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

by: blanketism

Began: October 27, 2025
Last Updated: November 22, 2026

Contents

Preface **3**

Contributors **4**

0 Preliminaries **5**
0.1 Basics . . . 5
0.2 Properties of the Integers . . . 7
0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n . . . 10

1 Introduction to Groups **13**
1.1 Basic Axioms and Examples . . . 13
1.2 Dihedral Groups . . . 21
1.3 Symmetric Groups . . . 25
1.4 Matrix Groups . . . 30
1.5 The Quaternion Group . . . 35
1.6 Homomorphisms and Isomorphisms . . . 36
1.7 Group Actions . . . 43

2 Subgroups **49**
2.1 Definitions and Examples . . . 49
2.2 Centralizers and Normalizers, Stabilizers and Kernels . . . 54
2.3 Cyclic Groups and Cyclic Subgroups . . . 59
2.4 Subgroups Generated by Subsets of a Group . . . 66
2.5 The Lattice of Subgroups of a Group . . . 72

3 Quotient Groups and Homomorphisms **79**
3.1 Definitions and Examples . . . 79
3.2 More on Cosets and Lagrange's Theorem . . . 94
3.3 The Isomorphism Theorems . . . 100
3.4 Composition Series and the Hölder Program . . . 104
3.5 Transpositions and the Alternating Group . . . 109

4 Group Actions **113**
4.1 Group Actions and Permutation Representations . . . 113
4.2 Groups Acting on Themselves by Left Multiplication–Cayley's Theorem . . . 120
4.3 Groups Acting on Themselves by Conjugation–The Class Equation . . . 125
4.4 Automorphisms . . . 136
4.5 Sylow's Theorem . . . 143
4.6 The Simplicity of A_n . . . 158

5 Direct and Semidirect Products and abelian Groups **161**
5.1 Direct Products . . . 161
5.2 The Fundamental Theorem of Finitely Generated abelian Groups . . . 170
5.3 Table of Groups of Small Order . . . 177
5.4 Recognizing Direct Products . . . 178
5.5 Semidirect Products . . . 184

6 Further Topics in Group Theory **202**
6.1 p-Groups, Nilpotent Groups, and Solvable Groups 202

Preface

Please reach out through the following channels for any corrections, suggestions, or feedback regarding the manual:

- Discord Errata Server: https://discord.gg/qecQk37vfm
- Reddit: https://www.reddit.com/user/ansv9a8fdh3/
- GitHub: https://github.com/blanketism/Dummit-Foote-Solutions

This collection contains solutions to the exercises in David S. Dummit and Richard M. Foote's *Abstract Algebra*, Third Edition, a comprehensive text that has become a standard reference in the field. There have been attempts at compiling solutions to this text before, but a complete and organized one has yet to be published, and solutions to various exercises are scattered between various sources and communities. Therefore, I would like to fill that gap by writing this manual.

Because this book is covered at both the undergraduate and graduate levels due to its massive breadth, a solid foundation in number theory, linear algebra, and proof techniques is recommended for readers approaching this manual. Moreover, it is important to pace one's study carefully, as this book's gargantuan problem sets and scope can be easily overwhelming if approached hastily. Additionally, I caution readers to first attempt each exercise on their own before consultation of the solutions, as practice is essential for developing a deep understanding of abstract algebra concepts.

Each exercise is presented verbatim, along with any author hints or notes. Differently colored exercises, as seen below, indicate special exercises that I found interesting, challenging, or foundational. It is a minor gripe I have with the book that special results and important concepts are left to the exercises, so I implore readers to pay close attention to these marked exercises for better comprehension and mastery of the material.

Exercise 0.0.1

This is an example exercise environment. (Items written in parentheses typically denote notes from the author, which usually provide additional context.) [This is a hint environment, which provides assistance for the exercise.] Exercises are referenced as Exercise 0.0.1.

Manual Remark. *This is my personal remark, which typically contains reasonings for the solutions posted, or additional information for the more curious reader.*

Exercise 0.0.2: Special Exercise

This is a special exercise environment.

Despite my best efforts to provide complete and accurate solutions, errors and omissions may still exist. Please reach out through the given channels listed above should you encounter mistakes or have any suggestions for improvement.

I would like to end this with an expression of gratitude to both David S. Dummit and Richard M. Foote for a fantastic and invaluable contribution to the field of abstract algebra. I prefer analysis, but it has been a joy to engage deeply with the content throughout my construction of this manual. I'm also appreciative of the various online communities and resources that have both maintained and shared knowledge, which have proved invaluable in my studies. I hope that this manual serves its purpose in aiding you and whoever else seeks it out in their math journey.

Contributors

As of now, I am independently forming solutions to each exercise myself. However, I welcome any corrections, suggestions, or slicker solutions from others. A (growing) list of contributors will be maintained here. If you'd like to contact me, please reach out on Reddit at my profile or via Discord, where my username is blanketism. Thank you to everyone who decided to take time out of their busy lives to contribute to this project. I appreciate your help in making it better for everyone.

- greysonbowser
- coolempire93
- Civil Service Pigeon

0 Preliminaries

0.1 Basics

For Exercise 0.1.1 through Exercise 0.1.4, let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}$$

Let

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

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

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. Let X_i denote the ith matrix in the list above. Then X_1, X_3, and X_5 are M, the zero matrix, and the identity matrix respectively, so $X_1, X_3, X_5 \in \mathcal{B}$. Direct calculation shows $X_2, X_4, X_6 \notin \mathcal{B}$. ■

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. If $P, Q \in \mathcal{B}$, then $M(P+Q) = MP + MQ = PM + QM = (P+Q)M$, so $P + Q \in \mathcal{B}$. ■

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. If $P, Q \in \mathcal{B}$, then $M(PQ) = (MP)Q = (PM)Q = P(MQ) = P(QM) = (PQ)M$, so $PQ \in \mathcal{B}$. ■

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 above. Computing $MX = XM$ gives the following system of equations:

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

Thus, $r = 0$ and $p = s$, so

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

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: $1/2 = 2/4$, but $f(1/2) = 1 \neq 2 = f(2/4)$.
(b) Yes: $a/b = c/d$ implies $a^2/b^2 = c^2/d^2$, so $f(a/b) = f(c/d)$. ■

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: $1 = 1.000\ldots = 0.999\ldots$, but $f(1.000\ldots) = 0$ 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

$$a \sim b \text{ if and only if } f(a) = f(b)$$

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

Solution. That $\sim$ is an equivalence relation follows from $=$ being an equivalence relation.

The equivalence class of $a \in A$ is $\{x \in A \mid x \sim a\}$. By definition, this is $\{x \in A \mid f(x) = f(a)\}$, which is precisely the fiber of f over $f(a)$. Conversely, given $b \in B$, surjectivity of f gives $a \in A$ such that $f(a) = b$, so $f^{-1}(b) = f^{-1}(f(a))$ is the equivalence class of a under $\sim$. ■

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.

	(a,b)	$\operatorname{lcm}(a,b)$	$ax+by$
(a)	1	260	$2(20)-3(13)$
(b)	3	8556	$27(69)-5(372)$
(c)	11	19800	$8(792)-23(275)$
(d)	3	21540381	$-126(11391)+253(5673)$
(e)	1	2759487	$-105(1761)+118(1567)$
(f)	691	44693880	$-17(507885)+142(60808)$

Here, the lcm was computed using $ab = (a,b)\operatorname{lcm}(a,b)$. ■

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. Put $a = kx, b = ky$ for $x, y \in \mathbb{Z}$. Then for any $s, t \in \mathbb{Z}$,

$$as + bt = (kx)s + (ky)t = k(xs + yt),$$

so $k \mid as + bt$. ■

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. Since n is composite, put $n = ab$ with $1 < a, b < n$. 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

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

are also solutions to $ax + by = N$ (this is in fact the general solution).
Manual Remark. *Such equations are called* Diophantine equations *and are an object of study in elementary number theory.*

Solution.

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + \frac{abt}{d} - \frac{abt}{d} = N.$$

■

Exercise 0.2.5

Determine the value $\varphi(n)$ for 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. Suppose S has no minimal element, and let T be $\mathbb{Z}^+ - S$, the set of positive integers not in S. Since 1 is minimal in $\mathbb{Z}^+$, $1 \notin S$, hence $1 \in T$. Fix $k \in \mathbb{Z}^+$, and suppose every j such that $1 \leq j \leq k$ is in T. Observe $k+1 \notin S$, for otherwise it would be minimal in S, since all $j \leq k$ are in T. Then $k+1 \in T$. By induction, every positive integer is in T, contradicting that S is nonempty. Therefore, S must have a minimal element. Moreover, if $s_1, s_2 \in S$ are both minimal, then $s_1 \leq s_2$ and $s_2 \leq s_1$ imply $s_1 = s_2$. ■

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. Suppose there exist $a, b \in \mathbb{Z} - \{0\}$ such that $a^2 = pb^2$. Without loss of generality, assume $(a, b) = 1$. Then $p \mid a^2$, so $p \mid a$. Put $a = pk$ for some $k \in \mathbb{Z}$. Then

$$a^2 = p^2k^2 = pb^2 \implies b^2 = pk^2,$$

so $p \mid b^2$, hence $p \mid b$. But then $p \mid (a, b)$, contradicting $(a, b) = 1$. ■

Exercise 0.2.8: Legendre's Formula

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).

Manual Remark. *This is known as the* p-adic valuation *of* $n!$ *and is typically denoted by* $v_p(n!)$*. In particular, for any* $m \in \mathbb{Z}$, $v_p(m)$ *denotes the exponent of the largest power of* p *dividing* m*. From this definition, there are two main facts that we can use:*

(1) For any $m, n \in \mathbb{Z}$, $v_p(mn) = v_p(m) + v_p(n)$*: if* $m = p^{v_p(m)}m'$ *and* $n = p^{v_p(n)}n'$ *with* $p \nmid m'$ *and* $p \nmid n'$*, then* $mn = p^{v_p(m)+v_p(n)}m'n'$ *with* $p \nmid m'n'$ *since* p *is prime.*

(2) $p^r \mid m$ *if and only if* $r \leq v_p(m)$*: if* $m = p^{v_p(m)}m'$ *with* $p \nmid m'$*, then* $p^r \mid m$ *exactly when* $r \leq v_p(m)$*.*

Solution. In $n!$, a factor of p appears in each of the integers $p, 2p, \dots, \lfloor n/p \rfloor p$, giving $\lfloor n/p \rfloor$ factors of p. In general, an integer $m \leq n$ divisible by exactly p^k appears among the multiples of p^i for each $i = 1, \dots, k$, so it is counted exactly k times. Hence, the exponent of the largest power of p which divides $n!$ is

$$\sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

where the terms with $p^i > n$ vanish. ■

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.

Solution. See `euclidean_algorithm.py` for the solution. ■

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 $\varphi(n)$ tends to infinity as n tends to infinity.

Solution. Fix $N \in \mathbb{Z}^+$, and consider $n \in \mathbb{Z}^+$ such that $\varphi(n) = N$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n. Then

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

Since each factor $p_i^{\alpha_i - 1}(p_i - 1)$ divides N, we have $p_i - 1 \leq N$, so $p_i \leq N + 1$, bounding the number of possible primes. For the exponents, $p_i^{\alpha_i - 1} \leq N$ gives $\alpha_i \leq 1 + \log_2 N$ since $p_i \geq 2$. With finitely many choices for each p_i and α_i, there are only finitely many n with $\varphi(n) = N$.

If φ did not tend to infinity, there would exist some $M \in \mathbb{Z}^+$ such that $\varphi(n) \leq M$ for infinitely many n. But then some value $M' \leq M$ would satisfy $\varphi(n) = M'$ for infinitely many n, contradicting the above. Hence, $\varphi(n) \to \infty$ as $n \to \infty$. ■

Exercise 0.2.11

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

Solution. Let $n, d \in \mathbb{Z}^+$ with $d \mid n$. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}$, where $p_1, \ldots, p_j$ are the primes dividing d and $1 \leq \beta_i \leq \alpha_i$ for $1 \leq i \leq j$. Then

$$\frac{\varphi(n)}{\varphi(d)} = \frac{\prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)}{\prod_{i=1}^{j} p_i^{\beta_i - 1}(p_i - 1)} = \prod_{i=1}^{j} p_i^{\alpha_i - \beta_i} \prod_{i=j+1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \in \mathbb{Z}^+.$$

■

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. Note that $\bar{x} = \{x + 18k \mid k \in \mathbb{Z}\}$ for $0 \leq x \leq 17$, so

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

■

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 $m \in \mathbb{Z}$ be given. By the Division Algorithm there exist $q, r \in \mathbb{Z}$ such that

$$m = nq + r, \quad 0 \leq r < n.$$

Then $m \equiv r \pmod{n}$ so that $\bar{m} = \bar{r}$. Since $0 \leq r < n$, every equivalence class $\bar{m}$ is equal to one of $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.
To see that they are distinct, suppose $\bar{x} = \bar{y}$ for $0 \leq x, y < n$. Then $x \equiv y \pmod{n}$ so that $n \mid (x - y)$. Since $-n < x - y < n$, we must have $x - y = 0$, so that $x = y$. Hence, $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ are distinct. ■

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 $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$. (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 $10 \equiv 1 \pmod{9}$.]

