_3$ that fixes $(1,2)$ is the identity permutation, so the stabilizer of $(1,2)$ in S_3 is 1. Again, $|G_a||O_2| = 1 \cdot 6 = 6 = |S_3|$. ■

(5) For each of parts (a) and (b) repeat the preceding exercise but with S_3 acting on the specified set:

(a) the set of 27 triples $\{(i,j,k) \mid 1 \leq i,j,k \leq 3\}$

(b) the set $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$ of all 7 nonempty subsets of $\{1,2,3\}$

Solution.

(a) We begin by classifying these set of triples. There are five types of triples:
- Type 1: Triples with all identical elements.
- Type 2: Triples whose two first coordinates are identical.
- Type 3: Triples whose first and last coordinates are identical.
- Type 4: Triples whose last two coordinates are identical.
- Type 5: Triples with all distinct elements.

Note that this is a correct classification. One may suggest to combine Types 2, 3, and 4 into a singular type. However, observe that no elements may be permuted such that the location of a pair of identical coordinates move to another one, i.e., there is no such permutation σ in S_3 such that $(1,1,2)$ maps to $(1,2,2)$.We now label the elements of Ω lexicographically as follows, i.e., we begin by increasing the last coordinate, then increasing the middle coordinate, and finally increasing the first coordinate:
- $1 = (1,1,1)$
- $2 = (1,1,2)$
- $3 = (1,1,3)$
- $4 = (1,2,1)$
- $5 = (1,2,2)$
- $6 = (1,2,3)$
- $7 = (1,3,1)$
- $8 = (1,3,2)$
- $9 = (1,3,3)$
- $10 = (2,1,1)$
- $11 = (2,1,2)$
- $12 = (2,1,3)$
- $13 = (2,2,1)$
- $14 = (2,2,2)$
- $15 = (2,2,3)$
- $16 = (2,3,1)$
- $17 = (2,3,2)$
- $18 = (2,3,3)$
- $19 = (3,1,1)$
- $20 = (3,1,2)$
- $21 = (3,1,3)$
- $22 = (3,2,1)$
- $23 = (3,2,2)$
- $24 = (3,2,3)$
- $25 = (3,3,1)$
- $26 = (3,3,2)$
- $27 = (3,3,3)$

The classification yields the following orbits of S_3 acting on Ω:
- $O_1 = \{(i,i,i) \mid i \in \{1,2,3\}\}$ with order 3.
- $O_2 = \{(i,i,j) \mid i \neq j\}$ with order 6.
- $O_3 = \{(i,j,i) \mid i \neq j\}$ with order 6.
- $O_4 = \{(j,i,i) \mid i \neq j\}$ with order 6.
- $O_5 = \{(i,j,k) \mid i,j,k \text{ distinct}\}$ with order 6.

The cycle decompositions for all elements of S_3 acting on Ω are as follows:
- $1 \in S_3$ is the same as $1 \in S_{27}$.

- (1 2): (1 14)(2 13)(3 15)(4 11)(5 10)(6 12)(7 17)(8 16)(9 18)(19 23)(20 22)(21 24)(25 26)
- (1 3): (1 27)(2 26)(3 25)(4 24)(5 23)(6 22)(7 21)(8 20)(9 19)(10 18)(11 17)(12 16)(13 15)
- (2 3): (2 3)(4 7)(5 9)(6 8)(10 19)(11 21)(12 20)(13 25)(14 27)(15 26)(16 22)(17 24)(18 23)
- (1 2 3): (1 14 27)(2 15 25)(3 13 26)(4 17 21)(5 18 19)(6 16 20)(7 11 24)(8 12 22)(9 10 23)
- (1 3 2): (1 27 14)(2 25 15)(3 26 13)(4 21 17)(5 19 18)(6 20 16)(7 24 11)(8 22 12)(9 23 10)

For O_1, pick $a = (1\ 1\ 1)$. The elements that stabilize a are the identity permutation and (2 3), so the stabilizer of a in S_3 is $\langle(2\ 3)\rangle$. We have $|G_a||O_1| = 2 \cdot 3 = 6 = |S_3|$. For the other orbits, note that S_3 acts transitively on each of them, so the stabilizer of any chosen element in these orbits is trivial. For example, for O_2, pick $a = (1\ 1\ 2)$. The only element that stabilizes a is the identity permutation, so the stabilizer of a in S_3 is 1. We have $|G_a||O_2| = 1 \cdot 6 = 6 = |S_3|$. The same logic applies to O_3, O_4, and O_5.

(b) We begin by classifying the nonempty subsets of $\{1, 2, 3\}$. There are three types of subsets: 1-element subsets, 2-element subsets, and the 3-element subset. We now label the elements of $\mathcal{P}(\{1, 2, 3\}) - \{\varnothing\}$ as follows:

- $1 = \{1\}$
- $2 = \{2\}$
- $3 = \{3\}$
- $4 = \{1, 2\}$
- $5 = \{1, 3\}$
- $6 = \{2, 3\}$
- $7 = \{1, 2, 3\}$

The classification yields the following orbits of S_3 acting on $\mathcal{P}(\{1, 2, 3\}) - \{\varnothing\}$:

- $O_1 = \{\{1\}, \{2\}, \{3\}\}$ with order 3.
- $O_2 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ with order 3.
- $O_3 = \{\{1, 2, 3\}\}$ with order 1.

The cycle decompositions for all elements of S_3 acting on $\mathcal{P}(\{1, 2, 3\}) - \{\varnothing\}$ are as follows:

- $1 \in S_3$ is the same as $1 \in S_7$.
- (1 2): (1 2)(5 6)
- (1 3): (1 3)(4 6)
- (2 3): (2 3)(4 5)
- (1 2 3): (1 2 3)(4 6 5)
- (1 3 2): (1 3 2)(4 5 6)

For O_1, pick $a = \{1\}$. The only elements that stabilize a are the identity permutation and (2 3), so the stabilizer of a in S_3 is $\langle(2\ 3)\rangle$. We have $|G_a||O_1| = 2 \cdot 3 = 6 = |S_3|$. For O_2, pick $a = \{1, 2\}$. The only elements that stabilize a are the identity permutation and (1 2), so the stabilizer of a in S_3 is $\langle(1\ 2)\rangle$. We have $|G_a||O_2| = 2 \cdot 3 = 6 = |S_3|$. For O_3, note that S_3 acts trivially on this orbit, so the stabilizer of $\{1, 2, 3\}$ in S_3 is all of S_3. We have $|G_a||O_3| = 6 \cdot 1 = 6 = |S_3|$. ■

(6) As in Exercise 2.2.12, let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 and let S_4 act on R by permuting the indices of the four variables: $\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$ for all $\sigma \in S_4$.

(a) Find the polynomials in the orbit of S_4 on R containing $x_1 + x_2$ (recall from Exercise 2.2.12 that the stabilizer of this polynomial has order 4).

(b) Find the polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ (recall from Exercise 2.2.12 that the stabilizer of this polynomial has order 8).

(c) Find the polynomials in the orbit of S_4 on R containing $(x_1 + x_2)(x_3 + x_4)$.

Solution.

(a) Note that the size of the orbit is given by $|S_4|/|G_{x_1+x_2}| = 24/4 = 6$. The polynomials in the orbit of S_4 on R containing $x_1 + x_2$ are

$$x_1 + x_2, x_1 + x_3, x_1 + x_4, x_2 + x_3, x_2 + x_4, x_3 + x_4$$

(b) The size of the orbit is 3. The polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ are

$$x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3$$

(c) Note that the stabilizer of $(x_1 + x_2)(x_3 + x_4)$ has order 8 (it is the same as that of $x_1x_2 + x_3x_4$). Thus, the size of the orbit is 3. The polynomials in the orbit of S_4 on R containing $(x_1 + x_2)(x_3 + x_4)$ are

$$(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3)$$ ■

(7) Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B) = \{\sigma(b) \mid b \in B\}$).

(a) Prove that if B is a block containing the element a of A, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G, cf. Exercise 2.4.16). [Use part (a).]

Solution.

(a) We first show that G_B is a subgroup of G. Since $1(B) = B$, then $1 \in G_B$, hence it is nonempty. If $\sigma, \tau \in G$ such that $\sigma(B) = B$ and $\tau(B) = B$, we note that $\tau^{-1}(B) = B$ as well, hence $\sigma, \tau^{-1} \in G_B$. Then $(\sigma\tau^{-1})(B) = \sigma(\tau^{-1}(B)) = \sigma(B) = B$, so $\sigma\tau^{-1} \in G_B$. Hence $G_B \leq G$.

Now, let $a \in B$. If $\sigma \in G_a$, then $\sigma(a) = a$. Since $a \in B$, then $\sigma(a) \in \sigma(B)$. But $\sigma(a) = a \in B$, so $\sigma(B) \cap B \neq \emptyset$. By the definition of a block, this implies that $\sigma(B) = B$, hence $\sigma \in G_B$. Therefore, we have shown that $G_a \leq G_B$.

(b) Let B be a block and let $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ be all the distinct images of B under the elements of G. By transitivity of G on A, then for some $a \in A$, there exists $b \in B$ such that $\sigma(b) = a$. Then $a \in \sigma(B)$, and since $\sigma(B)$ is one of the sets $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$, it follows that

$$\bigcup_{i=1}^{n} \sigma_i(B) = A.$$

Suppose there existed $i \neq j$ where $\sigma_i(B) \cap \sigma_j(B) \neq \emptyset$. Then there are $b, b' \in B$ such that $\sigma_i(b) = \sigma_j(b')$, or $(\sigma_j^{-1}\sigma_i)(b) = b'$, hence $\sigma_j^{-1}\sigma_i(B) \cap B \neq \emptyset$. Since B is a block, then $\sigma_j^{-1}\sigma_i(B) = B$, hence $\sigma_i(B) = \sigma_j(B)$, contradicting the assumption that they are distinct. Therefore, the sets $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are disjoint, and we conclude that they form a partition of A.

(c) Let $B \subset A$, i.e., a proper subset of A. If $|B| = 1$, then it is trivial. Suppose $|B| > 1$, and without loss of generality, let $1 \in B$ and some $1 \neq i \in B$ as well. Then there exists some $\sigma \in S_4$ such that $\sigma(1) = 1$ and $\sigma(i) = j$ for $j \notin B$. Then $\sigma(B) \cap B \neq \emptyset$ so that $\sigma(B) = B$, hence $j \in B$. We may repeat this to show that $B = A$, contradicting the assumption that B is a proper subset of A. Therefore, the only blocks in A are the trivial ones, and S_4 is primitive on A.

Now, consider D_8 acting on the four vertices of a square. Let B be the set containing the two opposite vertices. Then for any $\sigma \in D_8$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Thus, B is a nontrivial block, and D_8 is not primitive in its action on the four vertices of a square.

(d) ($\Rightarrow$) If G is primitive on A. Let $H \leq G$ such that $G_a \leq H \leq G$, and let B be the orbit of H so that $B = H \cdot a$. Since $1 \in H$ because $H \leq G$, then $1 \cdot a = a \in B$. By part (a), we know that $a \in B$ implies $G_a \leq G_B$ so that B is now a block containing a. Primitivity of G implies that B is either $\{a\}$ or A itself. If $B = \{a\}$, then for any $\sigma \in H$, we have $\sigma \cdot a \in B$, hence $\sigma \cdot a = a$, so $\sigma \in G_a$. Therefore, $H \leq G_a$, and since $G_a \leq H$, then $H = G_a$. If $B = A$, then for any $b \in A$, there exists some $\sigma \in H$ such that $\sigma \cdot a = b$. Thus, for any $b \in A$, there exists some $\sigma \in H$ such that $\sigma(b) = a$, hence H is transitive on A. Therefore, $H = G$. We have shown that the only subgroups of G containing G_a are G_a and G.
($\Leftarrow$) Suppose now that G_a is maximal in G. Let B be a block of A that contains some $a \in A$. By part (a), we know that $G_a \leq G_B \leq G$. Maximality of G_a implies that either $G_B = G_a$ or $G_B = G$. If $G_B = G_a$, then for any $\sigma \in G_B$, we have $\sigma \in G_a$, hence $\sigma(a) = a$. Since $a \in B$, then $\sigma(a) \in \sigma(B)$, so $\sigma(a) \in B$. Therefore, $\sigma(a) = a \in B$, and it follows that $\sigma(B) \cap B \neq \emptyset$. By the definition of a block, this implies that $\sigma(B) = B$. Thus, for any $\sigma \in G_B$, we have $\sigma(B) = B$, so $B = \{a\}$. If $G_B = G$, then for any $b \in A$, there exists some $\sigma \in G$ such that $\sigma(a) = b$. Since $\sigma \in G_B$, then $\sigma(B) = B$, hence $b \in B$. Therefore, $B = A$. We have shown that the only blocks in A are the trivial ones, so G is primitive on A. ■

(8) A transitive permutation group G on a set A is called *doubly transitive* if for any (hence all) $a \in A$ the subgroup

G_a is transitive on the set $A - \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the 4 vertices of a square.

Solution.

(a) Let G_a be the stabilizer of $a \in \{1, 2, \ldots, n\}$. Note that G_a is the set of all permutations that fix a and permute the remaining $n-1$ elements so that $G_a \cong S_{n-1}$. Since S_{n-1} is transitive on the set $\{1, 2, \ldots, n\} - \{a\}$ for all $n - 1 \geq 1$, then G_a is transitive on $A - \{a\}$ for all $n \geq 2$. Therefore, S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

(b) Let G be double transitive and let B be a block containing some $a \in A$. Take $b \in B$ such that $b \neq a$. Double transitivity of G implies that there exists some $\sigma \in G_a$ such that $\sigma(b) = c$ for any $c \in A - \{a\}$. Since $\sigma \in G_a$, then $\sigma(B) = B$, hence $c \in B$. Therefore, $B = A$, and we conclude that the only blocks in A are the trivial ones. Thus, G is primitive on A. Since D_8 is not primitive in its action on the four vertices of a square (as shown in part (c) of the previous exercise), then it is not doubly transitive. ■

(9) Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $O_1, O_2, \ldots, O_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $O_1, O_2, \ldots, O_r$, in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $gO_i = O_j$, where $gO = \{g \cdot a \mid a \in O\}$ (i.e., in the notation of Exercise 7 the sets $O_1, \ldots, O_r$ are blocks). Prove that G is transitive on $\{O_1, \ldots, O_r\}$. Deduce that all orbits of H on A have the same cardinality.

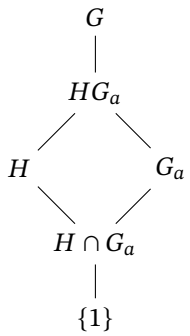
(b) Prove that if $a \in O_1$ then $|O_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$. [Draw the sublattice describing the Second Isomorphism Theorem for the subgroups H and G_a of G. Note that $H \cap G_a = H_a$.]

Solution.

(a) Let $g \in G$ and O_i be an orbit of H on A. Let $a \in O_i$ so that $O_i = H \cdot a = \{h \cdot a \mid h \in H\}$. Consider the set $gO_i = \{g \cdot (h \cdot a) \mid h \in H\}$. Since H is normal in G, then for any $h \in H$, we have $ghg^{-1} \in H$. Then $gO_i = H \cdot (g \cdot a)$, which is the orbit of H containing $g \cdot a$. Therefore, there exists some j such that $gO_i = O_j$.

To show that G is transitive on $\{O_1, \ldots, O_r\}$, let O_i and O_j be any two orbits of H on A. Since G is transitive on A, then for some $a \in O_i$ and $b \in O_j$, there exists some $g \in G$ such that $g \cdot a = b$. Then gO_i is the orbit of H containing b, hence $gO_i = O_j$. Therefore, G is transitive on $\{O_1, \ldots, O_r\}$. Since G is transitive on $\{O_1, \ldots, O_r\}$, then all orbits of H on A have the same cardinality.

(b) Suppose $a \in O_1$. By Proposition 4.2, we have $|O_1| = |H : H_a|$. Since $H_a = H \cap G_a$, then $|O_1| = |H : H \cap G_a|$. Moreover, the orbits of H partition A and have the same size by the previous solution, so we have $|A| = r|O_1|$. By applying Proposition 4.2 again, we have $|A| = |G : G_a|$. Therefore, $|G : G_a| = r|O_1| = r|H : H \cap G_a|$. By the Second Isomorphism Theorem, we also have that $H/(H \cap G_a) \cong HG_a/G_a$ so that $|H : H \cap G_a| = |HG_a : G_a|$. Now recall by Exercise 3.2.11 that $|G : K| = |G : H||H : K|$ for subgroups $K \leq H \leq G$. Applying this to the subgroups $G_a \leq HG_a \leq G$, we have $|G : G_a| = |G : HG_a||HG_a : G_a| = |G : HG_a||H : H \cap G_a|$. We then have $r|H : H \cap G_a| = |G : HG_a||H : H \cap G_a|$, or $r = |G : HG_a|$. Moreover, the sublattice is given as follows:



■

(10) Let H and K be subgroups of the group G. For each $x \in G$ define the HK *double coset* of x in G to be the set $HxK = \{hxk \mid h \in H, k \in K\}$.

(a) Prove that HxK is the union of the left cosets $x_1K, \ldots, x_nK$ where $\{x_1K, \ldots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K.

(b) Prove that HxK is a union of right cosets of H.

(c) Show that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Show that the set of HK double cosets partitions G.

(d) Prove that $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$.

(e) Prove that $|HxK| = |H| \cdot |K : K \cap x^{-1}Hx|$.

Solution.

(a) Let $\mathcal{O}$ be the orbit containing xK of H acting by left multiplication on the set of left cosets of K. Then $\mathcal{O} = \{hxK \mid h \in H\}$, and let $\{x_1K, \ldots, x_nK\}$ be the distinct left cosets in $\mathcal{O}$. Let $\mathcal{K}$ be the union of these left cosets, i.e., $\mathcal{K} = \bigcup_1^n x_iK$.

Now pick $y \in HxK$. Then there exist $h \in H$ and $k \in K$ such that $y = hxk$. Note that $hxK \in \mathcal{O}$, so there exists some i such that $hxK = x_iK$. Therefore, $y = hxk \in x_iK \subseteq \mathcal{K}$, hence $HxK \subseteq \mathcal{K}$. If $z \in \mathcal{K}$, then there exists some i and some $k' \in K$ such that $z = x_ik'$. Since $x_iK \in \mathcal{O}$, then there exists some $h' \in H$ such that $x_iK = h'xK$, hence $x_i = h'xk''$ for some $k'' \in K$. Therefore, $z = x_ik' = h'xkk'' \in HxK$, so $\mathcal{K} \subseteq HxK$. We have shown that $HxK = \mathcal{K}$, i.e., HxK is the union of the left cosets $x_1K, \ldots, x_nK$.

(b) The proof is similar to that of part (a).

(c) Let $x, y \in G$. Suppose $HxK \cap HyK \neq \emptyset$. Then there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1xk_1 = h_2yk_2$. Rearranging, we have $y = h_2^{-1}h_1xk_1k_2^{-1}$, hence $y \in HxK$. Therefore, $HyK \subseteq HxK$. By symmetry, we also have $HxK \subseteq HyK$, so $HxK = HyK$. We have shown that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Since every element of G is in some double coset of the form HxK, then the set of HK double cosets partitions G.

(d) Recall that the orbit of xK under this action is $\mathcal{O} = \{hxK \mid h \in H\}$. By Proposition 4.2, we have $|\mathcal{O}| = |H : H_{xK}|$, where H_{xK} is the stabilizer of xK in H. Observe that $H_{xK} = \{h \in H \mid hxK = xK\}$. Then $hxK = xK$ implies that there exists some $k \in K$ such that $hxk = x$, or equivalently, $h = xkx^{-1}$. Therefore, $H_{xK} = H \cap xKx^{-1}$. By part (a), we have $|HxK| = |\mathcal{O}| \cdot |K| = |H : H \cap xKx^{-1}| \cdot |K|$.

(e) Similar to part (d). ■

4.2 Groups Acting on Themselves by Left Mutliplication—Cayley's Theorem

(1) Let G be $\{1, a, b, c\}$, the Klein 4-group whose group table is written out in Section 2.5.

(a) Label $1, a, b, c$ with the integers $1, 2, 4, 3$, respectively, and prove that under the left regular representation of G into S_4 the nonidentity elements are mapped as follows:

$$a \mapsto (1\ 2)(3\ 4), \quad b \mapsto (1\ 4)(2\ 3), \quad c \mapsto (1\ 3)(2\ 4).$$

(b) Relabel $1, a, b, c$ as $1, 4, 2, 3$, respectively, and compute the image of each element of G under the left regular representation of G into S_4. Show that the image of G in S_4 under this labelling is the same *subgroup* as the image of G in part (a) (even though the nonidentity elements individually map to different permutations under the two different labellings).

Solution.

(a) We have $a \cdot 1 = a$ so that $\sigma_a(1) = 2$. Similarly, $\sigma_a(2) = 1$. We also have $a \cdot b = c$ so that $\sigma_a(4) = 3$, and $\sigma_a(3) = 4$, and we have $a \mapsto (1\ 2)(3\ 4)$. The others are computed similarly.

(b) Again, we have $a \cdot 1 = a$ so that $\sigma_a(1) = 4$. Similarly, $\sigma_a(4) = 1$. We also have $a \cdot b = c$ so that $\sigma_a(2) = 3$, and $\sigma_a(3) = 2$, and we have $a \mapsto (1\ 4)(2\ 3)$. For b, we have $b \mapsto (1\ 2)(3\ 4)$, and for c, we have $c \mapsto (1\ 3)(2\ 4)$. The image of G in S_4 under this labelling is $\{1, (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4)\}$, which is the same subgroup as in part (a). ■

(2) List the elements of S_3 as $1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)$ and label these with the integers $1, 2, 3, 4, 5, 6$ respectively. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6.

Solution. Consider $(1\ 2)$. Then we have the following computations:

$$\begin{aligned}
(1\ 2) \cdot 1 &= (1\ 2) & \sigma_{(1\ 2)}(1) &= 2 \\
(1\ 2) \cdot (1\ 2) &= 1 & \sigma_{(1\ 2)}(2) &= 1 \\
(1\ 2) \cdot (2\ 3) &= (1\ 3\ 2) & \sigma_{(1\ 2)}(4) &= 5 \\
(1\ 2) \cdot (1\ 3) &= (1\ 2\ 3) & \sigma_{(1\ 2)}(3) &= 6 \\
(1\ 2) \cdot (1\ 2\ 3) &= (2\ 3) & \sigma_{(1\ 2)}(5) &= 3 \\
(1\ 2) \cdot (1\ 3\ 2) &= (1\ 3) & \sigma_{(1\ 2)}(6) &= 4
\end{aligned}$$

Thus, we have $(1\ 2) \mapsto (1\ 2)(3\ 6\ 4\ 5)$. We calculate that $(2\ 3) \mapsto (1\ 3\ 5\ 2)(4\ 6)$. Since $(1\ 2)(2\ 3) = (1\ 2\ 3)$, then

$$(1\ 2\ 3) \mapsto (1\ 2)(3\ 6\ 4\ 5)(1\ 3\ 5\ 2)(4\ 6) = (1\ 5\ 6)(2\ 4\ 3)$$

Continuing in this way, we find that the images of the elements of S_3 under the left regular representation are as follows:

$$\begin{aligned}
1 &\mapsto 1 \\
(1\ 2) &\mapsto (1\ 2)(3\ 6\ 4\ 5) \\
(2\ 3) &\mapsto (1\ 3\ 5\ 2)(4\ 6) \\
(1\ 3) &\mapsto (1\ 4)(2\ 6)(3\ 5) \\
(1\ 2\ 3) &\mapsto (1\ 5\ 6)(2\ 4\ 3) \\
(1\ 3\ 2) &\mapsto (1\ 6\ 5)(2\ 3\ 4)
\end{aligned}$$

■

(3) Let r and s be the usual generators for the dihedral group of order 8.

(a) List the elements of D_8 as $1, r, r^2, r^3, s, sr, sr^2, sr^3$ and label these with the integers $1, 2, \ldots, 8$ respectively. Exhibit the image of each element of D_8 under the left regular representation of D_8 into S_8.

(b) Relabel this same list of elements of D_8 with the integers $1, 3, 5, 7, 2, 4, 6, 8$ respectively and recompute the image of each element of D_8 under the left regular representation with respect to this new labelling. Show that the two subgroups of S_8 obtained in parts (a) and (b) are different.

Solution.