Solution. By Theorem 0.3, $10 \equiv 1 \pmod{9}$ gives $10^i \equiv 1^i = 1 \pmod{9}$ for any nonnegative integer i so that each term $a_i 10^i \equiv a_i \pmod{9}$. Summing over all terms gives

$$a = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod{9}.$$

■

Exercise 0.3.4

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

Solution. By Theorem 0.3, $37 \equiv 8 \pmod{29}$ gives $37^{100} \equiv 8^{100} \pmod{29}$. Taking powers of 8 (mod 29), we compute

$$\begin{array}{lll}
8^2 \equiv 6 & 8^8 \equiv 20 & 8^{32} \equiv 7 \\
8^4 \equiv 7 & 8^{16} \equiv 23 & 8^{64} \equiv 20.
\end{array}$$

Then $8^{100} \equiv 8^{64} \cdot 8^{32} \cdot 8^4 \equiv 20 \cdot 7 \cdot 7 \equiv 23 \pmod{29}$, so the remainder when 37^{100} is divided by 29 is 23. ■

Exercise 0.3.5

Compute the last two digits of 9^{1500}.
Manual Remark. *One may also do this by considering the binomial expansion of* $(10 - 1)^{1500}$*, but we will maintain the approach of using modular arithmetic.*

Solution. Taking powers of 9 (mod 100), we have

$$9^2 \equiv 81 \pmod{100}, \quad 9^4 \equiv 61 \pmod{100}, \quad 9^8 \equiv 21 \pmod{100}.$$

Note that $9^{10} = 9^8 \cdot 9^2 \equiv 21 \cdot 81 \equiv 1 \pmod{100}$. By Theorem 0.3, $9^{1500} = (9^{10})^{150} \equiv 1^{150} \equiv 1 \pmod{100}$, so the last two digits are 01. ■

Exercise 0.3.6

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

Solution. By Exercise 0.3.2, we need only consider the integers 0, 1, 2, and 3. By Theorem 0.3, $\bar{a}^2 = \overline{a^2}$, so $0^2 \equiv 0 \pmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 0 \pmod 4$, and $3^2 \equiv 1 \pmod 4$. ■

Exercise 0.3.7

Prove 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. By Exercise 0.3.6 and Theorem 0.3, $a^2 + b^2 \equiv 0$, 1, or 2 (mod 4), so it can never be congruent to 3 (mod 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. Consider the equation (mod 4). By Exercise 0.3.7 and Exercise 0.3.6, $a^2 + b^2 \equiv 0$, 1, or 2 (mod 4), while $3c^2 \equiv 0$ or 3 (mod 4). Hence, both sides must be congruent to 0 (mod 4). Since $3c^2 \equiv 0 \pmod 4$, we have $c^2 \equiv 0 \pmod 4$, so that c is even. Since a^2 and b^2 are 0 or 1 (mod 4) by Exercise 0.3.6, $a^2 + b^2 \equiv 0 \pmod 4$ forces $a^2 \equiv b^2 \equiv 0 \pmod 4$, whence a and b are even. Divide each of a, b, and c by 2 to get a smaller solution to the original equation. Iterating this process leads to a sequence of strictly positive and decreasing integers $|c| > |c|/2 > |c|/4 > \ldots$, which is impossible. ■

Exercise 0.3.9

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

Solution. Put $a = 2k + 1$ for $k \in \mathbb{Z}$. Then $a^2 = 4k(k + 1) + 1 \equiv 1 \pmod 8$ since $k(k + 1)$ is even. ■

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. By Exercise 0.3.2, $a \mapsto \bar{a}$ is a bijection from $\{1, \ldots, n\}$ to $\mathbb{Z}/n\mathbb{Z}$, so by Proposition 0.4, $|(\mathbb{Z}/n\mathbb{Z})^\times|$ is the number of integers a with $1 \le a \le n$ such that $(a, n) = 1$, which is precisely $\varphi(n)$. ■

Exercise 0.3.11

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

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

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

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

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 $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

Solution. Let $(a, n) = d > 1$. Then $a/d, n/d \in \mathbb{Z}$. Put $b = n/d$, so that $1 \leq b < n$ and

$$ab = a(n/d) = (a/d)n \equiv 0 \pmod{n}.$$

If there existed some $c \in \mathbb{Z}$ such that $ac \equiv 1 \pmod{n}$, then $c(ab) \equiv b \pmod{n}$. However, $ab \equiv 0 \pmod{n}$, so $0 \equiv b \pmod{n}$, which is impossible since $1 \leq b < n$. ■

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 $ac \equiv 1 \pmod{n}$. [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 exist $c, x \in \mathbb{Z}$ such that $ac + nx = 1$. Then $ac \equiv 1 \pmod{n}$. ■

Exercise 0.3.14

Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ 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 $ab \equiv 1 \pmod{n}$. Since $\bar{a}$ has a representative in $\{1, \ldots, n\}$ and coprimality does not depend on the choice of representative, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $(a, n) = 1$, which proves the proposition.

For $n = 12$, note that $\bar{2} \cdot \bar{6} = \bar{3} \cdot \bar{4} = \bar{8} \cdot \bar{3} = \bar{9} \cdot \bar{4} = \overline{10} \cdot \bar{6} = \bar{0}$, so the classes $\bar{0}, \bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \overline{10}$ have no multiplicative inverse by Exercise 0.3.12. Moreover, $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$, so $\bar{1}, \bar{5}, \bar{7}, \overline{11}$ are their own multiplicative inverses. Therefore, $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$. ■

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 $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

(a) $a = 13, n = 20$.
(b) $a = 69, n = 89$.
(c) $a = 1891, n = 3797$.
(d) $a = 6003722857, n = 77695236973$. [The Euclidean Algorithm requires only 3 steps for these integers.]

Solution. We use the Euclidean Algorithm to find $x, y \in \mathbb{Z}$ such that $ax + ny = 1$ for each pair, so that $(a, n) = 1$. Then $ax \equiv 1 \pmod{n}$, and $\bar{x}$ is the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

(a) 17.
(b) 40.
(c) 253.
(d) 77695236753. ■

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. See `modular_arithmetic.py` for the solution. ■

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 $a \star b = \frac{a+b}{5}$
(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 $a \star b = \frac{a}{b}$.

Solution.
(a) Not associative: $(1 \star 0) \star 1 = 0 \neq 2 = 1 \star (0 \star 1)$.
(b) Associative.
(c) Not associative: $(1 \star 0) \star 2 = 11/25 \neq 7/25 = 1 \star (0 \star 2)$.
(d) Associative.
(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.

Solution.
(a) Not commutative: $1 \star 0 = 1 \neq 0 = 0 \star 1$.
(b) Commutative.
(c) Commutative.
(d) Commutative.
(e) Not commutative: $1 \star 2 = 1/2 \neq 2 = 2 \star 1$. ■

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 $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. By associativity of addition in $\mathbb{Z}$,

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + (\bar{b} + \bar{c}).$$ ■

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. Use the same argument as in the previous exercise, replacing $+$ with $\cdot$. ■

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. Since $0 \cdot a = 0$ for all $a \in \mathbb{Z}$, $\bar{a} \cdot \bar{0} = \bar{0}$. Since $n > 1$, $\bar{0} \neq \bar{1}$, so $\bar{0}$ does not have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. Hence, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes. ■

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) S has identity element 0, inverse element $-a/b$ for $a/b \in S$, and inherits associativity from $\mathbb{Q}$. Moreover, let $a/b, c/d \in S$. Then b and d are odd, so
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
with bd odd. Since the reduced denominator divides bd, it must also be odd. Hence, S is closed under addition, and it is a group.
(b) No: $1/2 \in S$, but $1/2 + 1/2 = 2/2 = 1/1 \notin S$.
(c) No: $1/2 \in S$, but $1/2 + 1/2 = 1 \notin S$.
(d) No: $3/2, -1 \in S$, but $3/2 + (-1) = 1/2 \notin S$.
(e) Note that $S = \{x/2 \mid x \in \mathbb{Z}\}$. Then for $\frac{a}{2}, \frac{b}{2} \in S$, we have $\frac{a}{2} + \frac{b}{2} = \frac{a+b}{2} \in S$, so S is closed under addition. Identity, inverses, and associativity are satisfied, so $(S, +)$ is a group.
(f) No: $1/3, 1/2 \in S$, but $1/3 + 1/2 = 5/6 \notin S$. ■

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. Let $x, y, z \in G$.
- Note that for any $a \in \mathbb{R}$, we have $[a] \leq a < [a] + 1$, so $0 \leq a - [a] < 1$. Applying this to $x + y$, we have $0 \leq x + y - [x + y] < 1$, so $x \star y \in G$, and $\star$ is well defined.
- Observe that $x \star y = x + y - [x + y] = y + x - [y + x] = y \star x$, so G is abelian under $\star$.
- Because $x \star 0 = x + 0 - [x + 0] = x - [x] = x$, it follows that 0 is the identity element of G under $\star$.
- Since $0 \star 0 = 0$, the inverse of 0 under $\star$ is itself. For $x \neq 0$, note that $0 < x < 1$ gives $0 < 1 - x < 1$, so $1 - x \in G$. Therefore, the inverse of x is $1 - x$, since $x \star (1 - x) = x + (1 - x) - [x + (1 - x)] = 0$.
- Note that $[\alpha + \beta] = [\alpha] + \beta$ for $\beta \in \mathbb{Z}$. Then

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

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 $1^1 = 1$, $1 \in G$. If $z \in G$, then $z^n = 1$ for some $n \in \mathbb{Z}^+$, so $z \neq 0$ and z^{-1} exists. Therefore, $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$, so $z^{-1} \in G$. Associativity from $\mathbb{C}$ is inherited by G. Finally, let $z, w \in G$ such that $z^n = w^m = 1$ for $n, m \in \mathbb{Z}^+$. 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) No; note $1, -1 \in G$, but $1 + (-1) = 0 \notin G$ since $0^n = 0 \neq 1$ for any $n \in \mathbb{Z}^+$. ■

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) For any $a + b\sqrt{2}, c + d\sqrt{2} \in G$, we have $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$, so G is closed under addition. The identity is $0 + 0\sqrt{2} = 0$, and the inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$. Associativity is inherited from $\mathbb{R}$. Hence, G is a group under addition.

(b) Suppose $a + b\sqrt{2}, c + d\sqrt{2} \in G$ are nonzero. Then $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Since a product of two nonzero reals is nonzero, $(a + b\sqrt{2})(c + d\sqrt{2})$ is nonzero. Moreover, $ac + 2bd, ad + bc \in \mathbb{Q}$, so $(a + b\sqrt{2})(c + d\sqrt{2}) \in G$. The identity is $1 + 0\sqrt{2} = 1$, and the inverse of a nonzero element $a + b\sqrt{2}$ is

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

If $a - b\sqrt{2} = 0$ and $b = 0$, then $a = 0$, contradicting that $a + b\sqrt{2}$ is nonzero. If $a - b\sqrt{2} = 0$ and $b \neq 0$, then $a = b\sqrt{2}$, contradicting that $a \in \mathbb{Q}$. Therefore, $a - b\sqrt{2} \neq 0$, so $a^2 - 2b^2 = (a - b\sqrt{2})(a + b\sqrt{2}) \neq 0$ since it is a product of two nonzero reals. Hence, the denominator is nonzero and the inverse exists in G. Since associativity is inherited from $\mathbb{R}$, the nonzero elements of G form 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 $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group. The (i, j)th and (j, i)th entries of the group table are $g_i g_j$ and $g_j g_i$, respectively. Then

$$\text{the group table is symmetric} \iff g_i g_j = g_j g_i \text{ for all } i, j \iff G \text{ is abelian.}$$ ■

Exercise 1.1.11

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

Solution.

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\lvert\bar{x}\rvert$	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 $\mathbb{Z}/36\mathbb{Z}$: $\bar{1}, \bar{2}, \bar{6}, \bar{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Solution.

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

. ■

Exercise 1.1.14

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

Solution.

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

■

Exercise 1.1.15

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

Solution. We proceed by induction on n. The base case $n = 1$ holds trivially since $(a_1)^{-1} = a_1^{-1}$. Suppose it holds for some $n \in \mathbb{Z}^+$. By Proposition 1.1(4), (5), and the inductive hypothesis, we have

$$(a_1 a_2 \cdots a_n a_{n+1})^{-1} = a_{n+1}^{-1}(a_1 a_2 \cdots a_n)^{-1} = a_{n+1}^{-1} a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}.$$

■

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.
$\boxed{\Rightarrow}$ Suppose $x^2 = 1$. Then $|x| \leq 2$. Since $|x| \in \mathbb{Z}^+$, $|x|$ is either 1 or 2.
$\boxed{\Leftarrow}$ If $|x| = 1$, then $x = 1$ and $x^2 = 1$. If $|x| = 2$, then $x^2 = 1$ by definition. ■

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 $x^n = x^{n-1}x = 1$, so $x^{n-1} = x^{-1}$. ■

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. $xy = yx \iff y^{-1}xy = y^{-1}yx = x \iff x^{-1}y^{-1}xy = x^{-1}x = 1$. ■

Exercise 1.1.19: Exponent Laws in Groups

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) By Proposition 1.1(5), both x^{a+b} and $x^a x^b$ have $a + b$ copies of x, up to bracketing, and thus $x^{a+b} = x^a x^b$. Similarly, both $(x^a)^b$ and x^{ab} have ab copies of x, up to bracketing, and thus $(x^a)^b = x^{ab}$.
(b) By Exercise 1.1.15, $(x^a)^{-1}$ consists of a instances of x^{-1}, and therefore $(x^a)^{-1} = x^{-a}$. In particular, $(x^n)^{-1} = x^{-n}$ for all $n \in \mathbb{Z}$, where $n > 0$ is the preceding argument. The case of $n = 0$ is trivial since $x^0 = 1$ and $1^{-1} = 1$, and if $n < 0$, then applying the preceding argument to $-n > 0$ and Proposition 1.1(3) gives $(x^n)^{-1} = x^{-n}$.
(c) Suppose one of a or b is 0. Then $x^{a+b} = x^a x^b$ trivially holds since $x^0 = 1$. Moreover, $(x^0)^b = 1^b = 1 = x^{0 \cdot b}$ for any integer b, and $(x^a)^0 = 1 = x^{a \cdot 0}$ for any integer a. Otherwise, consider the cases:
- If $a, b \in \mathbb{Z}^+$, then the result follows from part (a).