(a) We calculate $\sigma_r = (1\,2\,3\,4)(5\,8\,7\,6)$ and $\sigma_s = (1\,5)(2\,6)(3\,7)(4\,8)$. Continuing in this way, we find that the images of the elements of D_8 under the left regular representation are as follows:

$$\begin{aligned} 1 &\mapsto 1 & s &\mapsto (1\,5)(2\,6)(3\,7)(4\,8)\\ r &\mapsto (1\,2\,3\,4)(5\,8\,7\,6) & sr &\mapsto (1\,6)(2\,7)(3\,8)(4\,5)\\ r^2 &\mapsto (1\,3)(2\,4)(5\,7)(6\,8) & sr^2 &\mapsto (1\,7)(2\,8)(3\,5)(4\,6)\\ r^3 &\mapsto (1\,4\,3\,2)(5\,6\,7\,8) & sr^3 &\mapsto (1\,8)(2\,5)(3\,6)(4\,7) \end{aligned}$$

(b) The images of D_8 under the left regular representation with respect to this new labelling are as follows:

$$\begin{aligned} 1 &\mapsto 1 & s &\mapsto (1\,2)(3\,4)(5\,6)(7\,8)\\ r &\mapsto (1\,3\,5\,7)(2\,8\,6\,4) & sr &\mapsto (1\,4)(2\,7)(3\,6)(5\,8)\\ r^2 &\mapsto (1\,5)(3\,7)(2\,6)(4\,8) & sr^2 &\mapsto (1\,6)(2\,5)(3\,8)(4\,7)\\ r^3 &\mapsto (1\,7\,5\,3)(2\,4\,6\,8) & sr^3 &\mapsto (1\,8)(2\,3)(4\,5)(6\,7) \end{aligned}$$

Clearly, the two subgroups of S_8 obtained in parts (a) and (b) are different since, for example, the image of r in part (a) is a product of two 4-cycles while the image of r in part (b) is a product of two 4-cycles but with different elements. ■

(4) Use the left regular representation of Q_8 to produce two elements of S_8 which generate a subgroup of S_8 isomorphic to the quaternion group Q_8.

Solution. At minimum, we have that $Q_8 = \langle i, j\rangle$ (any 2 elements of order 4 can be used), so we compute the images of i and j under the left regular representation. We label Q_8 as $1, -1, i, -i, j, -j, k, -k$ and label these with the integers $1, 2 \ldots 8$ respectively. We find that

$$\begin{aligned} i &\mapsto \sigma_i = (1\,3\,4\,2)(5\,7)(6\,8)\\ j &\mapsto \sigma_j = (1\,5\,2\,6)(3\,8)(4\,7) \end{aligned}$$

Hence $Q_8 \cong \langle \sigma_i, \sigma_j\rangle \leq S_8$. ■

(5) Let r and s be the usual generators for the dihedral group of order 8 and let $H = \langle s\rangle$. List the left cosets of H in D_8 as $1H, rH, r^2H$ and r^3H.

(a) Label these cosets with the integers 1, 2, 3, 4, respectively. Exhibit the image of each element of D_8 under the representation π_H of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of H in D_8. Deduce that this representation is faithful (i.e., the elements of S_4 obtained form a subgroup isomorphic to D_8).

(b) Repeat part (a) with the list of cosets relabelled by the integers $1, 3, 2, 4$, respectively. Show that the permutations obtained from this labelling form a subgroup of S_4 that is different from the subgroup obtained in part (a).

(c) Let $K = \langle sr\rangle$, list the cosets of K in D_8 as $1K, rK, r^2K$ and r^3K, and label these with the integers $1, 2, 3, 4$. Prove that, with respect to this labelling, the image of D_8 under the representation π_K obtained from left multiplication on the cosets of K is the same *subgroup* of S_4 as in part (a) (even though the subgroups H and K are different and some of the elements of D_8 map to different permutations under the two homomorphisms).

Solution.

(a) We have $\pi_H(r) = (1\,2\,3\,4)$ and $\pi_H(s) = (2\,4)$. We continue in this way to find that the images of the elements of D_8 under π_H are:

$$\begin{aligned} \pi_H(1) &= 1 & \pi_H(s) &= (2\,4)\\ \pi_H(r) &= (1\,2\,3\,4) & \pi_H(sr) &= (1\,2)(3\,4)\\ \pi_H(r^2) &= (1\,3)(2\,4) & \pi_H(sr^2) &= (1\,3)\\ \pi_H(r^3) &= (1\,4\,3\,2) & \pi_H(sr^3) &= (1\,4)(2\,3) \end{aligned}$$

so that the subgroup $\langle \pi_H(r), \pi_H(s)\rangle \leq S_4$ is isomorphic to D_8. Since the kernel of π_H is trivial, then the representation is faithful.

(b) The new labelling affords the permutations $\pi_H(r) = (1\ 3\ 2\ 4)$ and $\pi_H(s) = (3\ 4)$. We have the following images:

$$\begin{aligned} \pi_H(1) &= 1 & \pi_H(s) &= (3\ 4) \\ \pi_H(r) &= (1\ 3\ 2\ 4) & \pi_H(sr) &= (1\ 3)(2\ 4) \\ \pi_H(r^2) &= (1\ 2)(3\ 4) & \pi_H(sr^2) &= (1\ 2) \\ \pi_H(r^3) &= (1\ 4\ 2\ 3) & \pi_H(sr^3) &= (1\ 4)(2\ 3) \end{aligned}$$

Moreover, the subgroup is different from that in part (a) since, for example, the image of r in part (a) is $(1\ 2\ 3\ 4)$ while the image of r in this part is $(1\ 3\ 2\ 4)$.

(c) Under π_K, we have $\pi_K(r) = (1\ 2\ 3\ 4)$ and $\pi_K(s) = (1\ 2)(3\ 4)$. With respect to this labeling, we have the subgroup $\widehat{K} = \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4)\rangle$. Let $\widehat{H}$ be the subgroup obtained in part (a). Note that $(1\ 2\ 3\ 4)$ is contained in both $\widehat{H}$ and $\widehat{K}$. Moreover, we have following:

$$(1\ 2\ 3\ 4)(2\ 4)(1\ 4\ 3\ 2) = (1\ 2)(3\ 4) \in \widehat{H} \quad \text{and} \quad (1\ 2\ 3\ 4)^2(1\ 2)(3\ 4) = (2\ 4) \in \widehat{K}$$

so that both subgroups contain the other generator of the other subgroup. Therefore, $\widehat{H} = \widehat{K}$. ■

(6) Let r and s be the usual generators for the dihedral group of order 8 and let $N = \langle r^2 \rangle$. List the left cosets of N in D_8 as $1N, rN, sN$ and srN. Label these cosets with the integers 1, 2, 3, 4 respectively. Exhibit the image of each element of D_8 under the representation π_N of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of N in D_8. Deduce that this representation is not faithful and prove that $\pi_N(D_8)$ is isomorphic to the Klein 4-group.

Solution. We have $\pi_N(r) = (1\ 2)(3\ 4)$ and $\pi_N(s) = (1\ 3)(2\ 4)$. Continuing in this way, we find that the images of the elements of D_8 under π_N are:

$$\begin{aligned} \pi_N(1) &= 1 & \pi_N(s) &= (1\ 3)(2\ 4) \\ \pi_N(r) &= (1\ 2)(3\ 4) & \pi_N(sr) &= (1\ 4)(2\ 3) \\ \pi_N(r^2) &= 1 & \pi_N(sr^2) &= (1\ 3)(2\ 4) \\ \pi_N(r^3) &= (1\ 2)(3\ 4) & \pi_N(sr^3) &= (1\ 4)(2\ 3) \end{aligned}$$

Since $\ker(\pi_N)$ contains the nontrivial element r^2, then the representation is not faithful. Moreover, we have $\pi_N(D_8) = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, which is isomorphic to the Klein 4-group. ■

(7) Let Q_8 be the quaternion group of order 8.

(a) Prove that Q_8 is isomorphic to a subgroup of S_8.

(b) Prove that Q_8 is not isomorphic to a subgroup of S_n for any $n \leq 7$. [If Q_8 acts on any set A of order ≤ 7 show that the stabilizer of any point $a \in A$ must contain the subgroup $\langle -1 \rangle$.]

Solution.

(a) This is done in Exercise 4.2.4.

(b) Let Q_8 act on a set A of order $n \leq 7$. For any $a \in A$, consider the orbit O_a of a under this action. By Proposition 4.2, we have $|O_a| = |Q_8 : (Q_8)_a|$, where $(Q_8)_a$ is the stabilizer of a in Q_8. Since $|O_a|$ divides $|A| \leq 7$, then $|O_a|$ must be 1, 2, 4, or 7. However, since Q_8 has no subgroup of index 7, then $|O_a|$ cannot be 7. If $|O_a| = 4$, then $(Q_8)_a$ has order 2, but the only subgroup of order 2 in Q_8 is $\langle -1 \rangle$. If $|O_a| = 2$, then $(Q_8)_a$ has order 4, and the only subgroups of order 4 in Q_8 are $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$, all of which contain $\langle -1 \rangle$. If $|O_a| = 1$, then $(Q_8)_a = Q_8$, which also contains $\langle -1 \rangle$. Therefore, in all cases, the stabilizer $(Q_8)_a$ contains $\langle -1 \rangle$. Since this holds for all $a \in A$, then $\langle -1 \rangle$ is contained in the kernel of the action. The action is not faithful, hence Q_8 cannot be isomorphic to a subgroup of S_n for any $n \leq 7$. ■

(8) Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Solution. Let G act by left multiplication on the set of left cosets of H in G. Then we have the homomorphism $\varphi : G \to S_n$, which is the permutation representation of G on G/H. Let $K = \ker(\varphi) \subseteq H$, since $g \in K$ if and only if $gH = H$. By the First Isomorphism Theorem, we have $G/K \cong \varphi(G) \leq S_n$, so that $|G : K| = |G/K| = |\varphi(G)|$ divides $n!$. Therefore, $|G : K| \leq n!$. ■

(9) Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

Solution. Let H be a subgroup of G with index p. Then $|G : H| = p$, so the action of G on the left cosets of H in G gives a homomorphism $\varphi : G \to S_p$. Since $|G| = p^\alpha$, then by Lagrange's Theorem, the order of $\varphi(G)$ divides p^α. However, the only subgroups of S_p whose order divides p^α are the trivial group and groups of order p. Since $\varphi(G)$ acts transitively on the p cosets of H, then $\varphi(G)$ cannot be trivial. Therefore, $|\varphi(G)| = p$, which is prime, so $\varphi(G)$ is cyclic and hence abelian. The kernel of φ is a normal subgroup of G contained in H. Since the image $\varphi(G)$ has order p, then by the First Isomorphism Theorem, we have $|G : \ker(\varphi)| = p$. But since $\ker(\varphi) \subseteq H$ and both have index p, then $\ker(\varphi) = H$. Therefore, H is normal in G.

To deduce that every group of order p^2 has a normal subgroup of order p, let G be a group of order p^2. By Cauchy's Theorem, there exists an element of order p in G, which generates a subgroup H of order p. Since the index of H in G is p, by the previous result, H is normal in G. ■

(10) Prove that every non-abelian group of order 6 has a nonnormal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into S_3.]

Solution. Note that $2 \mid 6$ and $3 \mid 6$. By Cauchy's Theorem, there exists subgroups H and K of orders 2 and 3 respectively. Let $H = \{1, h\}$, suppose it is normal, and let $g \in G - H$. Since $H \trianglelefteq G$, then $gHg^{-1} = H$. In particular, $ghg^{-1} \in H$, so either $ghg^{-1} = 1$ or $ghg^{-1} = h$. Since the first case implies $h = 1$, it must be that $ghg^{-1} = h$, or $gh = hg$. Then h commutes with every element. Moreover, we may use Exercise 3.3.3 to conclude that $G = HK$ since $H \trianglelefteq G$. Since K is also abelian as it is cyclic, then $G = hk$ for $h \in H$ and $k \in K$, implying that G is abelian, a contradiction. Therefore, H is not normal in G.

To classify groups of order 6, let G be a group of order 6. If G is abelian, then $G \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. If G is non-abelian, then by the above result, G has a nonnormal subgroup H of order 2. Let K be the subgroup of order 3. Then $G = HK$. Let G act by left multiplication on the left cosets of K in G. This action gives a homomorphism $\varphi : G \to S_3$. Since H is not normal in G, then the action is nontrivial, so φ is injective. Therefore, $G \cong \varphi(G) \leq S_3$. Since $|G| = 6 = |S_3|$, then $\varphi(G) = S_3$, and hence $G \cong S_3$. ■

(11) Let G be a finite group and let $\pi : G \to S_G$ be the left regular representation. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m n-cycles. Deduce that $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $|G|/|x|$ is odd.