- If $a \in \mathbb{Z}^+$ and $b < 0$, suppose $a + b \geq 0$. Then

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

where the last equality follows from part (b). Thus, $x^{a+b} = x^a x^b$. If $a + b < 0$, applying the preceding result to $-a < 0$ and $-b \in \mathbb{Z}^+$ gives $x^{-(a+b)} = x^{-b}x^{-a}$. By part (b), taking inverses gives

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

and uniqueness of inverses gives $x^{a+b} = x^a x^b$. The case of $a < 0$ and $b \in \mathbb{Z}^+$ is analogous to the previous case with roles of a and b swapped.

For the multiplication law, if $a \in \mathbb{Z}^+$ and $b < 0$, then

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

If $a < 0$ and $b \in \mathbb{Z}^+$, then

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

- If $a < 0$ and $b < 0$, then $a + b < 0$ and

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

Moreover, $((x^{-a})^{-1})^b = (x^{-a})^{-b} = ((x^{-a})^b)^{-1}$ follows from the definition of a negative exponent, Proposition 1.1(3), and part (b). Therefore,

$$(x^a)^b = ((x^{-a})^{-1})^b = ((x^{-a})^b)^{-1} = (x^{(-a)b})^{-1} = (x^{-ab})^{-1} = x^{ab}.$$ ■

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

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

so $|x^{-1}| \leq n$. Since $(x^{-1})^{-1} = x$, applying the preceding argument to x^{-1} gives $n \leq |x^{-1}|$, and therefore $|x^{-1}| = n = |x|$. In particular, x has finite order if and only if x^{-1} has finite order, and hence x has infinite order if and only if x^{-1} has infinite order. ■

Exercise 1.1.21

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

Solution. Put $n = 2k - 1$ for $k \in \mathbb{Z}^+$. Then $x^n = x^{2k-1} = 1$, so that $x^{2k} = x$. Hence, $x = (x^2)^k$. ■

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. A simple induction on n gives $(g^{-1}xg)^n = g^{-1}x^n g$ for all $n \in \mathbb{Z}^+$. Let $|x| = m \in \mathbb{Z}^+$. Then

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

so that $|g^{-1}xg| \leq m$. Note that $x = (g^{-1})^{-1}(g^{-1}xg)g^{-1}$, so applying the preceding argument with g^{-1} in place of g and $g^{-1}xg$ in place of x gives $m \leq |g^{-1}xg|$. Therefore, $|g^{-1}xg| = m = |x|$, so x has finite order if and only if $g^{-1}xg$ has finite order, and x has infinite order if and only if $g^{-1}xg$ has infinite order.

In particular, for any $a, b \in G$, putting $x = ab$ and $g = a$ gives $|ab| = |a^{-1}(ab)a| = |ba|$. ■

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. Since $(x^s)^t = x^{st} = x^n = 1$, we have $|x^s| \leq t$. Moreover, if $(x^s)^r = 1$ for some $r \in \mathbb{Z}^+$, then $x^{sr} = 1$, so $n = st \leq sr$, hence $t \leq r$. Therefore, $|x^s| = t$. ■

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 prove the statement by induction on $n \in \mathbb{Z}^+$. The case $n = 1$ is clear since $(ab)^1 = ab = a^1 b^1$. Suppose it holds for some $n \in \mathbb{Z}^+$. Noting that $b^n a = ab^n$ by another short induction, we have

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

If $n = 0$, then $(ab)^0 = 1 = a^0 b^0$. For $n < 0$, note that $-n > 0$. By the positive case,

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

Exercise 1.1.25

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

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

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

Exercise 1.1.26: Subgroups

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 and k in H, hk and $h^{-1} \in H$. 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 $h \in H$. By assumption, $h^{-1} \in H$, so $1 = hh^{-1} \in H$, whence H contains the identity. Moreover, $\star$ is a binary operation on H since H is closed under $\star$. Associativity is inherited from G. Finally, every element of H has an inverse in H by assumption. Therefore, $(H, \star|_H)$ is a group. ■

Exercise 1.1.27: Cyclic Subgroups

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 $H = \{x^n \mid n \in \mathbb{Z}\}$. Then $1 = x^0 \in H$, so that H is nonempty. Let $x^m, x^n \in H$. Then $x^m x^n = x^{m+n} \in H$ and $(x^m)^{-1} = x^{-m} \in H$. Hence, H is closed under the binary operation on G and inverses. By Exercise 1.1.26, 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, i.e., for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$:

$$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3),$$

(b) prove that $(1, 1)$ is the identity of $A \times B$, and

(c) 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

$$\begin{aligned}[(a_1, b_1)(a_2, b_2)](a_3, b_3) &= (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) \\ &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \\ &= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) \\ &= (a_1, b_1)[(a_2, b_2)(a_3, b_3)].\end{aligned}$$

(b) For $a \in A, b \in B$, we have $(a, b)(1, 1) = (a \star 1, b \diamond 1) = (a, b) = (1 \star a, 1 \diamond b) = (1, 1)(a, b)$.
(c) $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1) = (a^{-1} \star a, b^{-1} \diamond b) = (a^{-1}, b^{-1})(a, b)$. ■

Exercise 1.1.29

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

Solution. For all $a, a' \in A$ and $b, b' \in B$, we have

$$(a, b)(a', b') = (a', b')(a, b) \iff (aa', bb') = (a'a, b'b) \iff aa' = a'a \text{ and } bb' = b'b.$$

Thus, $A \times B$ is abelian if and only if A and B are 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. Note that $(a, b)^k = (a, 1)^k(1, b)^k = (a^k, b^k)$ for all $k \in \mathbb{Z}^+$ by Exercise 1.1.24. If $|(a, b)|$ is finite, then $(a^{|(a,b)|}, b^{|(a,b)|}) = (1, 1)$, whence $|a|$ and $|b|$ are both finite. Conversely, finite $|a|$ and $|b|$ imply that $|(a, b)|$ is finite since $(a, b)^{|a||b|} = (a^{|a||b|}, b^{|a||b|}) = (1, 1)$. Therefore, $|(a, b)| = \infty$ if and only if $|a| = \infty$ or $|b| = \infty$. Now suppose $|(a, b)|$ is finite, and let $n = |(a, b)|$ and $m = \operatorname{lcm}(|a|, |b|)$. Then $(a, b)^m = (a^m, b^m) = (1, 1)$, so that $n \leq m$. Suppose $(a, b)^\ell = (1, 1)$ for some $\ell \in \mathbb{Z}^+$. By the division algorithm, write $\ell = q_1|a| + r_1$ with $0 \leq r_1 < |a|$ and $\ell = q_2|b| + r_2$ with $0 \leq r_2 < |b|$. Then

$$(a, b)^\ell = (a^{q_1|a|+r_1}, b^{q_2|b|+r_2}) = (a^{r_1}, b^{r_2}).$$

By minimality of $|a|$ and $|b|$, we must have $r_1 = r_2 = 0$, and thus ℓ is a multiple of both $|a|$ and $|b|$. Therefore, $m \mid \ell$, and since ℓ was arbitrary, setting $\ell = n$ gives $m \mid n$. Combining this with $n \leq m$, we get $n = m$. ■

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 $g \in t(G)$. Since $(g^{-1})^{-1} = g$, we have $g^{-1} \in t(G)$. We have $|\{g, g^{-1}\}| = 2$ since $g \neq g^{-1}$. If $g, h \in t(G)$ and $\{g, g^{-1}\} \cap \{h, h^{-1}\} \neq \varnothing$, then either $g = h$ or $g = h^{-1}$, in which case $\{g, g^{-1}\} = \{h, h^{-1}\}$, so the sets are either equal or disjoint. Hence, $t(G)$ can be partitioned into pairs $\{g, g^{-1}\}$, and thus has even cardinality. Since G has even order, $G - t(G)$ has even cardinality. Since $1 = 1^{-1}$, $1 \notin t(G)$, so $|G - t(G)| \geq 2$, and therefore there exists some $k \in G - t(G)$ with $k \neq 1$. For such a k, we have $k = k^{-1}$, and thus $k^2 = 1$, so $|k| = 2$. ■

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. Suppose $x^a = x^b$ for some integers $0 \leq a < b < n$. Then

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

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

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) Since $x^n = 1$, we have $x^{-i} = x^{n-i}$. Additionally, $1 \leq n - i \leq n - 1$, so odd n gives $i \neq n - i$, whence $x^i \neq x^{n-i} = x^{-i}$ by Exercise 1.1.32.
(b) Since $n = 2k$, $i \neq k$ gives $i \neq n - i$, so $x^i \neq x^{-i}$ as in part (a). If $i = k$, then $x^{-k} = x^{n-k} = x^k = x^i$. ■

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. If $x^a = x^b$ for some $a, b \in \mathbb{Z}$ such that $a < b$, then $x^{b-a} = 1$, 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 above) of G generated by x).

Solution. Let $m \in \mathbb{Z}$. By the Division Algorithm, there exist integers q and r such that $m = qn + r$ with $0 \leq r < n$. Then

$$x^m = (x^n)^q x^r = x^r.$$ ■

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, one of a, b, c has order 2 by Exercise 1.1.31. Without loss of generality, let $a^2 = 1$.

We first show that $ab = c$. Indeed, if $ab = 1$, then $b = a^{-1} = a$, contradicting that $b \neq a$. If $ab = a$, then $b = 1$, contradicting that $b \neq 1$. If $ab = b$, then $a = 1$, contradicting that $a \neq 1$. Hence, $ab = c$. By cancellation, we have $b = a^{-1}c = ac$. By symmetry, $ba = c$ and $b = ca$.

To see that $|b| = |c| = 2$, we first note that $b^2 = (ca)(ac) = c(a^2)c = c^2$. If $b^2 = b$, then $b = 1$, contradicting that $b \neq 1$. If $b^2 = c$, then $b^2 = ab$, yielding $b = a$, contradicting that $b \neq a$. If $b^2 = a$, then $b^3 = ab = c \neq 1$, contradicting that $|b| \leq 3$. Hence, $b^2 = c^2 = 1$ so that $|b| = |c| = 2$. Then $bc = (ac)c = a(c^2) = a$, and similarly, $cb = c(ca) = (c^2)a = a$. Therefore, the group table is uniquely determined 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 see that G is abelian by Exercise 1.1.10. ■

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 $sr^k \neq 1$. By the properties of D_{2n}:

$$(sr^k)^2 = s(r^k s)r^k = s(sr^{-k})r^k = r^{-k}r^k = 1$$

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 $|r| = |r^2| = 3$.
(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 $x = sr^k$ for some $0 \leq k < n$. Therefore, we have

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

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.

Solution. Since every element that is not a power of r is of the form sr^k, it follows from Exercise 1.2.1 that such elements have order 2. Therefore, $|s| = |sr| = 2$. Moreover, $r = s(sr)$, so $r, s \in \langle s, sr \rangle$, and therefore $\langle s, sr \rangle = D_{2n}$. ■

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 the elements $1, r, \ldots, r^{n-1}$ are all distinct and $0 < k < n$, we have $r^k \neq 1$. Moreover, $(r^k)^2 = r^n = 1$, hence $|r^k| = 2$. In particular, $r^k = (r^k)^{-1} = r^{-k}$. Since r^k commutes with other powers of r, consider $sr^j \in D_{2n}$ for $0 \leq j < n$. By applying Exercise 1.2.2 k times with $x = sr^j$, we have $r^k(sr^j) = (sr^j)r^{-k} = (sr^j)r^k$.

Now let $w \in D_{2n}$ such that $wx = xw$ for all $x \in D_{2n}$. If $w = r^m$ for $0 < m < n$, then commuting with s gives $w = w^{-1}$, which implies $m = k$ by Exercise 1.1.33. If $w = sr^m$ instead, then $rw = wr$. By Exercise 1.2.2 with $x = w$, we have $rw = wr^{-1}$, so $wr = wr^{-1}$, and therefore $r^2 = 1$, contradicting $|r| \geq 4$. ■

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. Let $x \in D_{2n}$ commute with all elements of D_{2n}. If $x = r^m$ for some $0 < m < n$, commuting with s gives $r^m = r^{-m}$, which cannot occur by Exercise 1.1.33. If $x = sr^m$ for some $0 \leq m < n$, commuting with r gives $rsr^m = sr^m r$, and Exercise 1.2.2 gives $rsr^m = sr^m r^{-1}$. Then $r^2 = 1$, contradicting $|r| \geq 3$, so $x = 1$. ■

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, t satisfy the same relations in G as s, r do in D_{2n}).

Solution. Since $|x| = |y| = 2$, we have $x = x^{-1}$ 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 $a = s$ and $b = sr$ of order 2 computed in Exercise 1.2.3 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. If $a^2 = b^2 = (ab)^n = 1$, put $r = ab$ 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, if $r^n = s^2 = 1$ and $rs = sr^{-1}$, put $a = s$ and $b = sr$. Then

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

The first direction shows $sr = a(ab) = b$ and the second direction shows $ab = s(sr) = r$. Therefore, with $a = s$ and $b = sr$ as in Exercise 1.2.3, the presentations $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ and $\langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$ are equivalent, and thus both present the group D_{2n}. ■

Exercise 1.2.8

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

Solution. Distinctness of the elements $1, r, r^2, \ldots, r^{n-1}$ and the fact that $r^n = 1$ show that the cyclic subgroup generated by r has order 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 the tetrahedron 1 through 4. Vertex 1 has 4 choices, and vertex 2 has 3 choices. Since symmetries are rigid motions, the positions of the remaining vertices are determined once vertices 1 and 2 are fixed, so $|G| = 4 \cdot 3 = 12$. ■

Exercise 1.2.10

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

Solution. Label the vertices of the cube 1 through 8 with vertices 1 and 2 adjacent to each other. Vertex 1 has 8 choices, and vertex 2 has 3 choices. Since symmetries are rigid motions, the positions of the remaining vertices are determined once vertices 1 and 2 are fixed, so $|G| = 8 \cdot 3 = 24$. ■

Exercise 1.2.11

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

Solution. Label the vertices of the octahedron 1 through 6 with vertices 1 and 2 adjacent to each other. Vertex 1 has 6 choices, and vertex 2 has 4 choices. Since symmetries are rigid motions, the positions of the remaining vertices are determined once vertices 1 and 2 are fixed, so $|G| = 6 \cdot 4 = 24$. ■

Exercise 1.2.12

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

Solution. Label the vertices of the dodecahedron 1 through 20 with vertices 1 and 2 adjacent to each other. Vertex 1 has 20 choices, and vertex 2 has 3 choices. Since symmetries are rigid motions, the positions of the remaining vertices are determined once vertices 1 and 2 are fixed, so $|G| = 20 \cdot 3 = 60$. ■

Exercise 1.2.13

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

Solution. Label the vertices of the icosahedron 1 through 12 with vertices 1 and 2 adjacent to each other. Vertex 1 has 12 choices, and vertex 2 has 5 choices. Since symmetries are rigid motions, the positions of the remaining vertices are determined once vertices 1 and 2 are fixed, so $|G| = 12 \cdot 5 = 60$. ■

Exercise 1.2.14

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

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

Exercise 1.2.15

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

Solution. Since $n\bar{1} = \bar{0}$, every element in $\mathbb{Z}/n\mathbb{Z}$ is of the form $k\bar{1}$ for some $0 \leq k < n$, and these are distinct by Exercise 0.3.2, so $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \mid n\bar{1} = \bar{0} \rangle$. ■

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. Since $y_1^2 = 1$, we have $y_1^{-1} = y_1$, so

$$(x_1 y_1)^2 = 1 \iff x_1 y_1 x_1 y_1 = 1 \iff x_1 y_1 x_1 = y_1^{-1} = y_1 \iff x_1 y_1 = y_1 x_1^{-1}.$$

Therefore, the relations above are equivalent to the relations of D_4 with $r = x_1$ and $s = y_1$. ■

Exercise 1.2.17

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

(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) As shown in the text, $x^3 = 1$. Assume the relations of X_{6k} hold, and put $r = x$ and $s = y$. Then

$$r^3 = x^3 = 1, \quad s^2 = y^2 = 1, \quad rs = xy = yx^2 = sr^2 = sr^{-1}.$$

Now suppose the relations of D_6 hold, and put $x = r$ and $y = s$, so

$$x^{3k} = (r^3)^k = 1, \quad y^2 = s^2 = 1, \quad xy = rs = sr^2 = yx^2.$$

Therefore, 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} and as in (a), $x^n = 1$ and $x^3 = 1$, so

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

Since $x = 1$, the only remaining relation is $y^2 = 1$, and thus $X_{2n} = \{1, y\}$ with $|X_{2n}| = 2$. ■

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

$$v^2u^3v = (v^2u^2)(uv) = (uv)(uv) = u(vu)v = u(u^2v^2)v = u^3.$$

By part (a), $v^{-1} = v^2$, so $v^{-1}u^3v = u^3$, and thus v commutes with u^3.

(c) Since $u^4 = 1$, we have $u^9 = (u^4)^2u = u$, so part (b) gives $uv = u^9v = (u^3)^3v = v(u^3)^3 = vu$.

(d) We have $uv = v^2u^2 = u^2v^2$, and cancellation gives $1 = uv$.

(e) By part (c), $u^4v^3 = u(uv)^3$, and $u(uv)^3 = u1^3 = u$ by part (d). The relations $u^4 = v^3 = 1$ then give $u = 1$, and part (d) gives $v = 1$, 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. We have $\sigma = (1\,3\,5)(2\,4)$ and $\tau = (1\,5)(2\,3)$. Then

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

■

Exercise 1.3.2

Let σ be the permutation

$$\begin{array}{lllll} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

and let τ be the permutation

$$\begin{array}{lllll} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13. \end{array}$$

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

Solution. $\sigma = (1\,13\,5\,10)(3\,15\,8)(4\,14\,11\,7\,12\,9)$ and $\tau = (1\,14)(2\,9\,15\,13\,4)(3\,10)(5\,12\,7)(8\,11)$. Then

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

■

Exercise 1.3.3

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

Solution. Orders for Exercise 1.3.1 and Exercise 1.3.2:

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

■

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
(1 2)	2
(1 3)	2
(2 3)	2
(1 2 3)	3
(1 3 2)	3

(b)

Permutation	Order	Permutation	Order	Permutation	Order	Permutation	Order
1	1	(3 4)	2	(1 4 3)	3	(1 3 4 2)	4
(1 2)	2	(1 2 3)	3	(2 3 4)	3	(1 4 2 3)	4
(1 3)	2	(1 2 4)	3	(2 4 3)	3	(1 4 3 2)	4
(1 4)	2	(1 3 2)	3	(1 2 3 4)	4	(1 2)(3 4)	2
(2 3)	2	(1 3 4)	3	(1 2 4 3)	4	(1 3)(2 4)	2
(2 4)	2	(1 4 2)	3	(1 3 2 4)	4	(1 4)(2 3)	2

■

Exercise 1.3.5

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

Solution. Let σ be the permutation in question, and note that it is a product of commuting disjoint cycles, say $\sigma = \sigma_1\sigma_2\sigma_3\sigma_4$, so $\sigma^k = \sigma_1^k\sigma_2^k\sigma_3^k\sigma_4^k$. Then $\sigma^k = 1$ if and only if each $\sigma_i^k = 1$ since the σ_i are pairwise disjoint. Such a k must be a multiple of the lengths 5, 2, 3, and 2 of the cycles σ_1, σ_2, σ_3, and σ_4, respectively, and the least such k is 30, so $|\sigma| = 30$. ■

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

Solution. For each $n \geq 2$, consider the permutation $\sigma_n = (1\ n)$. Then for $n \neq m$, $\sigma_n(1) = n \neq m = \sigma_m(1)$, so $\sigma_n \neq \sigma_m$, and hence there are infinitely many distinct permutations in S_Ω. ■

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?

Manual Remark. *The reader should notice a pattern: integers i such that $(m, i) = 1$ produce an m-cycle, while integers i such that $(m, i) = k$ produce k disjoint m/k-cycles.*

Solution.

(a) Note that $\sigma^{12} = 1$, so we only need powers of σ up to σ^{11}:

$$\begin{aligned}
\sigma^1 &= \sigma & \sigma^7 &= (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)\\
\sigma^2 &= (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12) & \sigma^8 &= (1\ 9\ 5)(2\ 10\ 6)(3\ 11\ 7)(4\ 12\ 8)\\
\sigma^3 &= (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12) & \sigma^9 &= (1\ 10\ 7\ 4)(2\ 11\ 8\ 5)(3\ 12\ 9\ 6)\\
\sigma^4 &= (1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(4\ 8\ 12) & \sigma^{10} &= (1\ 11\ 9\ 7\ 5\ 3)(2\ 12\ 10\ 8\ 6\ 4)\\
\sigma^5 &= (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8) & \sigma^{11} &= (1\ 12\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2)\\
\sigma^6 &= (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12).
\end{aligned}$$

Hence, the set of integers that produce a 12-cycle is the set $\{i \in \mathbb{Z}^+ \mid i \equiv 1, 5, 7, 11 \pmod{12}\}$.

(b) By calculations similar to part (a) with $\tau^8 = 1$, the set of integers that produce an 8-cycle is $\{i \in \mathbb{Z}^+ \mid i \equiv 1, 3, 5, 7 \pmod 8\}$.
(c) By calculations similar to part (a) with $\omega^{14} = 1$, the set of integers that produce a 14-cycle is $\{i \in \mathbb{Z}^+ \mid i \equiv 1, 3, 5, 9, 11, 13 \pmod{14}\}$. ■

Exercise 1.3.10

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

Solution. Assume all subscripts of a use the least positive residues mod m. We proceed by induction on i, where the base case $i = 1$ is clear. If $\sigma^i(a_k) = a_{k+i}$ for $1 \le i \le m - 1$, then

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

Observe that $\sigma^m(a_k) = a_{k+m} = a_k$ for all $k \in \{1, 2, \dots, m\}$. Since σ fixes all points other than the a_k's, so does σ^m, and thus $\sigma^m = 1$. Moreover, $\sigma^d(a_k) = a_{k+d} \neq a_k$ for all $1 \le d < m$ by distinctness of the a_k's, so no smaller positive power of σ is the identity, and hence $|\sigma| = m$. ■

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.
$\boxed{\Rightarrow}$ We proceed by contrapositive. Suppose $(m, i) = d > 1$, and write $i = dk$ for some $k \in \mathbb{Z}^+$. Then $(\sigma^i)^{m/d} = \sigma^{dk \cdot m/d} = \sigma^{km} = 1$. Hence, $|\sigma^i| \le m/d < m$, so σ^i is not an m-cycle by Exercise 1.3.10.
$\boxed{\Leftarrow}$ Suppose that $(m, i) = 1$. Since $\sigma^m = 1$, we only need to consider i such that $1 \le i \le m - 1$. Let $\overline{n}$ denote the integer in $\{1, \dots, m\}$ such that $\overline{n} \equiv n \pmod m$. We claim that the integers

$$\overline{1}, \overline{1+i}, \overline{1+2i}, \dots, \overline{1+(m-1)i}$$

are all distinct. Indeed, if $\overline{1+xi} = \overline{1+yi}$ for some $0 \le x, y \le m - 1$, then $i(x - y) \equiv 0 \pmod m$. Because $(m, i) = 1$, we have $m \mid (x - y)$, and since $0 \le x, y \le m - 1$, it follows that $x - y = 0$, so $x = y$. By Exercise 1.3.10, $\sigma^i(\overline{1+xi}) = \overline{1+(x+1)i}$ for $0 \le x \le m - 1$. Since $\overline{1+mi} = \overline{1}$, and the integers $\overline{1}, \overline{1+i}, \dots, \overline{1+(m-1)i}$ are all distinct, the cycle decomposition of σ^i is

$$\sigma^i = (\overline{1}\ \overline{1+i}\ \overline{1+2i}\ \dots \overline{1+(m-1)i}),$$

which 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 a n-cycle σ ($n \ge 10$) with $\tau = \sigma^k$ for some integer k.
(b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n-cycle σ ($n \ge 5$) with $\tau = \sigma^k$ for some integer k.

Manual Remark. *Part (a) can be done systematically once we have access to Lagrange's Theorem.*

Solution.
(a) Put $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10)$. Then $\sigma^5 = \tau$, so there exists a 10-cycle σ such that $\tau = \sigma^k$ for $k = 5$.
(b) Assume for contradiction that there exist an n-cycle σ and an integer k such that $\sigma^k = \tau$. Then $\tau^2(1) = 1$ and $\tau^3(3) = 3$, so $\sigma^{2k}(1) = 1$ and $\sigma^{3k}(3) = 3$. Equivalently, $2k \equiv 0 \pmod n$ and $3k \equiv 0 \pmod n$ by Exercise 1.3.10. Then $n \mid (3k - 2k) = k$, which implies $\sigma^k = 1$, contradicting the assumption that $\sigma^k = \tau \neq 1$. Therefore, no such n-cycle σ exists. ■

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.
$\boxed{\Rightarrow}$ Let $\sigma \in S_n$ with $|\sigma| = 2$. Let $(a_1\ a_2\ \dots\ a_m)$ be one of the cycles in its cycle decomposition. Since $\sigma^2 = 1$, we have $\sigma(a_1) = a_2$ and $\sigma(a_2) = \sigma^2(a_1) = a_1$. If $m \geq 3$, then $\sigma(a_2) = a_3 \neq a_1$, contradicting $\sigma^2 = 1$, so $m = 2$. Therefore, every cycle in the cycle decomposition of σ is a 2-cycle, and since disjoint cycles commute, σ is a product of commuting 2-cycles.
$\boxed{\Leftarrow}$ Suppose σ's cycle decomposition is a product of commuting 2-cycles $(a_1\ b_1)(a_2\ b_2)\cdots(a_k\ b_k)$. Since each 2-cycle has order 2, and the 2-cycles commute, $\sigma^2 = 1$. Because $\sigma(a_1) = b_1 \neq a_1$, we have $\sigma \neq 1$, so $|\sigma| = 2$. ∎

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.
$\boxed{\Rightarrow}$ Let $\sigma \in S_n$ with $|\sigma| = p$. Let $(a_1\ a_2\ \dots\ a_m)$ be one of the cycles in its cycle decomposition, where $m \geq 2$ since 1-cycles are omitted from the decomposition. By Exercise 1.3.10, we know $\sigma^i(a_1) = a_{1+i}$ where $1 + i$ is replaced by the least positive residue modulo m when $1 + i > m$. Because $\sigma^p = 1$, we have $\sigma^p(a_1) = a_1$, and by distinctness of the a_k's, we must have $m \mid p$. Since p is prime, $m = p$, hence any cycle in the cycle decomposition of σ is a p-cycle. Moreover, each p-cycle in the decomposition is disjoint from the others, so they commute.
$\boxed{\Leftarrow}$ Let $\sigma = \tau_1\tau_2\cdots\tau_k$ be the cycle decomposition of σ, where each τ_i is a p-cycle. Since the cycles are disjoint, they commute. By Exercise 1.3.10, $\sigma^t(x) = \tau_1^t(x) \neq x$ for any x moved by τ_1 and t such that $1 \leq t < p$. Therefore, $\sigma^t \neq 1$ for all $1 \leq t < p$, and because $\tau_i^p = 1$ for all i, we have $\sigma^p = 1$, and hence $|\sigma| = p$.

For a counterexample when p is not prime, consider $\sigma = (1\,2\,3)(4\,5)$ in S_5. Then $\sigma^t = (1\,2\,3)^t(4\,5)^t \neq 1$ for all $1 \leq t \leq 5$, but $\sigma^6 = 1$, so $|\sigma| = 6$, even though σ contains no 6-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. [Use Exercise 1.3.10 and Exercise 1.1.24.]