Solution. Let $x \in G$ with $|x| = n$. Consider the action of $\langle x \rangle$ on G by left multiplication. The orbit of any $g \in G$ under this action is $O_g = \{x^k g \mid k = 0, 1, \ldots, n-1\}$. Since $|x| = n$, then $|O_g| = n$ for all $g \in G$. By Proposition 4.2, we have $|O_g| = |\langle x \rangle : (\langle x \rangle)_g|$, where $(\langle x \rangle)_g$ is the stabilizer of g in $\langle x \rangle$. Since $|O_g| = n$, then $(\langle x \rangle)_g$ is trivial for all $g \in G$. Therefore, the orbits of this action partition G into subsets of size n. Since $|G| = mn$, there are exactly m such orbits. Each orbit corresponds to an n-cycle in the permutation $\pi(x)$. Therefore, $\pi(x)$ is a product of m n-cycles.

To determine when $\pi(x)$ is an odd permutation, we note that an n-cycle is an odd permutation if and only if n is even. Since $\pi(x)$ is a product of m n-cycles, the parity of $\pi(x)$ is determined by the parity of m and n. Specifically, $\pi(x)$ is odd if and only if n is even and m is odd. Thus, $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $|G|/|x|$ is odd. ■

(12) Let G and π be as in the preceding exercise. Prove that if $\pi(G)$ contains an odd permutation then G has a subgroup of index 2. [Use Exercise 3.3.3.]

Solution. Recall the ϵ homomorphism from Proposition 3.23. Moreover, π is a homomorphism from G to S_G. Consider the composition $\epsilon \circ \pi : G \to \{\pm 1\}$. Since $\pi(G)$ contains an odd permutation, then $\epsilon \circ \pi$ is surjective. By the First Isomorphism Theorem, we have $G/\ker(\epsilon \circ \pi) \cong \{\pm 1\}$, so that $|\ker(\epsilon \circ \pi)| = |G|/2$. Therefore, $\ker(\epsilon \circ \pi)$ is a subgroup of G of index 2. ■

(13) Prove that if $|G| = 2k$ where k is odd then G has a subgroup of index 2. [Use Cauchy's Theorem to produce an element of order 2 and then use the preceding two exercises.]

Solution. By Cauchy's Theorem, there exists $x \in G$ such that $|x| = 2$. Then $\pi(x)$ is of order 2 and is hence a product of disjoint transpositions. Since $|G| = 2k$ with k odd, then use $m = k$ and $n = 2$ in Exercise 4.2.11 along with even $|x|$ to conclude that $\pi(x)$ is an odd permutation. By the Exercise 4.2.12, G has a subgroup of index 2. ■

(14) Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

Solution. Let S be the set of all prime factors of n. By the Well Ordering Principle, this has a minimal element p. By hypothesis, G has a subgroup P of order n/p with index p. By Corollary 4.5, P is normal in G since p is the smallest prime dividing n. Therefore, G is not simple. ■

4.3 Groups Acting on Themselves by Conjugation—The Class Equation

Let G be a group.

(1) Suppose G has a left action on a set A, denoted by $g \cdot a$ for all $g \in G$ and $a \in A$. Denote the corresponding right action on A by $a \cdot g$. Prove that the (equivalence) relations $\sim$ and $\sim'$ defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \quad \text{for some } g \in G$$

and

$$a \sim' b \quad \text{if and only if} \quad a = b \cdot g \quad \text{for some } g \in G$$

are the same relation (i.e., $a \sim b$ if and only if $a \sim' b$).

Solution. If $a \sim b$, there exists $g \in G$ such that $a = g \cdot b$. Let $h = g^{-1}$. Then $b = h \cdot a$, so $a = b \cdot g$. Thus, $a \sim' b$. Conversely, if $a \sim' b$, there exists $g \in G$ such that $a = b \cdot g$. Let $h = g^{-1}$. Then $b = h \cdot a$, so $a = g \cdot b$. Thus, $a \sim b$. Therefore, the relations $\sim$ and $\sim'$ are the same. ■

(2) Find all conjugacy classes and their sizes in the following groups:

(a) D_8

(b) Q_8

(c) A_4

Solution.

(a) Discussed in the text, the conjugacy classes of D_8 are $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, and $\{sr, sr^3\}$ with sizes 1, 1, 2, 2, and 2 respectively.

(b) Again discussed in the text, the conjugacy classes of Q_8 are $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, and $\{k, -k\}$ with sizes 1, 1, 2, 2, and 2 respectively.

(c) We proceed similarly as the text. The possible cycle types are 1, (1 2 3), and (1 2)(3 4).

For (1 2 3), we have $C_{A_4}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$ since the only permutation that fixes 1, 2, and 3 is the identity. Therefore, the conjugacy class of (1 2 3) has size $12/3 = 4$. However, there are 8 3-cycles in A_4, so there exists a 3-cycle $\sigma \in A_4$ not in the conjugacy class of (1 2 3). By similar reasoning, the conjugacy class of σ also has size 4. There are then 2 conjugacy classes of size 4 corresponding to the 3-cycles.

For (1 2)(3 4), it is trivial to calculate that the remaining double transpositions are in its conjugacy class. Therefore, the conjugacy class of (1 2)(3 4) has size 3. ■

(3) Find all conjugacy classes and their sizes in the following groups:

(a) $Z_2 \times S_3$

(b) $S_3 \times S_3$

(c) $Z_3 \times A_4$

Solution. We first prove a (somewhat) trivial idea: if G and H are groups, let $g \in G$ and $h \in H$. Let $\mathcal{K}_g$ and $\mathcal{K}_h$ be the conjugacy classes of g in G and h in H respectively. Then $\mathcal{K}_{(g,h)} = \mathcal{K}_g \times \mathcal{K}_h$ is the conjugacy class of (g, h) in $G \times H$. To see this, note that for any $(x, y) \in G \times H$, we have

$$(x, y)(g, h)(x, y)^{-1} = (xgx^{-1}, yhy^{-1}) \in \mathcal{K}_g \times \mathcal{K}_h.$$

Conversely, for any $(g', h') \in \mathcal{K}_g \times \mathcal{K}_h$, there exist $x \in G$ and $y \in H$ such that $g' = xgx^{-1}$ and $h' = yhy^{-1}$. Therefore, $(g', h') = (x, y)(g, h)(x, y)^{-1}$, so (g', h') is in the conjugacy class of (g, h) in $G \times H$. This result shows two important things: the conjugacy classes of $G \times H$ are precisely the products of the conjugacy classes of G and H, and the size of the conjugacy class of (g, h) in $G \times H$ is the product of the sizes of the conjugacy classes of g in G and h in H. We now use this to answer the question.

(a) Let $Z_2 = \langle x \rangle$. The conjugacy classes $\mathcal{K}_1$ and $\mathcal{K}_x$ of Z_2 have sizes 1 and 1 respectively. For S_3, the partitions of 3 are 3 1-cycles, 2-cycle and 1-cycle, and a 3-cycle with representatives 1, (1 2), and (1 2 3) respectively. Since $C_{S_3}((1\ 2)) = \langle (1\ 2) \rangle$ and $C_{S_3}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$, then the conjugacy classes $\mathcal{K}_1$, $\mathcal{K}_{(1\ 2)}$, and $\mathcal{K}_{(1\ 2\ 3)}$ of S_3 have sizes 1, 3, and 2 respectively. Therefore, $Z_2 \times S_3$ has 6 conjugacy classes of size 1, 3, 2, 1, 3, and 2 respectively.

(b) By the above, S_3 has 3 conjugacy classes of sizes 1, 3, and 2 respectively. Then $S_3 \times S_3$ has 9 conjugacy classes with sizes 1, 3, 2, 3, 9, 6, 2, 6, and 4 respectively.

(c) Z_3 has 3 conjugacy classes of size 1 each. From Exercise 4.3.2, we know that A_4 has 4 conjugacy classes of sizes 1, 4, 4, and 3. Therefore, $Z_3 \times A_4$ has 12 conjugacy classes with sizes 1, 4, 4, 3, 1, 4, 4, 3, 1, 4, 4, and 3 respectively. ■

(4) Prove that if $S \subseteq G$ and $g \in G$ then $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.

Solution. Suppose $x \in gN_G(S)g^{-1}$, and consider $xgSg^{-1}x^{-1}$. Since $x = gng^{-1}$ for some $n \in N_G(S)$, then we have $gng^{-1}gSg^{-1}gn^{-1}g^{-1} = gnSn^{-1}g^{-1} = gSg^{-1}$, so that $x \in N_G(gSg^{-1})$. Conversely, suppose $x \in N_G(gSg^{-1})$. Then $xgSg^{-1}x^{-1} = gSg^{-1}$. Letting $n = g^{-1}xg$, we have $nSn^{-1} = S$, so $n \in N_G(S)$ and hence $x \in gN_G(S)g^{-1}$. Therefore, $gN_G(S)g^{-1} = N_G(gSg^{-1})$.

Suppose $x \in gC_G(S)g^{-1}$, and consider xsx^{-1} for some $s \in gSg^{-1}$. Since $x = gng^{-1}$ for some $n \in C_G(S)$, then we have $gng^{-1}sgn^{-1}g^{-1} = gn(g^{-1}sg)n^{-1}g^{-1} = g(g^{-1}sg)g^{-1} = s$, so that $x \in C_G(gSg^{-1})$. Conversely, suppose $x \in C_G(gSg^{-1})$. Then $xsx^{-1} = s$ for all $s \in gSg^{-1}$. Letting $n = g^{-1}xg$, we have $ntn^{-1} = t$ for all $t \in S$, so $n \in C_G(S)$ and hence $x \in gC_G(S)g^{-1}$. Therefore, $gC_G(S)g^{-1} = C_G(gSg^{-1})$. ■

(5) If the center of G is of index n, prove that every conjugacy class has at most n elements.

Solution. Let $\mathcal{K}_g$ be the conjugacy class of some $g \in G$. By Proposition 4.6, we have $|\mathcal{K}_g| = |G : C_G(g)|$. Since $Z(G) \leq C_G(g)$ for all $g \in G$, Lagrange's Theorem shows that $|Z(G)|$ divides $|C_G(g)|$. Therefore, $|G : C_G(g)|$ divides $|G : Z(G)| = n$. Hence, $|\mathcal{K}_g| \leq n$. ■

(6) Assume G is a non-abelian group of order 15. Prove that $Z(G) = 1$. Use the fact that $\langle g \rangle \leq C_G(g)$ for all $g \in G$ to show that there is at most one possible class equation for G. [Use Exercise 3.1.36.]

Solution. Recall that $Z(G) \leq G$. Since G is non-abelian, then $Z(G) \neq G$. Assume $1 < Z(G) < 15$. By Lagrange's Theorem, $Z(G)$ has order 3 or 5. If $|Z(G)| = 3$, then $|G/Z(G)| = 5$ and $G/Z(G) \cong Z_5$. If $|Z(G)| = 5$, then $|G/Z(G)| = 3$ and $G/Z(G) \cong Z_3$. In either case, $G/Z(G)$ is cyclic by Corollary 3.10, and Exercise 3.1.36 implies that G is abelian, a contradiction. Therefore, $Z(G) = 1$.

Now suppose $g \in G$ is nonidentity. Since $\langle g \rangle \leq C_G(g)$, then $|C_G(g)|$ is 3, 5, or 15 by Lagrange's Theorem. If $|C_G(g)| = 15$, then $C_G(g) = G$, so $g \in Z(G)$, a contradiction. Therefore, $|C_G(g)|$ is 3 or 5 for all nonidentity $g \in G$. By Proposition 4.6, we have $|\mathcal{K}_g| = |G : C_G(g)|$, so that $|\mathcal{K}_g|$ is 5 or 3 respectively. The identity element forms a conjugacy class of size 1, and the class equation must involve a summation of sizes 3 and 5 that adds to 14. The only such combination is three classes of size 3 and one class of size 5. Therefore, the class equation of G is $15 = 1 + 3 + 3 + 3 + 5$. ■

(7) For $n = 3, 4, 6$, and 7 make lists of the partitions of n and give representatives for the corresponding conjugacy classes of S_n.

Solution. $n = 3$:

Partition of 3	**Representative of Cycle Type**
1, 1, 1	1
2, 1	(1 2)
3	(1 2 3)

$n = 4$:

Partition of 4	**Representative of Cycle Type**
1, 1, 1, 1	1
2, 1, 1	(1 2)
2, 2	(1 2)(3 4)
3, 1	(1 2 3)
4	(1 2 3 4)

$n = 6$:

Partition of 6	Representative of Cycle Type
1, 1, 1, 1, 1, 1	1
2, 1, 1, 1, 1	(1 2)
2, 2, 1, 1	(1 2)(3 4)
2, 2, 2	(1 2)(3 4)(5 6)
3, 1, 1, 1	(1 2 3)
3, 2, 1	(1 2 3)(4 5)
3, 3	(1 2 3)(4 5 6)
4, 1, 1	(1 2 3 4)
4, 2	(1 2 3 4)(5 6)
5, 1	(1 2 3 4 5)
6	(1 2 3 4 5 6)

$n = 7$:

Partition of 7	Representative of Cycle Type
1, 1, 1, 1, 1, 1, 1	1
2, 1, 1, 1, 1, 1	(1 2)
2, 2, 1, 1, 1	(1 2)(3 4)
2, 2, 2, 1	(1 2)(3 4)(5 6)
3, 1, 1, 1, 1	(1 2 3)
3, 2, 1, 1	(1 2 3)(4 5)
3, 2, 2	(1 2 3)(4 5)(6 7)
3, 3, 1	(1 2 3)(4 5 6)
4, 1, 1, 1	(1 2 3 4)
4, 2, 1	(1 2 3 4)(5 6)
4, 3	(1 2 3 4)(5 6 7)
5, 1, 1	(1 2 3 4 5)
5, 2	(1 2 3 4 5)(6 7)
6, 1	(1 2 3 4 5 6)
7	(1 2 3 4 5 6 7)

■

(8) Prove that $Z(S_n) = 1$ for all $n \geq 3$.

Solution. Suppose $\sigma \in Z(S_n)$ for some $n \geq 3$. Then σ commutes with every element of S_n. In particular, σ commutes with all transpositions (the set of which generate S_n). Let $(a\ b)$ be any transposition in S_n. Then we have $\sigma(a\ b)\sigma^{-1} = (a\ b)$. This implies that $(\sigma(a)\ \sigma(b)) = (a\ b)$, so $\sigma(a) = a$ and $\sigma(b) = b$. Since a and b were arbitrary, σ fixes every element of $\{1, 2, \ldots, n\}$. Therefore, σ is the identity permutation. Hence, $Z(S_n) = \{1\}$ for all $n \geq 3$. ■

(9) Show that $|C_{S_n}((1\ 2)(3\ 4))| = 8(n-4)!$ for all $n \geq 4$. Determine the elements in this centralizer explicitly.

Solution. The $(n-4)!$ factor arises from the fact that permutations on the $n-4$ integers not involved in the cycle $(1\ 2)(3\ 4)$ commute with it. Therefore, we need only consider the permutations of $\{1, 2, 3, 4\}$ that commute with $(1\ 2)(3\ 4)$. Computing $C_{S_4}((1\ 2)(3\ 4))$ directly, the permutations that fall in this set need to leave $(1\ 2)(3\ 4)$ unchanged, or swap the two transpositions. The permutations that leave $(1\ 2)(3\ 4)$ unchanged are 1, $(1\ 2)$, $(3\ 4)$, and $(1\ 2)(3\ 4)$. The permutations that swap the two transpositions are $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, $(1\ 3\ 2\ 4)$, and $(1\ 4\ 2\ 3)$. Therefore,

$$C_{S_4}((1\ 2)(3\ 4)) = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\},$$

which has size 8. Combining this with the $(n-4)!$ factor, we have $|C_{S_n}((1\ 2)(3\ 4))| = 8(n-4)!$ for all $n \geq 4$. ■

(10) Let σ be the 5-cycle $(1\ 2\ 3\ 4\ 5)$ in S_5. In each of (a) to (c) find an explicit element $\tau \in S_5$ which accomplishes the specified conjugation:

(a) $\tau\sigma\tau^{-1} = \sigma^2$

(b) $\tau\sigma\tau^{-1} = \sigma^{-1}$

(c) $\tau\sigma\tau^{-1} = \sigma^{-2}$

Solution.

(a) $\sigma^2 = (1\ 3\ 5\ 2\ 4)$. Then $\tau = (2\ 3\ 5\ 4)$.

(b) $\sigma^{-1} = (1\ 5\ 4\ 3\ 2)$. Then $\tau = (1\ 5)(2\ 4)$.

(c) $\sigma^{-2} = (1\ 4\ 2\ 5\ 3)$. Then $\tau = (2\ 4\ 5\ 3)$. ■

(11) In each of (a) – (d) determine whether σ_1 and σ_2 are conjugate. If they are, given an explicit permutation τ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.

(a) $\sigma_1 = (1\ 2)(3\ 4\ 5)$ and $\sigma_2 = (1\ 2\ 3)(4\ 5)$

(b) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = (3\ 7\ 5\ 10)(4\ 9)(13\ 11\ 2)$

(c) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = \sigma_1^3$

(d) $\sigma_1 = (1\ 3)(2\ 4\ 6)$ and $\sigma_2 = (3\ 5)(2\ 4)(5\ 6)$

Solution.

(a) Rewrite σ_2 as $(4\ 5)(1\ 2\ 3)$ so that both have the same cycle type. Then $\tau = (1\ 4\ 2\ 5\ 3)$.

(b) Rewrite σ_2 as $(4\ 9)(13\ 11\ 2)(3\ 7\ 5\ 10)$. Then $\tau = (1\ 4)(8\ 5\ 9)(6\ 7\ 11\ 10\ 3\ 13)$.

(c) Note that $\sigma_2 = (1\ 5)(6\ 10\ 11\ 8)$, which does not have the same cycle type as σ_1. Therefore, they are not conjugate.

(d) $\sigma_2 = (2\ 4)(3\ 5\ 6)$. Then $\tau = (1\ 2\ 3\ 4\ 5)$. ■

(12) Find a representative for each conjugacy class of elements of order 4 in S_8 and S_{12}.

Solution. S_8:

Cycle Type	Representative
4, 4	(1 2 3 4)(5 6 7 8)
4, 2, 2	(1 2 3 4)(5 6)(7 8)
4, 2, 1, 1	(1 2 3 4)(5 6)
4, 1, 1, 1, 1	(1 2 3 4)

S_{12}:

Cycle Type	Representative
4, 4, 4	(1 2 3 4)(5 6 7 8)(9 10 11 12)
4, 4, 2, 2	(1 2 3 4)(5 6 7 8)(9 10)(11 12)
4, 4, 2, 1, 1	(1 2 3 4)(5 6 7 8)(9 10)
4, 4, 1, 1, 1, 1	(1 2 3 4)(5 6 7 8)
4, 2, 2, 2, 2	(1 2 3 4)(5 6)(7 8)(9 10)(11 12)
4, 2, 2, 2, 1, 1	(1 2 3 4)(5 6)(7 8)(9 10)
4, 2, 2, 1, 1, 1, 1	(1 2 3 4)(5 6)(7 8)
4, 2, 1, 1, 1, 1, 1, 1	(1 2 3 4)(5 6)
4, 1, 1, 1, 1, 1, 1, 1, 1	(1 2 3 4)

■

(13) Find all finite groups which have exactly two conjugacy classes.

Solution. Let G be a finite group with exactly two conjugacy classes. One of these classes must be $\{1\}$, the identity element. Let $\mathcal{K}$ be the other conjugacy class, and let $g \in \mathcal{K}$. By Proposition 4.6, we have $|\mathcal{K}| = |G : C_G(g)|$. Since there are only two conjugacy classes, then $|\mathcal{K}| = |G| - 1$. Therefore, $|G : C_G(g)| = |G| - 1$, which implies that $|C_G(g)| = |G|/(|G| - 1)$. Since $|C_G(g)|$ is an integer, then $|G| - 1$ divides $|G|$. This is only possible if $|G| - 1 = 1$, so that $|G| = 2$. Therefore, the only finite group with exactly two conjugacy classes is the group of order 2, which is isomorphic to Z_2. ■

(14) In Exercise 4.2.1 two labellings of the elements $\{1, a, b, c\}$ of the Klein 4-group V_4 were chosen to give two versions of the left regular representation of V_4 into S_4. Let π_1 be the version of regular representation obtained in part (a) of that exercise, and let π_2 be the version obtained via the labelling in part (b). Let $\tau = (2\ 4)$. Show that $\tau \circ \pi_1(g) \circ \tau^{-1} = \pi_2(g)$ for each $g \in V_4$ (i.e., conjugation by τ sends the image of π_1 to the image of π_2 elementwise).

Solution. We will compute for a, as the rest follow similarly. We have $\pi_1(a) = (1\ 2)(3\ 4)$ and $\pi_2(a) = (1\ 4)(2\ 3)$. Then $\tau \circ \pi_1(a) \circ \tau^{-1} = (2\ 4)(1\ 2)(3\ 4)(2\ 4) = (1\ 4)(2\ 3) = \pi_2(a)$. ■

(15) Find an element of S_8 which conjugates the subgroup of S_8 obtained in part (a) of Exercise 4.2.3 to the subgroup of S_8 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).

Solution. Recall by Exercise 1.7.17 that left conjugation is an automorphism, so it suffices to find an element which sends the generators of the first subgroup to the generators of the second subgroup. The generators of the first subgroup are $(1\ 2\ 3\ 4)(5\ 8\ 7\ 6)$ and $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$, while the generators of the second subgroup are $(1\ 3\ 5\ 7)(2\ 8\ 6\ 4)$ and $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$ respectively. It suffices to check some element τ which sends the first generator to the second; the second generator will follow automatically. One such element is $\tau = (5\ 2\ 3)(6\ 4\ 7)$. ■

(16) Find an element of S_4 which conjugates the subgroup of S_4 obtained in part (a) of Exercise 4.2.5 to the subgroup of S_4 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).

Solution. We proceed similarly to the preceding exercise. The generators of the first subgroup are $(1\ 2\ 3\ 4)$ and $(2\ 4)$, while the generators of the second subgrgoup are $(1\ 3\ 2\ 4)$ and $(3\ 4)$. We obtain $\tau = (2\ 3)$. ■

(17) Let A be a nonempty set and let X be any subset of S_A. Let

$$F(X) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in X\} \qquad \text{—the } \textit{fixed set} \text{ of } X$$

Let $M(X) = A - F(X)$ be the elements which are *moved* by some element of X. Let $D = \{\sigma \in S_A \mid |M(\sigma)| < \infty\}$. Prove that D is a normal subgroup of S_A.

Solution. Note that $1 \in D$, since $M(1) = \varnothing$ as it fixes all elements of A. Let $\sigma, \tau \in D$. Then $|M(\sigma)| < \infty$ and $|M(\tau)| < \infty$. Suppose $a \in F(\sigma) \cap F(\tau)$. Clearly, $a \in F(\sigma\tau)$. By contrapositive, then $a \in M(\sigma\tau)$ implies $a \in M(\sigma) \cup M(\tau)$, which are both finite, hence $M(\sigma\tau)$ is finite. Therefore, $\sigma\tau \in D$.

Now consider $\sigma \in D$. If $a \in A$ is fixed by σ, then it is fixed by σ^{-1}. Therefore, any element moved by σ^{-1} must be moved by σ, and vice-versa. Hence, $M(\sigma^{-1}) = M(\sigma)$, which is finite. Therefore, $\sigma^{-1} \in D$.

Finally, consider $\sigma \in D$ and $\tau \in S_A$. Suppose $a \in F(\tau\sigma\tau^{-1})$ so that $\tau\sigma\tau^{-1}(a) = a$. Then $\sigma(\tau^{-1}(a)) = \tau^{-1}(a)$, hence $\tau^{-1}(a) \in F(\sigma)$. By contrapositive, if $a \in M(\tau\sigma\tau^{-1})$, then $\tau^{-1}(a) \in M(\sigma)$. Since $M(\sigma)$ is finite, then $M(\tau\sigma\tau^{-1})$ is finite. Therefore, $\tau\sigma\tau^{-1} \in D$. ■

(18) Let A be a set, let H be a subgroup of S_A, and let $F(H)$ be the fixed points of H on A as defined in the preceding exercise. Prove that if $\tau \in N_{S_A}(H)$, then τ stabilizes the set $F(H)$ and its complement $A - F(H)$.

Solution. Suppose $\sigma \in H$. Since $\tau \in N_{S_A}(H)$, we have $\tau^{-1} \in N_{S_A}(H)$, hence $\tau^{-1}\sigma\tau \in H$. Suppose $a \in F(H)$. Then $\tau^{-1}\sigma\tau(a) = a$, so that $\sigma\tau(a) = \tau(a)$. Therefore, $\tau(a) \in F(H)$, and $\tau(F(H)) \subseteq F(H)$. Bijectivity of τ also implies that $\tau^{-1}(F(H)) \subseteq F(H)$, which shows that $F(H) \subseteq \tau(F(H))$, hence $\tau(F(H)) = F(H)$. Therefore, τ stabilizes $F(H)$. Moreover, since τ is a bijection, it also stabilizes the complement $A - F(H)$. ■

(19) Assume H is a normal subgroup of G, $\mathcal{K}$ is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Prove that $\mathcal{K}$ is a union of k conjugacy classes of equal size in H, where $k = |G : HC_G(x)|$. Deduce that a conjugacy class in S_n which consists of even permutations is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n. [Let $A = C_G(x)$ and $B = H$ so $A \cap B = C_H(x)$. Draw the lattice diagram associated to the Second Isomorphism Theorem and interpret the appropriate indices. See also Exercise 4.1.9.]