Solution. Let $\sigma \in S_n$ have cycle decomposition $\tau_1\tau_2\cdots\tau_k$, where each τ_i is a cycle of length m_i. For any $t \geq 1$,

$$\sigma^t = 1 \iff \tau_i^t = 1 \text{ for all } i \iff m_i \mid t \text{ for all } i \iff \operatorname{lcm}(m_1, \dots, m_k) \mid t,$$

where the first equivalence follows from disjointness of the cycles and commutativity of disjoint cycles; the second equivalence is Exercise 1.3.10; and the third equivalence is by the definition of the least common multiple. Therefore, $|\sigma|$ is the least $t \geq 1$ for which $\sigma^t = 1$, which is precisely $\operatorname{lcm}(m_1, \dots, m_k)$. ∎

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. If $m = 1$, then any single element forms a 1-cycle, and there are n such 1-cycles. Let $m \geq 2$. There are $n(n-1)(n-2)\cdots(n-m+1)$ ways to choose m distinct integers from $\{1, \dots, n\}$ and arrange them in a sequence. For a given sequence $a_1, \dots, a_m$, a cycle $(a_1\ \dots a_m)$ has m equivalent representations, corresponding to the m choices for the starting element of the cycle, which then determines the order of the remaining elements. Therefore, the number of distinct m-cycles is

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

∎

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. By Exercise 1.3.16, the first 2-cycle has $\frac{n(n-1)}{2}$ choices, and the second 2-cycle has $\frac{(n-2)(n-3)}{2}$ choices. Since these 2-cycles are disjoint, there are 2 representations for the same permutation corresponding to the order in which we choose the two 2-cycles, and the permutation determines the cycles up to this order. Therefore, the number of permutations which are the product of two disjoint 2-cycles is

$$\frac{\frac{n(n-1)}{2} \cdot \frac{(n-2)(n-3)}{2}}{2} = \frac{n(n-1)(n-2)(n-3)}{8}.$$

■

Exercise 1.3.18

Find all numbers n such that S_5 contains an element of order n. [Use Exercise 1.3.15.]

Solution. S_5 contains n-cycles for $n = 1, 2, 3, 4$, and 5. We can also have a product of disjoint 2- and 3-cycles, which has order 6 by Exercise 1.3.15. The remaining elements of S_5 are products of disjoint cycles whose lengths sum to at most 5, namely the product of two disjoint 2-cycles, which has order 2. Therefore, the numbers n such that S_5 contains an element of order n are 1, 2, 3, 4, 5, and 6. ■

Exercise 1.3.19

Find all numbers n such that S_7 contains an element of order n. [Use Exercise 1.3.15.]

Solution. S_7 contains n-cycles for $n = 1, 2, 3, 4, 5, 6$, and 7. We can also have the products of disjoint 2- and 5-cycles and disjoint 3- and 4-cycles, which have orders 10 and 12 respectively by Exercise 1.3.15. The remaining elements of S_7 are products of disjoint cycles whose lengths sum to at most 7, namely $2+2$, $2+3$, $2+4$, $2+2+2$, $2+2+3$, and $3+3$. The orders of these products are 2, 6, 4, 2, 6, and 3 respectively. Therefore, the numbers n such that S_7 contains an element of order n are 1, 2, 3, 4, 5, 6, 7, 10, and 12. ■

Exercise 1.3.20

Find a set of generators and relations for S_3.

Solution. Let $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$. Direct computation gives $\sigma^3 = \tau^2 = 1$ and $\sigma\tau = (1\ 3) = \tau\sigma^{-1}$. The elements $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ are all distinct and account for all six elements of S_3, so σ and τ generate S_3.

Let $G = \langle \alpha, \beta \mid \alpha^3 = \beta^2 = 1, \alpha\beta = \beta\alpha^{-1} \rangle$. By induction on i, we have $\alpha^i\beta = \beta\alpha^{-i}$ for $i = 0, 1, 2$. Therefore, every element of G is of the form α^i or $\beta\alpha^i$ for $i = 0, 1, 2$, and hence $|G| \leq 6$. Since S_3 has six elements and is generated by σ and τ satisfying the same relations, we must have

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle.$$

■

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. The first column of a matrix in $\mathrm{GL}_2(\mathbb{F}_2)$ cannot be the zero vector, so there are $2^2 - 1 = 3$ choices for the first column. The second column cannot lie in the span of the first column, so there are $2^2 - 2 = 2$ choices for the second column, and therefore $|\mathrm{GL}_2(\mathbb{F}_2)| = 3 \cdot 2 = 6$. ■

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 calculation, 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. The following two matrices do not commute:

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

Therefore, $\mathrm{GL}_2(\mathbb{F}_2)$ 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. If $n = 1$, then $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$ is not a field, since $\mathbb{Z}/1\mathbb{Z} - \{\bar{0}\} = \varnothing$ is not a group under multiplication. Otherwise, suppose n is composite. Then there exists $a \in \mathbb{Z}^+$ such that $1 < a < n$ and $a \mid n$, so $\bar{a} \neq \bar{0}$. In particular, $(a, n) \neq 1$, so Proposition 0.4 gives $\bar{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times$, and hence $\mathbb{Z}/n\mathbb{Z}$ 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.
$\boxed{\Rightarrow}$ If $\mathrm{GL}_n(F)$ is finite, the subset $\{\alpha I \mid \alpha \in F^\times\}$ must also be finite, which implies that F has a finite number of elements.
$\boxed{\Leftarrow}$ Suppose $|F| = q$. Each $n \times n$ matrix over F has n^2 entries, and each entry has q possible values, so there are q^{n^2} total $n \times n$ matrices over F. Since $\mathrm{GL}_n(F)$ is a subset of the set of all $n \times n$ matrices over F, it follows that $\mathrm{GL}_n(F)$ is finite. ■

Exercise 1.4.6

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

Solution. See $\boxed{\Leftarrow}$ in Exercise 1.4.5, and note that the zero matrix is not invertible, so the inequality is strict. ■

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. There are p^4 total 2×2 matrices over $\mathbb{F}_p$. Consider the cases for the first row of a noninvertible matrix:

- If the first row is $(0, 0)$, then there are p^2 choices for the second row.
- There are $p^2 - 1$ nonzero choices for the first row (a, b). The second row must be some $c(a, b)$ for $c \in \mathbb{F}_p$, giving p choices.

Then the number of noninvertible matrices is $p^2 + p(p^2 - 1) = p^3 + p^2 - p$. Subtracting from the total number of matrices, we get $p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p$. ■

Exercise 1.4.8

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

Solution. Consider the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A' = \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}, \quad B' = \begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}.$$

Note that $\det A = \det A' = \det B = \det B' = 1$, so $A', B' \in \mathrm{GL}_n(F)$. Moreover, $(AB)_{11} = 2 \neq 1 = (BA)_{11}$, so $AB \neq BA$, whence $A'B' \neq B'A'$ and $\mathrm{GL}_n(F)$ is non-abelian. ■

Exercise 1.4.9

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

Solution.

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\begin{pmatrix} i & j \\ k & \ell \end{pmatrix} &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}\begin{pmatrix} i & j \\ k & \ell \end{pmatrix} \\
&= \begin{pmatrix} (ae + bg)i + (af + bh)k & (ae + bg)j + (af + bh)\ell \\ (ce + dg)i + (cf + dh)k & (ce + dg)j + (cf + dh)\ell \end{pmatrix} \\
&= \begin{pmatrix} a(ei + fk) + b(gi + hk) & a(ej + f\ell) + b(gi + hk) \\ c(ei + fk) + d(gi + hk) & c(ej + f\ell) + d(gi + hk) \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei + fk & ej + f\ell \\ gi + hk & gj + h\ell \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & \ell \end{pmatrix}\right).
\end{aligned}$$

■

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

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \text{ and } \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$$

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)

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

Since $a_i \neq 0$ and $c_i \neq 0$, $a_1 a_2 \neq 0$ and $c_1 c_2 \neq 0$ so that G is closed under matrix multiplication.

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

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

Because $a \neq 0$ and $c \neq 0$, $\frac{1}{a}$ and $\frac{1}{c}$ exist and are nonzero, so the inverse matrix is also in G.

(c) For any $A \in G$, $\det A = A_{11} A_{22} \neq 0$ by assumption, so $A \in \mathrm{GL}_2(\mathbb{R})$. Since $I_2 \in G$ and G is closed under matrix multiplication and inverses, it follows that G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

(d) Let $H = \{X \in G \mid X_{11} = X_{22}\}$. Setting $a_i = c_i$ for $i = 1, 2$ in part (a) gives diagonal entries $a_1 a_2$ and $a_1 a_2$, showing that the product of two elements of H is again in H. Similarly, setting $a = c$ in part (b) yields diagonal entries $\frac{1}{a}$ and $\frac{1}{a}$, showing that the inverse of an element of H is again in H. Since $I_2 \in H$, it follows that H is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. ■

The next exercise introduces the **Heisenberg group** over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally — for example, with entries in $\mathbb{Z}$.

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 element of the group $H(\mathbb{R})$ has infinite order.

Manual Remark. *The choice of rewriting the matrix as a tuple is simply a time saver/ease of notation for the sake of computation. However, it does allow one to encode $H(F)$ in terms of the field operations.*

Solution.

(a) Calculating the product, we have

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

For ease of notation, we may start representing matrices as 3-tuples, so $X = (a, b, c)$, $Y = (d, e, f)$, and $XY = (a + d, af + b + e, c + f)$.

Consider $A = (1, 0, 0)$ and $B = (0, 0, 1)$. Then $AB = (1, 1, 1) \neq (1, 0, 1) = BA$, so $H(F)$ is non-abelian.

(b) Suppose $(a, b, c)(x, y, z) = (0, 0, 0) = I_3$. Then $(a + x, az + b + y, c + z) = (0, 0, 0)$ implies $x = -a$, $y = -b + ac$, and $z = -c$. Moreover, $(x, y, z)(a, b, c) = (0, 0, 0)$, so

$$X^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = (-a, -b + ac, -c),$$

and thus $H(F)$ is closed under inverses.

(c) For each $(s, t, u) \in H(F)$, there are $|F|$ choices for each of s, t, and u, so $|H(F)| = |F|^3$. Now let $(g, h, i) \in H(F)$. Then we have

$$\begin{aligned} ((a, b, c)(d, e, f))(g, h, i) &= (a + d, af + b + e, c + f)(g, h, i) \\ &= (a + d + g, (a + d)i + af + b + e + h, c + f + i) \\ &= (a + d + g, ai + di + af + b + e + h, c + f + i) \\ &= (a, b, c)(d + g, di + e + h, f + i) \\ &= (a, b, c)((d, e, f)(g, h, i)), \end{aligned}$$

so matrix multiplication in $H(F)$ is associative. Since closure under matrix multiplication holds by part (a), $H(F)$ contains the identity $(0, 0, 0) = I_3$, and is closed under inverses by part (b), it follows that $H(F)$ is a group under matrix multiplication.

(d) The elements of $H(\mathbb{Z}/2\mathbb{Z})$ are

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

Since $(a, b, c)^2 = (2a, 2b + ac, 2c) = (0, ac, 0)$ in $\mathbb{Z}/2\mathbb{Z}$, we have two cases:

- If $ac = 0$, then $(a, b, c)^2 = (0, 0, 0)$, so these elements have order 1 or 2.
- If $ac = 1$, then $(a, b, c)^2 = (0, 1, 0)$, so $(a, b, c)^4 = (0, 0, 0)$, and these elements have order 4.

(e) Let $X \in H(\mathbb{R})$ be nonidentity. It is easy to see by induction that

$$X^n = (na, n(n-1)ac/2 + nb, nc).$$

Since $X \neq I_3$, at least one of a, b, c is nonzero. It is clear that $a \neq 0$ or $c \neq 0$ implies $X^n \neq I_3$. Now suppose $a = c = 0$ and $b \neq 0$. Then $X^n = (0, nb, 0)$. Since $b \neq 0$, $nb \neq 0$ for all $n \in \mathbb{Z}^+$. Hence, $X^n \neq I_3$ for all $n \in \mathbb{Z}^+$. 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.
Manual Remark. *Tedious, but straightforward.*

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	$(1\,3\,2)$	$(1\,2\,3)$	$(2\,3)$	$(1\,3)$
$(1\,3)$	$(1\,3)$	$(1\,2\,3)$	1	$(1\,3\,2)$	$(1\,2)$	$(2\,3)$
$(2\,3)$	$(2\,3)$	$(1\,3\,2)$	$(1\,2\,3)$	1	$(1\,3)$	$(1\,2)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3)$	$(2\,3)$	$(1\,2)$	$(1\,3\,2)$	1
$(1\,3\,2)$	$(1\,3\,2)$	$(2\,3)$	$(1\,2)$	$(1\,3)$	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.
Manual Remark. *One may notice I dropped k. Since $k = ij$, it is not necessary to include k as a generator.*

Solution. $\langle i, j \mid i^4 = 1, i^2 = j^2 = (ij)^2 \rangle$. ■

1.6 Homomorphisms and Isomorphisms

Let G and H be groups.