Solution. Let G act on $\mathcal{K}$ by conjugation. Since $\mathcal{K}$ is a conjugacy class of G, this action is transitive. Because $H \trianglelefteq G$ and $\mathcal{K} \subseteq H$, then H also acts on $\mathcal{K}$ by conjugation. Let $\mathcal{O}$ be one such orbit of this action, and suppose $y \in \mathcal{O}$. By Proposition 4.6, we have $|\mathcal{O}| = |H : C_H(y)|$. By normality of H in G, we have $C_H(y) = C_G(y) \cap H$. Using the Second Isomorphism Theorem, we have

$$HC_G(y)/C_G(y) \cong H/C_H(y)$$

so that $|H : C_H(y)| = |HC_G(y) : C_G(y)|$. Therefore, $|\mathcal{O}| = |HC_G(y) : C_G(y)|$. Using Exercise 4.1.9, we know that each orbit of H on $\mathcal{K}$ has the same size, so every orbit has size $|HC_G(y) : C_G(y)|$. Suppose there are k orbits. Then

$$|\mathcal{K}| = k|HC_G(y) : C_G(y)|.$$

By Proposition 4.6, we also have $|\mathcal{K}| = |G : C_G(y)|$. Therefore,

$$|G : C_G(y)| = k|HC_G(y) : C_G(y)|.$$

Dividing both sides by $|HC_G(y) : C_G(y)|$, we obtain $k = |G : HC_G(y)|$. Hence, $\mathcal{K}$ is a union of k conjugacy classes of equal size in H.

Now suppose $\mathcal{K} \subseteq A_n$ is a conjugacy class of S_n consisting of even permutations. Let $x \in \mathcal{K}$. Applying the preceding result with $H = A_n$, we have that $\mathcal{K}$ is a union of k conjugacy classes of equal size in A_n, where $k = |S_n : A_nC_{S_n}(x)|$. Since $|S_n : A_n| = 2$, then k is either 1 or 2. Therefore, $\mathcal{K}$ is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n. ■

(20) Let $\sigma \in A_n$. Show that all elements in the conjugacy class of σ in S_n (i.e., all elements of the same cycle type as σ) are conjugate in A_n if and only if σ commutes with an odd permutation. [Use the preceding exercise.]

Solution. ($\Rightarrow$) Recall by the previous exercise that the conjugacy class of σ in S_n is either a single conjugacy class in A_n or a union of two conjugacy classes of equal size in A_n. Suppose all elements in the conjugacy class of σ in S_n are conjugate in A_n. Then the conjugacy class of σ in S_n is a single conjugacy class in A_n, so that $k = |S_n : A_nC_{S_n}(\sigma)| = 1$. Therefore, $S_n = A_nC_{S_n}(\sigma)$, so that there exists some odd permutation $\tau \in S_n$ such that $\tau \in C_{S_n}(\sigma)$. Hence, σ commutes with an odd permutation.

($\Leftarrow$) Suppose σ commutes with an odd permutation $\tau \in S_n$. Then $\tau \in C_{S_n}(\sigma)$, so that $A_nC_{S_n}(\sigma)$ contains odd permutations. Therefore, $|S_n : A_nC_{S_n}(\sigma)| = 1$, so that the conjugacy class of σ in S_n is a single conjugacy class in A_n. Hence, all elements in the conjugacy class of σ in S_n are conjugate in A_n. ■

(21) Let $\mathcal{K}$ be a conjugacy class in S_n and assume that $\mathcal{K} \subseteq A_n$. Show $\sigma \in S_n$ does *not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers. Deduce that $\mathcal{K}$ consists of two conjugacy clases in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers. [Assume first that $\sigma \in \mathcal{K}$ does not commute with any odd permutation. Observe that σ commutes with each individual cycle in its cycle decomposition—use this to show that all its cycles must be of odd length. If two cycles have the same odd length, k, find a product of k transpositions which interchanges them and commutes with σ. Conversely, if the cycle type of σ consists of distinct integers, prove that σ commutes *only* with the group generated by the cycles in its cycle decomposition.]

Solution. ($\Rightarrow$) Suppose $\sigma \in S_n$ does not commute with any odd permutation. Let the cycle decomposition of σ be $\sigma = \tau_1\tau_2 \cdots \tau_k$, where each τ_i is a disjoint cycle. Since σ commutes with each τ_i, then each τ_i must be of odd length; otherwise, τ_i would be an odd permutation commuting with σ. Now suppose two cycles τ_i and τ_j have the same odd length m. Then the product of m transpositions which interchanges the elements of τ_i and τ_j is an odd permutation which commutes with σ, contradicting our assumption. Therefore, all cycles in the cycle decomposition of σ must have distinct odd lengths.

($\Leftarrow$) Suppose the cycle type of σ consists of distinct odd integers. Let the cycle decomposition of σ be $\sigma = \tau_1\tau_2 \cdots \tau_k$, where each τ_i is a disjoint cycle of odd length. Any permutation that commutes with σ must permute the cycles τ_i among themselves. However, since the lengths of the cycles are distinct, the only way to permute them while preserving their lengths is to leave them unchanged. Therefore, any permutation that commutes with σ must be a product of powers of the individual cycles τ_i. Since each τ_i has odd length, any such product will be an even permutation. Hence, σ does not commute with any odd permutation. ■

(22) Show that if n is odd, then the set of all n-cycles consists of two conjugacy classes of equal size in A_n.

Solution. Let $\sigma \in S_n$ be an n-cycle. Since n is odd, the cycle type of σ consists of the single odd integer n, which is distinct. By the previous exercise, σ does not commute with any odd permutation. Therefore, by the exercise before that, the conjugacy class of σ in S_n consists of two conjugacy classes of equal size in A_n. Since this holds for any n-cycle σ, the set of all n-cycles consists of two conjugacy classes of equal size in A_n. ■

(23) Recall (cf. Exercise 2.4.16) that a proper subgroup M of G is called *maximal* if whenever $M \leq H \leq G$, either $H = M$ or $H = G$. Prove that if M is a maximal subgroup of G then either $N_G(M) = M$ or $N_G(M) = G$. Deduce that if M is a maximal subgroup of G that is not normal in G, then the number of nonidentity elements of G that are contained in conjugates of M is at most $(|M| - 1)|G : M|$.

Solution. Suppose M is a maximal subgroup of G. By definition, $N_G(M)$ is a subgroup of G containing M. Therefore, by maximality of M, either $N_G(M) = M$ or $N_G(M) = G$.

Now suppose M is a maximal subgroup of G that is not normal in G. Then by the previous result, we have $N_G(M) = M$. By Proposition 4.6, the size of the conjugacy class of M in G is $|G : N_G(M)| = |G : M|$. Each conjugate of M contains $|M| - 1$ nonidentity elements. Therefore, the total number of nonidentity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$. ■

(24) Assume H is a proper subgroup of the finite group G. Prove

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

i.e., G is not the union of the conjugates of any proper subgroup. [Put H in some maximal subgroup and use the preceding exercise.]

Solution. Suppose H is a proper subgroup of the finite group G. Then there exists a maximal subgroup M of G such that $H \leq M < G$. By the previous exercise, either $N_G(M) = M$ or $N_G(M) = G$, so that we have two cases: either $M \trianglelefteq G$ or M is not normal in G.

If M is normal in G, then all conjugates of M are equal to M. Therefore, the union of the conjugates of H is contained in M, which is a proper subset of G. Hence,

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

Now suppose M is not normal in G. Then by the previous exercise, the number of nonidentity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$. Moreover, $H \leq M$ implies that any conjugate of H is contained in a conjugate of M. Therefore, the number of nonidentity elements of G contained in conjugates of H is also at most $(|M| - 1)|G : M|$. Since M is a proper subgroup of G, then $|G : M| \geq 2$, so that $(|M| - 1)|G : M| < |G| - 1$. Therefore, there exists at least one nonidentity element of G that is not contained in any conjugate of H, hence

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$ ■

(25) Let $G = \mathrm{GL}_2(\mathbb{C})$ and let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{C}, ac \neq 0 \right\}.$$

Prove that every element of G is conjugate to some element of the subgroup H and deduce that G is the union of conjugates of H. [Show that every element of $\mathrm{GL}_2(\mathbb{C})$ has an eigenvector.]

Solution. Suppose $X \in G$, where X is the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and consider the characteristic polynomial $\chi_X(t) = \det(X - tI) = t^2 - (a + d)t + (ad - bc)$. Since $\mathbb{C}$ is closed under complex multiplication, $\chi_X(t)$ has at least one root $\lambda \in \mathbb{C}$. Therefore, there exists a nonzero vector $\mathbf{v} \in \mathbb{C}^2$ such that $X\mathbf{v} = \lambda\mathbf{v}$, so that $\mathbf{v}$ is an eigenvector of X corresponding to the eigenvalue λ. We may extend $\mathbf{v}$ to a basis $\{\mathbf{v}, \mathbf{w}\}$ of $\mathbb{C}^2$. Let P be the matrix whose columns are $\mathbf{v}$ and $\mathbf{w}$. Then P is invertible, and we have

$$P^{-1}XP = \begin{pmatrix} \lambda & \alpha \\ 0 & \beta \end{pmatrix} \in H.$$

for some $\alpha, \beta \in \mathbb{C}$ such that $X\mathbf{w} = \alpha\mathbf{v} + \beta\mathbf{w}$. Therefore, every element of G is conjugate to some element of the subgroup H, hence every element of G is contained in some conjugate of H. Thus,

$$G = \bigcup_{g \in G} gHg^{-1}.$$ ■

(26) Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$ (such an element σ is called *fixed point free*).

Solution. For each $a \in A$, consider G_a. By transitivity of G on A, we have $|G : G_a| = |A| > 1$, so that G_a is a proper subgroup of G. By Exercise 4.3.24, we have

$$G \neq \bigcup_{g \in G} gG_ag^{-1}.$$

Therefore, there exists some $\sigma \in G$ such that $\sigma \notin gG_ag^{-1}$ for all $g \in G$. Moreover, if $\sigma(a) = a$ for some $a \in A$, then $\sigma \in G_a$, hence $\sigma \in gG_ag^{-1}$ for $g = 1$, a contradiction. Therefore, $\sigma(a) \neq a$ for all $a \in A$. ■

(27) Let $g_1, g_2, \ldots, g_r$ be representatives of the conjugacy classes of the finite group G and assume these elements pairwise commute. Prove that G is abelian.

Solution. Pick some g_i and consider its conjugacy class $\mathcal{K}_i$. Since g_i commutes with all g_j for $1 \leq j \leq r$, then for any $x \in G$, we have $xg_ix^{-1} = g_i$ so that $x \in C_G(g_i)$. Therefore, $C_G(g_i) = G$, so that $\mathcal{K}_i = \{g_i\}$. Since this holds for all $1 \leq i \leq r$, then every conjugacy class of G is a singleton set. Hence, for any $x, y \in G$, we have $xyx^{-1} = y$, so that $xy = yx$. Therefore, G is abelian. ■

(28) Let p and q be primes with $p < q$. Prove that a non-abelian group G of order pq has a nonnormal subgroup of index q so that there exists an injective homomorphism into S_q. Deduce that G is isomorphic to a subgroup of the normalizer in S_q of the cyclic group generated by the q-cycle $(1\ 2\ \cdots\ q)$.

Solution. By Cauchy's Theorem, there exists $g \in G$ such that $|g| = q$, hence $\langle g \rangle$ has order q and is of index p. Moreover, $\langle g \rangle$ is not normal in G, for otherwise $G/\langle g \rangle$ would be cyclic and isomorphic to Z_p, contradicting that G is non-abelian. Similarly, G also contains a subgroup P of order p and index q and is similarly not normal in G.

Let G act on the left cosets of P in G by left multiplication. Then there is the associated permutation representation $\pi : G \to S_q$. In particular, π is injective: If $\pi(x) = 1$ for some $x \in G$, then $xgP = gP$ for every $g \in G$, or $g^{-1}xg \in P$ for every $g \in G$. But $\ker \pi \trianglelefteq G$ and is contained in P so that $\ker \pi$ has order 1 or p. If $|\ker \pi| = p$, then $\ker \pi = P$ is normal in G, a contradiction. Therefore, $\ker \pi = 1$ and π is injective.