Exercise 1.6.1

Let $\varphi\colon G \to H$ 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) Fix $x \in G$. We proceed by induction on n, where the base case $n = 1$ is trivial. Suppose the result holds for some $n \in \mathbb{Z}^+$, so $\varphi(x^n) = \varphi(x)^n$. We then have

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

(b) Let 1_G and 1_H denote the identity elements of G and H, respectively. We have $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)^2$, so Proposition 1.2 gives $\varphi(1_G) = 1_H$. Thus, for any $x \in G$, we have

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

and left multiplying by $\varphi(x)^{-1}$ gives $\varphi(x)^{-1} = \varphi(x^{-1})$. For $n = 0$, we have $\varphi(x^0) = \varphi(1_G) = 1_H = \varphi(x)^0$. Then for any $n < 0$, we use part (a) with $-n$ to yield

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

Exercise 1.6.2

If $\varphi\colon G \to H$ 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 $x \in G$ and $k \in \mathbb{Z}^+$. By Exercise 1.6.1 and injectivity of φ,

$$x^k = 1_G \iff \varphi(x)^k = \varphi(x^k) = 1_H.$$

Then x and $\varphi(x)$ have the same set of positive integers k such that $x^k = 1_G$ and $\varphi(x)^k = 1_H$, respectively, and thus $|x| = |\varphi(x)|$. Consequently, the restriction $\varphi|_S$, where $S = \{g \in G \mid |g| = n\}$, is a bijection onto $\{h \in H \mid |h| = n\}$, so the number of elements of order n in G and H is the same.

The result is not true if φ is only assumed to be a homomorphism. Consider $\varphi\colon G \to 1$ for some nontrivial group G. Then any nonidentity $x \in G$ has order greater than 1, but $\varphi(x) = 1$ has order 1. ■

Exercise 1.6.3

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

Solution.

$\boxed{\Rightarrow}$ Suppose that G is abelian. Given $h_1, h_2 \in H$, there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. 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.

$\boxed{\Leftarrow}$ Suppose that H is abelian. Then for any $g_1, g_2 \in G$, we have

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1) = \varphi(g_2g_1),$$

and injectivity of φ implies $g_1g_2 = g_2g_1$, so G is abelian.

Let $\varphi\colon G \to H$ be a homomorphism. In the $\boxed{\Rightarrow}$ direction, observe that the only additional property of φ used was its surjectivity, so it is sufficient for φ to be surjective. ■

Exercise 1.6.4

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

Solution. By Exercise 1.6.2, isomorphisms preserve the number of elements of each order. The element $i \in \mathbb{C} - \{0\}$ has order 4, and if $x \in \mathbb{R} - \{0\}$ is such that $x^4 = 1$, then $x = \pm 1$, which has order 1 or 2. ■

Exercise 1.6.5

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

Solution. $\mathbb{R}$ is uncountable, while $\mathbb{Q}$ is countable, so no such isomorphism can exist. ■

Exercise 1.6.6

Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.
Manual Remark. *In fact, no nontrivial homomorphism exists from $\mathbb{Q}$ to $\mathbb{Z}$.*

Solution. Suppose that $\varphi\colon \mathbb{Q} \to \mathbb{Z}$ is an isomorphism. Because $\varphi(0) = 0$ by Exercise 1.6.1, injectivity of φ gives $r = \varphi(1) \neq 0$. Fix $n > |r|$. By Exercise 1.6.1(a) in additive notation, we have

$$r = \varphi(1) = \varphi\left(n \cdot \frac{1}{n}\right) = n\varphi\left(\frac{1}{n}\right),$$

and thus $\varphi(\frac{1}{n}) = \frac{r}{n} \in \mathbb{Z}$, contradicting the choice of n. ■

Exercise 1.6.7

Prove that D_8 and Q_8 are not isomorphic.

Solution. The tables in Exercise 1.2.1 and Exercise 1.5.1 give 2 elements of order 4 in D_8 and 6 elements of order 4 in Q_8, so they cannot be isomorphic by Exercise 1.6.2. ■

Exercise 1.6.8

Prove that if $n \neq m$, 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. By Exercise 1.3.15, S_4 has no elements of order 12, while $r \in D_{24}$ has order 12, and thus they cannot be isomorphic by Exercise 1.6.2. ■

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 $\theta\colon \Delta \to \Omega$ be a bijection. Define

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

and prove the following:
(a) 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) φ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ.]
(c) 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) The map $\theta \circ \sigma \circ \theta^{-1}$ is a composition of bijections that takes $\Omega \to \Delta \to \Delta \to \Omega$, and hence is a permutation of Ω, so φ is well defined.

(b) Define the mapping

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

The map $\theta^{-1} \circ \tau \circ \theta$ is a composition of bijections that takes $\Delta \to \Omega \to \Omega \to \Delta$, and hence is a permutation of Δ, so ψ is well defined. For any $\sigma \in S_\Delta$, we have

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

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

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

wherefore 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

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

Therefore, φ is a homomorphism, whence it is an isomorphism, so $S_\Delta \cong S_\Omega$. ■

Exercise 1.6.11

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

Solution. Consider the map $\varphi \colon A \times B \to B \times A$ given by

$$\varphi((a, b)) = (b, a) \quad \text{for all } a \in A, b \in B.$$

The map $(b, a) \mapsto (a, b)$ is the two-sided inverse of φ, so φ is bijective. Moreover, for all $(a_1, b_1), (a_2, b_2) \in A \times B$, we have

$$\varphi((a_1, b_1)(a_2, b_2)) = \varphi((a_1 a_2, b_1 b_2)) = (b_1 b_2, a_1 a_2) = (b_1, a_1)(b_2, a_2) = \varphi((a_1, b_1))\varphi((a_2, b_2)).$$

Therefore, φ is a homomorphism, and hence an isomorphism, so $A \times B \cong B \times A$. ■

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 map $\varphi \colon G \times C \to A \times H$ given by

$$\varphi(((a, b), c)) = (a, (b, c)) \quad \text{for all } a \in A, b \in B, c \in C.$$

The map $(a, (b, c)) \mapsto ((a, b), c)$ is the two-sided inverse of φ, so φ is bijective. As in Exercise 1.6.11, φ is a homomorphism, and hence an isomorphism, so $G \times C \cong A \times H$. ■

Exercise 1.6.13: Image

Let G and H be groups and let $\varphi \colon G \to H$ 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. Let $g_1, g_2 \in G$. By Exercise 1.6.1(b), $\varphi(1_G) = 1_H$, so $1_H \in \varphi(G)$, and

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \in \varphi(G), \quad \varphi(g_1^{-1}) = \varphi(g_1)^{-1} \in \varphi(G),$$

showing that $\varphi(G)$ is a subgroup of H.

Now suppose φ is injective. The map $\psi \colon G \to \varphi(G)$ defined by $g \mapsto \varphi(g)$ is injective since φ is injective, surjective by definition of $\varphi(G)$, and a homomorphism since φ is a homomorphism, so $G \cong \varphi(G)$. ■

Exercise 1.6.14: Kernel

Let G and H be groups and let $\varphi\colon G \to H$ 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 (cf. Exercise 1.1.26) of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Solution. Denote the kernel of φ by $\ker\varphi$. By Exercise 1.6.1(b), $\varphi(1_G) = 1_H$, so $1_G \in \ker\varphi$, and for $g_1, g_2 \in \ker\varphi$, we have

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

so $g_1g_2, g_1^{-1} \in \ker\varphi$, and thus $\ker\varphi$ is a subgroup of G.
$\boxed{\Rightarrow}$ Suppose φ is injective, and let $g \in \ker\varphi$. By definition, $\varphi(g) = 1_H = \varphi(1_G)$, and injectivity of φ gives $g = 1_G$, so $\ker\varphi = 1$.
$\boxed{\Leftarrow}$ Suppose $\ker\varphi = 1$, and let $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$. By Exercise 1.6.1(b), we have

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

so $g_1g_2^{-1} \in \ker\varphi$. Then $g_1g_2^{-1} = 1_G$, so $g_1 = g_2$, and hence φ is injective. ■

Exercise 1.6.15

Define a map $\pi\colon \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x,y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 1.6.14).

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

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

Exercise 1.6.16

Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1\colon G \to A$ and $\pi_2\colon G \to B$ defined by $\pi_1((a,b)) = a$ and $\pi_2((a,b)) = b$ are homomorphisms and find their kernels (cf. Exercise 1.6.14).

Solution. As in Exercise 1.6.15, π_1 and π_2 are homomorphisms. Moreover, $(a,b) \in \ker\pi_1$ if and only if $\pi_1((a,b)) = a = 1_A$, and $(a,b) \in \ker\pi_2$ if and only if $\pi_2((a,b)) = b = 1_B$. Therefore,

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

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. Let $\varphi\colon G \to G$ be defined by $\varphi(g) = g^{-1}$.
$\boxed{\Rightarrow}$ Suppose φ is a homomorphism. Then for $g, h \in G$, we have

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

so G is abelian.
$\boxed{\Leftarrow}$ 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. Let $\varphi : G \to G$ be defined by $\varphi(g) = g^2$. Then for all $g, h \in G$, we have

$$\varphi(gh) = \varphi(g)\varphi(h) \iff (gh)^2 = g^2h^2 \iff hg = gh.$$

■

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. Define the map $\varphi : G \to G$ by $\varphi(z) = z^k$. Since $G \subseteq \mathbb{C}$, G is abelian, so for any $z, w \in G$,

$$\varphi(zw) = (zw)^k = z^k w^k = \varphi(z)\varphi(w),$$

and hence φ is a homomorphism. To show surjectivity, let $w \in G$ with $w^n = 1$ for some $n \in \mathbb{Z}^+$. Then there exists $z \in \mathbb{C}$ such that $z^k = w$, so $z^{nk} = (z^k)^n = w^n = 1$ and hence $z \in G$. Moreover, $\varphi(z) = z^k = w$, so φ is surjective. Finally, $u = e^{2\pi i/k} \in G$ is such that $\varphi(u) = u^k = 1$ with $u \neq 1$ since $k > 1$, so φ is not injective, and therefore not an isomorphism. ■

Exercise 1.6.20: The Automorphism Group

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. Recall that function composition is associative. Observe that $\mathrm{Aut}(G)$ contains the identity map $1 : G \to G$ defined by $1(g) = g$ for all $g \in G$. For any $\varphi, \psi \in \mathrm{Aut}(G)$ and $g, h \in G$, we have

$$(\varphi \circ \psi)(gh) = \varphi(\psi(gh)) = \varphi(\psi(g)\psi(h)) = \varphi(\psi(g))\varphi(\psi(h)) = (\varphi \circ \psi)(g)(\varphi \circ \psi)(h),$$

so $\varphi \circ \psi$ is a bijective homomorphism, and hence $\mathrm{Aut}(G)$ is closed under composition. Finally, for any $\varphi \in \mathrm{Aut}(G)$, φ^{-1} exists and is also a bijection. Then for any $g, h \in G$, we have

$$\varphi^{-1}(gh) = \varphi^{-1}(\varphi(\varphi^{-1}(g))\varphi(\varphi^{-1}(h))) = \varphi^{-1}(\varphi(\varphi^{-1}(g)\varphi^{-1}(h))) = \varphi^{-1}(g)\varphi^{-1}(h),$$

so φ^{-1} is a homomorphism, and $\varphi^{-1} \in \mathrm{Aut}(G)$. Therefore, $(\mathrm{Aut}(G), \circ)$ is a group. ■

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 $\mathbb{Q}$ (cf. Exercise 1.6.20).

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

$$\varphi(p + q) = k(p + q) = kp + kq = \varphi(p) + \varphi(q),$$

so that φ is a homomorphism. The map $q \mapsto \frac{q}{k}$ is the two-sided inverse of φ, so $\varphi \in \mathrm{Aut}(\mathbb{Q})$. ■

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

$$\varphi(a_1a_2) = (a_1a_2)^k = a_1^k a_2^k = \varphi(a_1)\varphi(a_2),$$

and thus φ is a homomorphism. If $k = -1$, then $\varphi \circ \varphi = 1$, so $\varphi = \varphi^{-1}$, and hence $\varphi \in \mathrm{Aut}(A)$. ■

Exercise 1.6.23

Let G be a finite group which possesses an automorphism σ (cf. Exercise 1.6.20) 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. Define the map $\varphi\colon G \to G$ by

$$\varphi(x) = x^{-1}\sigma(x) \quad \text{for all } x \in G.$$

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

For any $g \in G$, there exists $x \in G$ such that $g = x^{-1}\sigma(x)$. Applying σ to both sides, we have

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

By Exercise 1.6.17, 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 $n = |xy|$. [See Exercise 1.2.6.]

Solution. Observe that G must contain the distinct elements 1, x, and y. Put $t = xy$, and note that $x \neq y$ gives $t \neq 1$, so $n \geq 2$. Note that $t^n = (xy)^n = 1$, $x^2 = 1$, and $txt = (xy)x(xy) = xyy = x$, so $tx = xt^{-1}$. Moreover, $y = xt$, so $G = \langle x, t\rangle$. Then the map $r \mapsto t$ and $s \mapsto x$ extends to a surjective homomorphism $\varphi\colon D_{2n} \to G$.

Now, Exercise 1.1.32 gives that $1, t, \ldots, t^{n-1}$ are all distinct elements of G. If $xt^j = xt^k$ for some $0 \leq j, k \leq n-1$ such that $j \neq k$, then left cancelling by x gives $t^j = t^k$, contradicting the distinctness of $1, t, \ldots, t^{n-1}$, so the elements $x, xt, \ldots, xt^{n-1}$ are also distinct. If $x \in \langle t\rangle$, then x must commute with t, so $xt = tx = xt^{-1}$. This yields $t^2 = 1$, so $y = xt \in \langle t\rangle$ as well, and therefore $G = \langle t\rangle$. But then G would have at most 2 elements, contradicting the fact that 1, x, and y are distinct elements of G. Therefore, no $xt^j \in \langle t\rangle$, for otherwise $x \in \langle t\rangle$, so all the elements $1, t, \ldots, t^{n-1}, x, xt, \ldots, xt^{n-1}$ are distinct. Thus, $|G| = 2n$ and $G \cong D_{2n}$. ■

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 $\varphi\colon D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ 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 in part (b) is injective.

Solution.

(a) Let $\mathbb{R}^2$ be spanned by the standard basis vectors $\mathbf{e}_1 = (1 \quad 0)^t$ and $\mathbf{e}_2 = (0 \quad 1)^t$ and 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 $\mathbf{e}_1$ and $\mathbf{e}_2$ is exactly the desired rotation matrix.