Recall that $|g| = q$ so that $|\pi(g)| = q$, so $\pi(g)$ acts transitively on G/P since its powers generate q distinct cosets. Now pick $h \in G$. From Exercise 1.1.22, it follows that $|hgh^{-1}| = |g| = q$ so that $hgh^{-1} = g^k$ for some integer k with $1 \leq k < q$. Therefore,

$$\pi(h)\pi(g)\pi(h)^{-1} = \pi(hgh^{-1}) = \pi(g^k) = (\pi(g))^k \in \langle \pi(g) \rangle.$$

Hence, $\pi(h) \in N_{S_q}(\langle \pi(g) \rangle)$. Since h was arbitrary, we have $G \cong \pi(G) \leq N_{S_q}(\langle \pi(g) \rangle)$. Therefore, G is isomorphic to a subgroup of the normalizer in S_q of the cyclic group generated by the q-cycle $(1\ 2\ \cdots\ q)$. ■

(29) Let p be a prime and let G be a group of order p^α. Prove that G has a subgroup of order p^β, for every β with $0 \leq \beta \leq \alpha$. [Use Theorem 8 and induction on α.]

Solution. We proceed by induction on α. If $\alpha = 0$, then G is the trivial group, which has a subgroup of order $p^0 = 1$. Now suppose the result holds for all groups of order p^k for some $k \geq 0$. Let G be a group of order p^{k+1}. By Theorem 8, $Z(G)$ is nontrivial, so there exists some $x \in Z(G)$ such that $|x| = p$. Then $\langle x \rangle$ is a normal subgroup of G of order p. Consider the quotient group $G/\langle x \rangle$, which has order p^k. By the induction hypothesis, for every β with $0 \leq \beta \leq k$, there exists a subgroup $H/\langle x \rangle$ of $G/\langle x \rangle$ such that $|H/\langle x \rangle| = p^\beta$. By the Lattice Isomorphism Theorem, there exists a subgroup H of G such that $\langle x \rangle \leq H$ and $|H| = p^{\beta+1}$. Therefore, for every β with $1 \leq \beta \leq k+1$, there exists a subgroup of G of order p^β. Since the trivial subgroup has order $p^0 = 1$, the result holds for all β with $0 \leq \beta \leq k+1$. By induction, the result holds for all $\alpha \geq 0$. ■

(30) If G is a group of odd order, prove for any nonidentity element $x \in G$ that x and x^{-1} are not conjugate in G.

Solution. Suppose for contradiction that x and x^{-1} are conjugate in G. Then there exists $g \in G$ such that $gxg^{-1} = x^{-1}$. If we conjugate both sides by g again, we obtain

$$g^2xg^{-2} = gx^{-1}g^{-1} = (gxg^{-1})^{-1} = (x^{-1})^{-1} = x$$

so that $g^2x = xg^2$. Then $g^2 \in C_G(x)$. Consider the quotient group $G/C_G(x)$. Since $g^2 \in C_G(x)$, we have $(gC_G(x))^2 = C_G(x)$, so that the order of $gC_G(x)$ in $G/C_G(x)$ is 1 or 2. However, since G has odd order, then $G/C_G(x)$ also has odd order, so the order of $gC_G(x)$ cannot be 2. Therefore, the order of $gC_G(x)$ is 1, so that $g \in C_G(x)$. But this implies that $gxg^{-1} = x$, contradicting our assumption. Therefore, x and x^{-1} are not conjugate in G. ∎

(31) Using the usual generators and relations for the dihedral group D_{2n} (cf. Section 1.2) show that for $n = 2k$ an even integer the conjugacy classes in D_{2n} are the following: $\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\}$ and $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Give the class equation for D_{2n}.

Solution. We immediately have two conjugacy classes, $\{1\}$ and $\{r^n\}$, since $r^n \in Z(D_{2n})$ when n is even. Moreover, recall that the elements of D_{2n} are of the form r^m or sr^m for some integer m. Consider the conjugacy class of r^k for some $1 \leq k < n$ except $k = n/2$. For any j, we have

$$r^j r^k r^{-j} = r^k, \quad \text{and} \quad sr^j r^k r^{-j} s = r^{-k}$$

so that the conjugacy class of r^k is $\{r^{\pm k}\}$. Now consider the conjugacy class of sr^m for some integer m. For any j, we have

$$r^j sr^m r^{-j} = sr^{m-2j}, \quad \text{and} \quad sr^j sr^m r^{-j} s = r^{-(m-2j)}$$

so that the conjugacy class of sr^m is $\{sr^{m-2j} \mid j \in \mathbb{Z}\}$. If m is even, then this conjugacy class is $\{sr^{2b} \mid b = 1, \ldots, k\}$; if m is odd, then this conjugacy class is $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Therefore, the conjugacy classes in D_{2n} when n is even are $\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\}$ and $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. Lastly, the class equation for D_{2n} is

$$|D_{2n}| = 1 + 1 + 2(k-1) + k + k.$$ ∎

(32) For $n = 2k + 1$ an odd integer, show that the conjugacy classes in D_{2n} are $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}$, and $\{sr^b \mid b = 1, \ldots, n\}$. Give the class equation for D_{2n}.

Solution. We immediately have the conjugacy class $\{1\}$. Moreover, recall that the elements of D_{2n} are of the form r^m or sr^m for some integer m. Consider the conjugacy class of r^k for some $1 \leq k \leq n$ except $k = n/2$. For any j, we have

$$r^j r^k r^{-j} = r^k, \quad \text{and} \quad sr^j r^k r^{-j} s = r^{-k}$$

so that the conjugacy class of r^k is $\{r^{\pm k}\}$. Now consider the conjugacy class of sr^m for some integer m. For any j, we have

$$r^j sr^m r^{-j} = sr^{m-2j}, \quad \text{and} \quad sr^j sr^m r^{-j} s = r^{-(m-2j)}$$

so that the conjugacy class of sr^m is $\{sr^{m-2j} \mid j \in \mathbb{Z}\}$. Since n is odd, this conjugacy class is $\{sr^b \mid b = 1, \ldots, n\}$. Therefore, the conjugacy classes in D_{2n} when n is odd are $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}$, and $\{sr^b \mid b = 1, \ldots, n\}$. Lastly, the class equation for D_{2n} is

$$|D_{2n}| = 1 + 2k + n.$$ ∎

(33) This exercise gives a formula for the size of each conjugacy class in S_n. Let σ be a permutation in S_n and let $m_1, m_2, \ldots, m_s$ be the *distinct* integers which appear in the cycle type of σ (including 1-cycles). For each $i \in \{1, 2, \ldots, s\}$ assume σ has k_i cycles of length m_i (so that $\sum_1^s k_i m_i = n$). Prove that the number of conjugates of σ is

$$\frac{n!}{(k_1! m_1^{k_1})(k_2! m_2^{k_2}) \cdots (k_s! m_s^{k_s})}$$

[See Exercise 1.3.6 and Exercise 1.3.7 where this formula was given in some special cases.]

Solution. We start with n integers. We see that there are $n!$ ways to arrange these integers. Now consider the k_1 cycles of length m_1 in the cycle decomposition of σ. Clearly, we must use $k_1 m_1$ of the n integers to form these cycles. However, there are $m_1^{k_1}$ ways to arrange the integers within each of these k_1 cycles, and there are $k_1!$ ways to arrange the k_1 cycles among themselves. Therefore, we must divide $n!$ by $(k_1! m_1^{k_1})$ to account

for these arrangements. Continuing in this manner for each i from 1 to s, we see that the total number of distinct arrangements of the n integers that correspond to the same cycle type as σ is given by

$$\frac{n!}{(k_1!m_1^{k_1})(k_2!m_2^{k_2})\cdots(k_s!m_s^{k_s})}.$$

Since the conjugacy class of σ in S_n consists of all permutations with the same cycle type as σ, the number of conjugates of σ is given by this formula. ■

(34) Prove that if p is a prime and P is a subgroup of S_p of order p, then $|N_{S_p}(P)| = p(p-1)$. [Argue that every conjugate of P contains exactly $p-1$ p-cycles and use the formula for the number of p-cycles to compute the index of $N_{S_p}(P)$ in S_p.]

Solution. Note that P is cyclic of order p, so $P = \langle\sigma\rangle$ for some p-cycle $\sigma \in S_p$. Moreover, every nonidentity element of P is a p-cycle, so P contains exactly $p-1$ p-cycles. Now for some $\tau \in S_p$, the conjugate $\tau P\tau^{-1} = \langle\tau\sigma\tau^{-1}\rangle$ also has order p and contains exactly $p-1$ p-cycles. Therefore, each conjugate of P contains exactly $p-1$ p-cycles. Note that the number of distinct p-cycles in S_p is given by $p!/p = (p-1)!$.

Recall by Proposition 4.6 that the size of the conjugacy class of P in S_p is given by $|S_p : N_{S_p}(P)|$. Let this index be k. Since each conjugate of P contains exactly $p-1$ p-cycles, the total number of distinct p-cycles contained in all conjugates of P is $k(p-1)$. However, since every p-cycle in S_p is contained in some conjugate of P, we have $k(p-1) = (p-1)!$. Therefore, $k = (p-2)!$, so that

$$|N_{S_p}(P)| = \frac{|S_p|}{k} = \frac{p!}{(p-2)!} = p(p-1).$$ ■

(35) Let p be a prime. Find a formula for the number of conjugacy classes of elements of order p in S_n (using the greatest integer function).

Solution. Note that elements of order p in S_n are products of disjoint p-cycles. Moreover, each p-cycle is conjugate to any other p-cycle in S_n. Therefore, the conjugacy class of an element of order p in S_n is determined by the number of disjoint p-cycles in its cycle decomposition. Let k be the number of disjoint p-cycles in the cycle decomposition of such an element. Then we have $1 \le k \le \lfloor n/p \rfloor$, hence the number of conjugacy classes of elements of order p in S_n is given by $\lfloor n/p \rfloor$. ■

(36) Let $\pi : G \to S_G$ be the left regular representation afforded by the action of G on itself by left multiplication. For each $g \in G$ denote the permutation $\pi(g)$ by σ_g so that $\sigma_g(x) = gx$ for all $x \in G$. Let $\lambda : G \to S_G$ be the permutation representation afforded by the corresponding right action of G on itself, and for each $h \in G$ denote the permutation $\lambda(h)$ by τ_h. Thus $\tau_h(x) = xh^{-1}$ for all $x \in G$ (λ is called the *right regular representation* of G).

(a) Prove that σ_g and τ_h commute for all $g, h \in G$. (Thus the centralizer in S_G of $\pi(G)$ contains the subgroup $\lambda(G)$ which is isomorphic to G).

(b) Prove that $\sigma_g = \tau_g$ if and only if g is an element of order 1 or 2 in the center of G.

(c) Prove that $\sigma_g = \tau_h$ if and only if g and h lie in the center of G. Deduce that $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$.

Solution.

(a) For any $x \in G$, we have

$$\sigma_g(\tau_h(x)) = \sigma_g(xh^{-1}) = g(xh^{-1}) = (gx)h^{-1} = \tau_h(gx) = \tau_h(\sigma_g(x)).$$

Therefore, σ_g and τ_h commute for all $g, h \in G$.

(b) If $\sigma_g = \tau_g$, then $gx = xg^{-1}$ for all $x \in G$. In particular, $x = 1$ implies $g = g^{-1}$ so that $g^2 = 1$, hence $|g|$ is 1 or 2. Moreover, for any $x \in G$, we have $gx = xg^{-1} = xg$, so that $g \in Z(G)$

If g is an element of order 1 or 2 in the center of G, then for any $x \in G$, we have $\sigma_g(x) = gx = xg = xg^{-1} = \tau_g(x)$. Therefore, $\sigma_g = \tau_g$.

(c) If $\sigma_g = \tau_h$, then $gx = xh^{-1}$ for all $x \in G$. In particular, $x = 1$ implies $g = h^{-1}$, so that $h = g^{-1}$. Therefore, $gx = xg^{-1}$ for all $x \in G$, so that by part (b), g lies in the center of G. Since $h = g^{-1}$, then h also lies in the center of G.