(b) By induction on k, $\varphi(r)^k$ is given by

$$\varphi(r)^k = \begin{pmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{pmatrix},$$

and thus $\varphi(r)^n = I_2$. Since $\det \varphi(r) = 1$, we have

$$\varphi(r)^{-1} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Direct computation gives $\varphi(s)^2 = I_2$, and

$$\varphi(r)\varphi(s) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \varphi(s)\varphi(r)^{-1}.$$

Since these relations match those of D_{2n}, φ extends to a homomorphism from D_{2n} to $\mathrm{GL}_2(\mathbb{R})$.

(c) By Exercise 1.6.14, it suffices to show $\ker\varphi = 1$. Let $g \in \ker\varphi$, so $\varphi(g) = I_2$. If $g = r^k$ for some $1 \le k < n$, then $\varphi(g)_{11} = \cos(k\theta) = \cos(\frac{2\pi k}{n}) \neq 1$, so $\varphi(g) \neq I_2$. If $g = sr^k$ for some $0 \le k < n$, then $\varphi(g) = \varphi(s)\varphi(r)^k$. Since $\det\varphi(s) = -1$ and $\det\varphi(r)^k = 1$, it follows that $\det\varphi(g) = -1 \neq 1 = \det I_2$. Hence, $g = 1$, and $\ker\varphi = 1$, so 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. Matrix multiplication shows that the relations described in Exercise 1.5.3 are satisfied, so that φ extends to a homomorphism from Q_8 to $\mathrm{GL}_2(\mathbb{C})$. By Exercise 1.6.14, it suffices to show that $\ker\varphi = 1$. By Exercise 1.5.1, every element of $Q_8 - \{\pm 1\}$ squares to -1, so a nontrivial kernel must contain -1. However, $\varphi(-1) = -I_2 \neq I_2$, so $-1 \notin \ker\varphi$. Therefore, $\ker\varphi = 1$, and φ is injective. ■

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 $a \in F$. The action is well defined by closure of multiplication in F. Then

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

where the associativity of multiplication in F was used to conclude that $g(ha) = (gh)a$. Moreover, $1 \cdot a = 1a = a$ by the multiplicative identity axiom 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 $\mathbb{Z}$ 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 $r \cdot (x, y) = (x + ry, y)$.

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

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

Moreover, $0 \cdot (x, y) = (x + 0y, y) = (x, y)$, and thus $\mathbb{R}$ acts on $\mathbb{R}^2$. ■

Exercise 1.7.4: Kernel and Stabilizer of a Group Action

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) Let K denote the kernel of the action and let $b \in A$. Since $1 \cdot b = b$, we have $1 \in K$. Then for any $g, h \in K$, we have

$$gh \cdot b = g \cdot (h \cdot b) = g \cdot b = b, \quad g^{-1} \cdot b = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b,$$

and therefore $gh, g^{-1} \in K$. Hence, K is a subgroup of G.

(b) Let G_a denote the stabilizer of a in G. The same computations as in part (a) with $b = a$ show that 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 $\varphi \colon G \to S_A$ be the permutation representation corresponding to the action, so $\varphi(g)(a) = g \cdot a$ for all $g \in G$ and $a \in A$. Then

$$g \in K \iff g \cdot a = a \text{ for all } a \in A \iff \varphi(g) = 1 \iff g \in \ker \varphi.$$ ■

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. By definition, the action is faithful if and only if its permutation representation $\varphi\colon G \to S_A$ is injective. By Exercise 1.6.14, this holds if and only if $\ker \varphi = 1$, which by Exercise 1.7.5 is equivalent to the kernel of the action being the set consisting only of the identity. ■

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. If $V = \{0\}$ and $|F| > 2$, then $|F^\times| > 1$, so there exists $r \in F^\times$ with $r \neq 1$ such that $r \cdot 0 = 0$, and thus the action is not faithful. If $|F| = 2$, then $F^\times = \{1\}$, so the action is faithful. Otherwise, $V \neq \{0\}$, so we may pick $v \in V$ with $v \neq 0$. Suppose $r \cdot v = v$ for some $r \in F^\times$. Then $rv = v$, so $(r-1)v = 0$. Since $v \neq 0$ and F is a field, $r = 1$, so the action is faithful by Exercise 1.7.6. ■

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

(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 $\sigma, \tau \in S_A$ and let $S = \{x_1, \ldots, x_k\} \in B$. Since σ is injective, $|\sigma(S)| = |S| = k$, so $\sigma \cdot S \in B$. Then

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

Moreover, $1 \cdot S = \{1(x_1), \ldots, 1(x_k)\} = S$, so S_A acts on B.

(b)

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

■

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).

Manual Remark. *With respect to the note, we assume that the ordered k-tuples have distinct entries.*

Solution.

(a) The proof is similar to that of Exercise 1.7.8(a).

(b) Since order matters, there are twice as many cases to check:

S	$(1\,2)\cdot S$	$(1\,2\,3)\cdot S$
$(1,2)$	$(2,1)$	$(2,3)$
$(1,3)$	$(2,3)$	$(2,1)$
$(1,4)$	$(2,4)$	$(2,4)$
$(2,3)$	$(1,3)$	$(3,1)$
$(2,4)$	$(1,4)$	$(3,4)$
$(3,4)$	$(3,4)$	$(1,4)$

S	$(1\,2)\cdot S$	$(1\,2\,3)\cdot S$
$(2,1)$	$(1,2)$	$(3,2)$
$(3,1)$	$(3,2)$	$(1,2)$
$(4,1)$	$(4,2)$	$(4,2)$
$(3,2)$	$(3,1)$	$(1,3)$
$(4,2)$	$(4,1)$	$(4,3)$
$(4,3)$	$(4,3)$	$(4,1)$

■

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. Let $A = \{1, \dots, n\}$. If $n = 1$, then S_n is trivial, so the action is faithful for all k. Assume $n > 1$ and let $\sigma \in S_n$ be nonidentity. Then there exists $a \in A$ such that $\sigma(a) \neq a$.

(a) If $k < n$, then $|A - \{\sigma(a)\}| = n - 1 \geq k$, so there exists $S \subseteq A$ with $|S| = k$ and $\sigma(a) \notin S$ but $a \in S$. Then $\sigma(S) \neq S$, so the action is faithful for $k < n$. If $k = n$, then the only k-element subset of A is A itself, which is fixed by all permutations, so the action is not faithful for $k = n$.

(b) Consider the ordered k-tuple $T = (a, x_2, \dots, x_k)$, where $x_2, \dots, x_k \in A \setminus \{a\}$ are distinct and exist since $k \leq n$. Then $\sigma(T) = (\sigma(a), \sigma(x_2), \dots, \sigma(x_k)) \neq T$ because $\sigma(a) \neq a$. Therefore, no nonidentity permutation fixes every ordered k-tuple of elements of A, and the action is faithful for all $1 \leq k \leq n$. ■

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 labelled as in Section 2).

Solution. Let $\varphi\colon D_8 \to S_4$ 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 as in Section 1.2. Then the cycle decompositions are as follows:

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

■

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. For convenience, label the vertices with $0, 1, \dots, n-1$ clockwise and let $n \geq 4$ be even. Let r denote the rotation from vertex 0 to vertex 1 and let s denote the reflection across the line from the center to vertex 0, so $r(j) = j + 1$ and $s(j) = -j$ for all j with vertex labels read mod n. Let P_k denote the kth pair of opposite vertices

$$P_k = \{k, k + n/2\} \quad \text{for } k = 0, \dots, n/2 - 1,$$

where the subscripts are read mod $n/2$. Then for any j, $r(j + n/2) = j + n/2 + 1 = r(j) + n/2$ and $s(j + n/2) = -j - n/2 \equiv s(j) + n/2 \pmod{n}$, so r and s indeed map opposite pairs to opposite pairs. Thus, for any $g \in D_{2n}$, define $g \cdot \{a, b\} = \{g(a), g(b)\}$, which is a group action by Exercise 1.7.8(a).

For all i and k, we have $r^k \cdot P_i = P_{i+k}$ and $sr^k \cdot P_i = P_{-(i+k)}$ with subscripts read mod $n/2$. Thus, $r^k \cdot P_i = P_i$ if and only if $k \equiv 0 \pmod{n/2}$ and $sr^k \cdot P_i = P_i$ if and only if $2i + k \equiv 0 \pmod{n/2}$ for all i. Taking $i = 0$ gives $k \equiv 0 \pmod{n/2}$, while $i = 1$ gives $n/2 \mid 2$, so $n = 4$. Conversely, $n = 4$ and k even satisfy $2i + k \equiv 0 \pmod{2}$ for all i, so the kernel of the action is $\{1, r^2, s, sr^2\}$, and for $n \geq 6$, the kernel is $\{1, r^{n/2}\}$. ■

Exercise 1.7.13

Find the kernel of the left regular action.

Solution. If $g \cdot a = a$ for all $a \in G$, then $g = g1 = g \cdot 1 = 1$, so the kernel is 1. ■

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 $g \cdot a = ag$ 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 exist $g, h \in G$ such that $gh \neq hg$. Then $g \cdot (h \cdot 1) = hg \neq gh = (gh) \cdot 1$, so 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 $g \cdot a = ag^{-1}$ 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 have

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

Moreover, $1 \cdot a = a1 = a$, and thus this defines a left group action. ■

Exercise 1.7.16: Conjugation

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ 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, $1 \cdot a = 1a1^{-1} = a$, and therefore 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., is an automorphism of G — cf. Exercise 1.6.20). 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. Let $\varphi : x \mapsto gxg^{-1}$. Let $x, y \in G$. Then

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

so φ is a homomorphism. Conjugation by g^{-1} is a two-sided inverse of φ, and hence φ is an isomorphism. By Exercise 1.6.2, we have $|x| = |gxg^{-1}|$. Moreover, the bijection φ restricts to a bijection from A to gAg^{-1}, so $|A| = |gAg^{-1}|$. ■

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.

- Let $a \in A$. Then $a = 1a$, hence $a \sim a$.
- Let $a, b \in A$ such that $a \sim b$. Then $a = hb$ for some $h \in H$, so $b = h^{-1}a$ and $b \sim a$.
- Let $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then $a = h_1 b$ and $b = h_2 c$ for some $h_1, h_2 \in H$, so $a = h_1(h_2 c) = (h_1 h_2)c$ and $a \sim c$. ■

Exercise 1.7.19: Lagrange's Theorem

Let H be a subgroup (cf. Exercise 1.1.26) 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

$$H \to O \quad \text{defined by} \quad h \mapsto hx$$

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 $\varphi\colon H \to O$ be the map defined by $\varphi(h) = hx$ for all $h \in H$. Then φ is surjective by definition of O. Moreover, if $\varphi(h_1) = \varphi(h_2)$ for some $h_1, h_2 \in H$, then $h_1 x = h_2 x$, implying $h_1 = h_2$, so φ is injective. Therefore, φ is a bijection, whence $|O| = |H|$. By Exercise 1.7.18, the orbits of the action of H on G partition G, each of cardinality $|H|$. Thus, $|G| = k|H|$, where k is the number of orbits and is finite since G is finite, and hence $|H|$ divides $|G|$. ■

Exercise 1.7.20

Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 1.1.26) of S_4.

Solution. Let G be the group of rigid motions of a tetrahedron with vertices labeled 1, 2, 3, and 4. Then each $\alpha \in G$ sends vertices to vertices, so the elements of G permute the set of vertices $A = \{1, 2, 3, 4\}$. This gives rise to the homomorphism

$$\varphi\colon G \to S_4 \quad \text{where} \quad \varphi(\alpha)(i) = \alpha(i) \quad \text{for all} \quad i \in A.$$

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, α is the identity element of G. By Exercise 1.6.14, φ is injective, and Exercise 1.6.13 gives $G \cong \varphi(G)$, which is 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. 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, where the cube is centered at the origin. By Exercise 1.2.10, we know that $|G| = 24$. Each rigid motion $\alpha \in G$ permutes the set of pairs of opposite vertices, giving an action of G on A. Thus, we have the homomorphism

$$\varphi\colon G \to S_4 \quad \text{where} \quad \varphi(\alpha)(a_i) = \alpha(a_i) \quad \text{for all} \quad a_i \in A.$$

To see that φ is injective, suppose $\alpha \in \ker \varphi$. Then $\varphi(\alpha)(a_i) = a_i$ for all $a_i \in A$, so $\alpha(v) = \pm v$ for each vertex v of the cube. Let $d(v, w)$ denote the distance between vertices v and w. For some vertex v, suppose $\alpha(v) = v$, but $\alpha(w) = -w$ for an adjacent vertex w. Then $d(\alpha(v), \alpha(w)) = d(v, -w) \neq d(v, w)$, contradicting that α is a rigid motion. Since any two vertices are joined by some path of edges, α must send all vertices to themselves or swap each vertex with its opposite vertex. The former case corresponds to the identity rigid motion, while the latter case corresponds to a reflection through the origin, reversing the orientation, which is not a rigid motion of the cube. Hence, the kernel of φ is trivial, and φ is injective by Exercise 1.6.14. Since $|G| = 24 = |S_4|$, it follows that φ is surjective as well, and thus $G \cong S_4$. ■

Exercise 1.7.22

Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exercise 1.1.26) 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 an octahedron are isomorphic. (These groups are isomorphic because these solids are "dual" — see *Introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well — these solids are also dual.)