If g and h lie in the center of G, then for any $x \in G$, we have $\sigma_g(x) = gx = xg = xh^{-1} = \tau_h(x)$. Therefore, $\sigma_g = \tau_h$. Moreover, if $\sigma_g \in \pi(G) \cap \lambda(G)$, then there exists $h \in G$ such that $\sigma_g = \tau_h$. By the above result, both g and h lie in the center of G, so that $\sigma_g \in \pi(Z(G))$ and $\tau_h \in \lambda(Z(G))$. Conversely, if $g \in Z(G)$, then by part (b), we have $\sigma_g = \tau_g$, so that $\sigma_g \in \pi(G) \cap \lambda(G)$. Therefore, $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$. ■

4.4 Automorphisms

(1) Let G be a group. If $\sigma \in \mathrm{Aut}(G)$ and ϕ_g is conjugation by g, prove that $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)

Solution. For any $x \in G$, then

$$(\sigma\varphi_g\sigma^{-1})(x) = \sigma(\varphi_g(\sigma^{-1}(x))) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g)^{-1} = \sigma(g)x\sigma(g)^{-1} = \varphi_{\sigma(g)}(x).$$

Then $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Therefore, for any $\varphi_g \in \mathrm{Inn}(G)$ and any $\sigma \in \mathrm{Aut}(G)$, we have $\sigma\varphi_g\sigma^{-1} \in \mathrm{Inn}(G)$, so that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. ■

(2) Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic. (Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.)

Solution. By Cauchy's Theorem, there are elements $g, h \in G$ such that $|g| = p$ and $|h| = q$. Since G is abelian, we have $|gh| = \mathrm{lcm}(|g|, |h|) = \mathrm{lcm}(p, q) = pq$. Therefore, $G = \langle gh \rangle$ is cyclic. ■

(3) Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images (where r and s are the usual generators). Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.

Solution. Since $|r| = 4$, any automorphism σ of D_8 must send r to an element of order 4. The only elements of order 4 in D_8 are r and r^3, so r has at most 2 possible images under σ. Moreover, $|s| = 2$, so $\sigma(s)$ must be an element of order 2. The elements of order 2 in D_8 are s, sr, sr^2, and sr^3, so s has at most 4 possible images under σ. Therefore, there are at most $2 \cdot 4 = 8$ possible automorphisms of D_8, so that $|\mathrm{Aut}(D_8)| \leq 8$. ■

(4) Use arguments similar to those in the preceding exercise to show that $|\mathrm{Aut}(Q_8)| \leq 24$.

Solution. Note that $|i| = |j| = |k| = 4$, so any automorphism σ of Q_8 must send i to an element of order 4. The only elements of order 4 in Q_8 are $i, j, k, i^{-1}, j^{-1}, k^{-1}$, so i has at most 6 possible images under σ. Moreover, since $ij = k$, we have $\sigma(i)\sigma(j) = \sigma(k)$. Therefore, once we choose the image of i, there are 4 possible choices for the image of j (since it cannot be the inverse of the image of i). Hence, there are at most $6 \cdot 4 = 24$ possible automorphisms of Q_8, so that $|\mathrm{Aut}(Q_8)| \leq 24$. ■

(5) Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\mathrm{Aut}(D_8) \cong D_8$.

Solution. Consider the subgroup $H = \langle r^2, s \rangle$ of D_{16}. Note that $(r^2)^4 = s^2 = 1$, so this satisfies the same relations as D_8, hence $H \cong D_8$. Moreover, H is normal in D_{16} as it has index 2. Then $N_{D_{16}}(H) = D_{16}$. Moreover, $C_{D_{16}}(H)$ can be computed by considering the centralizers of the generators of H. Note that $C_{D_{16}}(r^2) = \langle r \rangle$ since only rotations commute with each other. Consider now the centralizer of s. For any rotation r^k, we have $sr^k = r^k s$ if and only if $r^{-k} = r^k$, which holds if and only if $k = 0$ or $k = 4$. For any reflection sr^k, we obtain the same conclusion so that $C_{D_{16}}(s) = \{1, r^4, s, sr^4\}$. Intersecting these, it is easy to see that $C_{D_{16}}(H) = Z(D_{16})$.

We now have that $N_{D_{16}}(H)/C_{D_{16}}(H) \cong D_{16}/Z(D_{16}) \cong D_8$. Now recall that $D_{16}/Z(D_{16})$ is still isomorphic to a subgroup of $\mathrm{Aut}(H)$ when acted on by conjugation. By Exercise 4.4.3, we know that $|\mathrm{Aut}(D_8)| \leq 8$, so that $\mathrm{Aut}(H) \cong D_8$. Therefore, $\mathrm{Aut}(D_8) \cong D_8$. ■

(6) Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.

Solution. If H char G, then $\varphi(H) = H$ for every $\varphi \in \mathrm{Aut}(G)$. In particular, this holds for every $\varphi_g \in \mathrm{Inn}(G)$ so that $\varphi_g(H) = gHg^{-1} = H$ for every $g \in G$. Therefore, $H \trianglelefteq G$.

Consider the abelian group $G = Z_2 \times Z_2$. Then every subgroup of G is normal since G is abelian. However, the subgroup $H = \{(0,0), (1,0)\}$ is not characteristic in G since the automorphism $\sigma : G \to G$ defined by $\sigma((a,b)) = (b,a)$ sends H to the distinct subgroup $\{(0,0), (0,1)\}$. Therefore, H is a normal subgroup of G that is not characteristic. ■

(7) If H is the unique subgroup of a given order in a group G, prove that H is characteristic in G.

Solution. For any $\sigma \in \mathrm{Aut}(G)$, the subgroup $\sigma(H)$ has the same order as H. Since H is the unique subgroup of that order in G, we must have $\sigma(H) = H$. Therefore, H is characteristic in G. ■

(8) Let G be a group with subgroups H and K with $H \leq K$.
   (a) Prove that if H is characteristic in K and K is normal in G, then H is normal in G.
   (b) Prove that if H is characteristic in K and K is characteristic in G, then H is characteristic in G. Use this to prove that the Klein 4-group V_4 is characteristic in S_4.
   (c) Give an example to show that if H is normal in K and K is characteristic in G, then H need not be normal in G.

Solution.
   (a) For any $g \in G$, consider the inner automorphism $\varphi_g \in \text{Inn}(G)$. Since $K \trianglelefteq G$, we have $\varphi_g(K) = K$. Moreover, since H char K, we have $\varphi_g(H) = H$. Therefore, $gHg^{-1} = H$ for all $g \in G$, so that $H \trianglelefteq G$.
   (b) For any $\sigma \in \text{Aut}(G)$, since K char G, we have $\sigma(K) = K$. Moreover, since H char K, we have $\sigma(H) = H$. Therefore, H char G.
   Consider V_4. By Exercise 3.5.8, V_4 is the unique subgroup of order 4 in A_4 so that V_4 char A_4 by Exercise 4.4.7. Moreover, A_4 is the unique subgroup of order 12 in S_4, for otherwise if $H \leq S_4$ such that $|H| = 12$, then it would contain only odd permutations, which is impossible since the product of two odd permutations is an even permutation. Therefore, A_4 char S_4 by Exercise 4.4.7. By the above result, V_4 char S_4.
   (c) Consider A_4. Then V_4 char A_4 as shown previously. Consider $H = \langle (1\,2)(3\,4) \rangle \leq V_4$. Since V_4 is abelian, then $H \trianglelefteq V_4$. However, taking $(1\,2\,3) \in A_4$, we have

$$(1\,2\,3)(1\,2)(3\,4)(3\,2\,1) = (1\,4)(2\,3) \notin H$$

   so that H is not normal in A_4. ■

(9) If r, s are the usual generators for the dihedral group D_{2n}, use the preceding two exercises to deduce that every subgroup of $\langle r \rangle$ is normal in D_{2n}.

Solution. By Exercise 3.1.34, we know $\langle r \rangle$ is normal in D_{2n}. Moreover, every subgroup of a cyclic group is characteristic, so every subgroup of $\langle r \rangle$ is characteristic in $\langle r \rangle$. Since $\langle r \rangle \trianglelefteq D_{2n}$, then by Exercise 4.4.8, every subgroup of $\langle r \rangle$ is normal in D_{2n}. ■

(10) Let G be a group, let A be an abelian normal subgroup of G, and write $\overline{G} = G/A$. Show that $\overline{G}$ acts (on the left) by conjugation on A by $\bar{g} \cdot a = gag^{-1}$, where g is any representative of the coset $\bar{g}$ (in particular, show that this action is well defined). Give an explicit example to show that this action is not well defined if A is non-abelian.

Solution. Let $\bar{g}$ and $\bar{h}$ be the same coset in $\overline{G}$. Then there exists some $a_0 \in A$ such that $h = ga_0$. Then for any $a \in A$, we have

$$\bar{g} \cdot a = gag^{-1} = gaa_0a_0^{-1}g^{-1} = ga_0a(ga_0)^{-1} = hah^{-1} = \bar{h} \cdot a$$

since A is abelian. Therefore, the action is well defined.
   Consider $G = S_3$ and $A = S_3$ itself. Then $\bar{1} = \overline{(1\,2)}$ in $\overline{G}$. However, for $a = (1\,3)$, we have $\bar{1} \cdot a = a = (1\,3)$ but, but $\overline{(1\,2)} \cdot a = (1\,2)(1\,3)(1\,2) = (2\,3) \neq a$. Therefore, the action is not well defined if A is non-abelian. ■

(11) If p is a prime and P is a subgroup of S_p of order p, prove that $N_{S_p}(P)/C_{S_p}(P) \cong \text{Aut}(P)$. (Use Exercise 4.3.34).

Solution. ■

(12) Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.

(13) Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

(14) Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.

(15) Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$, and $(\mathbb{Z}/18\mathbb{Z})^\times$.

(16) Prove that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group of order 8. (We shall see later that $(\mathbb{Z}/n\mathbb{Z})^\times$ is an elementary abelian group if and only if $n \mid 24$.)

(17) Let $G = \langle x \rangle$ be a cyclic group of order n. For $n = 2, 3, 4, 5, 6$ write out the elements of $\mathrm{Aut}(G)$ explicitly (by Proposition 16 above we know $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so for each element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, write out explicitly what the automorphism ψ_a does to the elements $\{1, x, x^2, \ldots, x^{n-1}\}$ of G).

(18) This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.

(a) Prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e. for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class $\mathcal{K}$ of G, the set $\sigma(\mathcal{K})$ is also a conjugacy class of G.

(b) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_n and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions. (See Exercise 33 in Section 3.)

(c) Prove that for each $\sigma \in \mathrm{Aut}(S_n)$,

$$\sigma : (1\,2) \mapsto (a\,b_2), \qquad \sigma : (1\,3) \mapsto (a\,b_3), \qquad \ldots, \qquad \sigma : (1\,n) \mapsto (a\,b_n),$$

for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.

(d) Show that $(1\,2), (1\,3), \ldots, (1\,n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$.

(19) This exercise shows that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| \leq 2$ (Exercise 10 in Section 6.3 shows that equality holds by exhibiting an automorphism of S_6 that is not inner).

(a) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_6 and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_6 that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$ unless $\mathcal{K}'$ is the conjugacy class of products of three disjoint transpositions. Deduce that $\mathrm{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.

(b) Prove that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| \leq 2$. (Follow the same steps as in (c) and (d) of the preceding exercise to show that any automorphism that sends transpositions to transpositions is inner.)

(20) For any finite group P let $d(P)$ be the minimum number of generators of P (so, for example, $d(P) = 1$ if and only if P is a nontrivial cyclic group and $d(Q_8) = 2$). Let $m(P)$ be the maximum of the integers $d(A)$ as A runs over all abelian subgroups of P (so, for example, $m(Q_8) = 1$ and $m(D_8) = 2$). Define

$$J(P) = \langle A \mid A \text{ is an abelian subgroup of } P \text{ with } d(A) = m(P) \rangle.$$

($J(P)$ is called the *Thompson subgroup* of P.)

(a) Prove that $J(P)$ is a characteristic subgroup of P.

(b) For each of the following groups P, list all abelian subgroups A of P that satisfy $d(A) = m(P)$: Q_8, D_8, D_{16}, and QD_{16} (where QD_{16} is the quasidihedral group of order 16 defined in Exercise 11 of Section 2.5). (Use the lattices of subgroups for these groups in Section 2.5.)

(c) Show that $J(Q_8) = Q_8$, $J(D_8) = D_8$, $J(D_{16}) = D_{16}$, and $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16}.

(d) Prove that if $Q \leq P$ and $J(P)$ is a subgroup of Q, then $J(P) = J(Q)$. Deduce that if P is a subgroup (not necessarily normal) of the finite group G and $J(P)$ is contained in some subgroup Q of P such that $Q \trianglelefteq G$, then $J(P) \trianglelefteq G$.