Solution. Let G be the group of rigid motions of an octahedron and let A be the set of four pairs of opposite faces of the octahedron. Each $\alpha \in G$ sends each pair of opposite faces to a pair of opposite faces, so G acts on A. By the argument in Exercise 1.7.21 with centers of faces in place of vertices and pairs of opposite faces in place of pairs of opposite vertices, we see that the homomorphism from G to S_4 induced by this action is injective. By Exercise 1.2.11, we know that $|G| = 24 = |S_4|$, so the injective homomorphism is also surjective, wherefore it is an isomorphism. By Exercise 1.7.21, the group of rigid motions of a cube is isomorphic to $S_4 \cong G$. ■

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. Let G be the group of rigid motions of a cube. By Exercise 1.2.10, $|G| = 24 > 6 = |S_3|$, so the permutation representation cannot be injective, and hence the action is not faithful. Let φ be the permutation representation of G acting on the set of three pairs of opposite faces and let $K = \ker \varphi$. By Exercise 1.6.14, K is a subgroup of G. Now let K act on G by left multiplication. Let $\mathcal{O}_a$ be the orbit of some $a \in G$ under this action. By Exercise 1.7.18, the orbits partition G, and by Exercise 1.7.19, each orbit has size $|K|$.

Place the cube with vertices $(\pm 1, \pm 1, \pm 1)$, let r_1 be the rotation by 90° about the z-axis, and let r_2 be the map $(x, y, z) \mapsto (z, x, y)$ defined by a 120° rotation about the axis through the vertices $(1, 1, 1)$ and $(-1, -1, -1)$. Observe that r_1 swaps the x- and y-pairs of opposite faces of the cube, while r_2 sends the x-pair of opposite faces to the y-pair, the y-pair to the z-pair, and the z-pair to the x-pair. Denoting the x-, y-, and z-pairs of opposite faces by 1, 2, and 3, respectively, we have $\varphi(r_1) = (1\ 2)$ and $\varphi(r_2) = (1\ 2\ 3)$. Since $\varphi(G)$ is closed under composition, it must contain the subgroup generated by $(1\ 2)$ and $(1\ 2\ 3)$, which is all of S_3 by Exercise 1.3.20. Therefore, φ is surjective. For any $a, b \in G$, we have $b \in \mathcal{O}_a$ if and only if $ba^{-1} \in K$, which holds if and only if $\varphi(b) = \varphi(a)$, so the orbits of G under the action of K correspond to the fibers of φ. Therefore, there are $|S_3| = 6$ distinct orbits of G under the action of K. Since $|G| = 24$ and each orbit has size $|K|$, we have $24 = |G| = |K| \cdot 6$, so $|K| = 4$. Finally, the identity and the three 180° rotations about the coordinate axes are in K, and thus all elements of K are accounted for. ■

2 Subgroups

2.1 Definitions and Examples

Let G be a group.

Exercise 2.1.1

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 and H be the subset in question. Each result follows from the Subgroup Criterion.
(a) Since $0 + 0i \in H$, H is nonempty. Let $a + ai, b + bi \in H$. Then

$$(a + ai) - (b + bi) = (a - b) + (a - b)i \in H$$

so that $H \leq G$.
(b) Since $|1| = 1$, $1 \in H$ so that it is nonempty. Let $z, w \in H$. Then

$$|zw^{-1}| = \frac{|z|}{|w|} = 1$$

so that $zw^{-1} \in H$, hence $H \leq G$.
(c) Fix $n \in \mathbb{Z}^+$. Since $1 \mid n$, $0 = 0/1 \in H$ so that H is nonempty. Let $a/b, c/d \in H$, and let $\ell = \text{lcm}(b, d)$. From $b \mid n$ and $d \mid n$, we have $\ell \mid n$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{a\ell/b - c\ell/d}{\ell},$$

where reducing denominators still gives an integer dividing ℓ, hence dividing n, so that $H \leq G$.
(d) Fix $n \in \mathbb{Z}^+$. Since $(1, n) = 1$, $0 = 0/1 \in H$ so that H is nonempty. Let $a/b, c/d \in H$ so that $(b, n) = (d, n) = 1$. Then

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

Any prime p such that $p \mid bd$ gives $p \mid b$ or $p \mid d$, and thus $p \nmid n$. Reducing denominators gives an integer dividing bd which is still relatively prime to n, wherefore $H \leq G$.
(e) Since $1 = 1^2 = 1/1$, $1 \in H$ so that H is nonempty. Let $x, y \in H$ so $x^2, y^2 \in \mathbb{Q}$. Then

$$\left(\frac{x}{y}\right)^2 = \frac{x^2}{y^2} \in \mathbb{Q}$$

so that $x/y \in H$, hence $H \leq G$. ■

Exercise 2.1.2

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 G be the group and H be the subset in question.
(a) For all S_n with $n \geq 3$, $(1\,2), (1\,3) \in H$, but $(1\,2)(1\,3) = (1\,3\,2) \notin H$.
(b) For all D_{2n} with $n \geq 3$, $s, sr \in H$, but $s(sr) = r \notin H$ since $|r| = n \geq 3$.
(c) Let $n = ab$ for some $a, b \in \mathbb{Z}^+$ with $1 < a, b < n$. Let $x \in G$ with $|x| = n$, so $x \in H$. If $H \leq G$, then $x^a \in H$, but $(x^a)^b = x^n = 1$ implies that $|x^a| \leq b < n$. Because $0 < a < n$, $x^a \neq 1$, so $x^a \notin H$.
(d) Observe that $1 \in H$, but $1 + 1 = 2 \notin H$.
(e) Observe that $\sqrt{2}, \sqrt{3} \in H$, but $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \notin \mathbb{Q}$. ■

Exercise 2.1.3

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, so each subset is a subgroup of D_8 by the finite case of the Subgroup Criterion. ■

Exercise 2.1.4

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. Let $G = \mathbb{Z}$ and $H = \mathbb{Z}^+$. Then for any $m, n \in \mathbb{Z}^+$, we have $m + n \in \mathbb{Z}^+$ but $m - n \notin \mathbb{Z}^+$ when $m < n$. Hence, H is not a subgroup of G. ■

Exercise 2.1.5

Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution. If $H \leq G$ with $|H| = n - 1$, then there exists $k \in \mathbb{Z}^+$ such that $k(n-1) = n$ by Exercise 1.7.19. But since $1 < n/(n-1) < 2$ for all $n > 2$, no such k can exist. ■

Exercise 2.1.6: Torsion Subgroup

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 set of elements of finite order in G. Since $|1| = 1$, $1 \in \mathrm{Tor}(G)$. Let $g, h \in \mathrm{Tor}(G)$ with $|g| = m$ and $|h| = n$. Since G is abelian, we have

$$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn} = (g^m)^n((h^n)^{-1})^m = 1^n(1^{-1})^m = 1.$$

Thus, $|gh^{-1}| \leq mn$, so $gh^{-1} \in \mathrm{Tor}(G)$ and $\mathrm{Tor}(G) \leq G$ by the Subgroup Criterion.

Consider $G = \mathrm{GL}_2(\mathbb{R})$ where

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Note that $|A| = |B| = 2$ so that $A, B \in \mathrm{Tor}(G)$. However,

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

By induction, we may show that

$$(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

for all $n \in \mathbb{Z}^+$. Hence, $|AB| = \infty$, so $AB \notin \mathrm{Tor}(G)$. ■

Exercise 2.1.7

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. If $(x, \overline{y}) \in \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ is such that $k(x, \overline{y}) = (0, \overline{0})$ for $k \geq 1$, then $kx = 0$ in $\mathbb{Z}$, so $x = 0$. Conversely, $n(0, \overline{y}) = (0, \overline{0})$, so $(0, \overline{y})$ has finite order. Therefore, $(x, \overline{y}) \in \mathrm{Tor}(\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z}))$ if and only if $x = 0$, so

$$\mathrm{Tor}(\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})) = \{(0, \overline{y}) \mid \overline{y} \in \mathbb{Z}/n\mathbb{Z}\}.$$

Consider $H = \{(x, \overline{y}) \in \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z}) \mid x \neq 0\} \cup \{(0, \overline{0})\}$. By the first part, $(x, \overline{y}) \in \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ has infinite order if and only if $x \neq 0$, so H is exactly the set of elements of infinite order together with the identity. We have $(1, \overline{1}), (-1, \overline{0}) \in H$, but $(0, \overline{1}) = (1, \overline{1}) + (-1, \overline{0}) \notin H$ since $\overline{1} \neq \overline{0}$. Hence, H is not a subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. ■

Exercise 2.1.8

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.
$\boxed{\Rightarrow}$ Suppose $H \cup K \leq G$ and $H \not\subseteq K$. Then there exists $h \in H$ such that $h \notin K$. Since $H \cup K \leq G$, for any $k \in K$, we have $hk \in H \cup K$. If $hk \in K$, then $h = (hk)k^{-1} \in K$, contradicting our assumption. Therefore, $hk \in H$, so $k = h^{-1}(hk) \in H$, and hence $K \subseteq H$.
$\boxed{\Leftarrow}$ If $H \subseteq K$ or $K \subseteq H$, then $H \cup K$ equals K or H, respectively, so $H \cup K \leq G$. ■

Exercise 2.1.9: Special Linear Group

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 $\det(I_n) = 1$, $I_n \in \mathrm{SL}_n(F)$. Suppose $A, B \in \mathrm{SL}_n(F)$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \frac{\det(A)}{\det(B)} = 1,$$

wherefore $AB^{-1} \in \mathrm{SL}_n(F)$, and hence $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$ by the Subgroup Criterion. ■

Exercise 2.1.10

(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. We prove (b) and note that (a) is a special case with $I = \{1, 2\}$ and $H_1 = H$, $H_2 = K$. Let I be a nonempty indexing set, and consider the collection of subgroups $\{H_i\}_{i \in I}$ of G. Let

$$L = \bigcap_{i \in I} H_i.$$

Since $1 \in H_i$ for all $i \in I$, $1 \in L$. Suppose $a, b \in L$. Then $a, b \in H_i$ for all $i \in I$. Since each H_i is a subgroup of G, $ab^{-1} \in H_i$ for all $i \in I$. Hence, $ab^{-1} \in L$, so $L \leq G$ by the Subgroup Criterion. ■

Exercise 2.1.11

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 here we assume $B = A$ (called the **diagonal subgroup**).

Solution. Let C be the set in each part.
(a) Since $1 \in A$, $(1,1) \in C$ so that C is nonempty. Suppose $(a_1,1),(a_2,1) \in C$. Then

$$(a_1,1)(a_2,1)^{-1} = (a_1,1)(a_2^{-1},1) = (a_1a_2^{-1},1) \in C$$

since $a_1a_2^{-1} \in A$. Hence, $C \leq A \times B$ by the Subgroup Criterion.
(b) This is part (a) with the roles of A and B reversed.
(c) Since $1 \in A$, $(1,1) \in C$ so that C is nonempty. Suppose $(a_1,a_1),(a_2,a_2) \in C$. Then

$$(a_1,a_1)(a_2,a_2)^{-1} = (a_1,a_1)(a_2^{-1},a_2^{-1}) = (a_1a_2^{-1},a_1a_2^{-1}) \in C$$

since $a_1a_2^{-1} \in A$. Hence, $C \leq A \times B$ by the Subgroup Criterion. ■

Exercise 2.1.12

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 set in each part.
(a) Since $1 = 1^n$, $1 \in B$ so that B is nonempty. Suppose $a^n, b^n \in B$. Since A is abelian, we have

$$(a^n)(b^n)^{-1} = a^nb^{-n} = (ab^{-1})^n \in B,$$

and thus $B \leq A$ by the Subgroup Criterion.
(b) Since $1^n = 1$, $1 \in B$ so that B is nonempty. Suppose $a, b \in B$. Since A is abelian, we have

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

so $ab^{-1} \in B$, and thus $B \leq A$ by the Subgroup Criterion. ■

Exercise 2.1.13

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. If H has no nonzero element, then $H = 0$. Otherwise, let $a/b \in H$ be nonzero with $a, b \in \mathbb{Z}$, where $b \neq 0$ and $a \neq 0$ since $a/b \neq 0$. Then $b(a/b) = a \in H$ so that $1/a \in H$, whence $1 \in H$. Now let $c/d \in \mathbb{Q}$ for some $c, d \in \mathbb{Z}$ with $d \neq 0$. Then $d(1) = d \in H$ so that $1/d \in H$, and $c(1/d) = c/d \in H$. Since c/d was arbitrary, $H = \mathbb{Q}$. ■

Exercise 2.1.14

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. All reflections are in H. In particular, s and sr are in H, but $r = s(sr) \notin H$ since $|r| = n > 2$. ■

Exercise 2.1.15

Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Solution. Let H be the union in question. Then $1 \in H_1 \subseteq H$. Let $a, b \in H$ so that there exist $m, n \in \mathbb{Z}^+$ where $a \in H_m$ and $b \in H_n$. With $k = \max(m,n)$, we have $H_m \subseteq H_k$ and $H_n \subseteq H_k$, and thus $a, b \in H_k$. Since $H_k \leq G$, $ab^{-1} \in H_k$, and hence $ab^{-1} \in H$. Therefore, $H \leq G$ by the Subgroup Criterion. ■

Exercise 2.1.16

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 in question. Observe that $I_n \in \mathrm{UT}_n(F)$ so that $\mathrm{UT}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{UT}_n(F)$, and consider $C = AB$. Since $\mathrm{GL}_n(F)$ is a group, $C \in \mathrm{GL}_n(F)$. Moreover, the (i, j)th entry of C is given by

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

If $i > j$, then for each k, either $i > k$ or $k \geq i > j$, and thus $a_{ik} b_{kj} = 0$. Therefore, $c_{ij} = 0$ for all $i > j$, and $C \in \mathrm{UT}_n(F)$.

Now let $A \in \mathrm{UT}_n(F)$ and $X = A^{-1}$. Since $A \in \mathrm{GL}_n(F)$, $\det A = \prod_i a_{ii} \neq 0$, so $a_{ii} \neq 0$ for all i. Fix column j and consider $i > j$. Because $a_{ik} = 0$ for $k < i$ and $i \neq j$, the ith row of $AX = I_n$ gives

$$a_{ii} x_{ij} + \sum_{k>i} a_{ik} x_{kj} = 0.$$

By induction on i from n down to $j + 1$, we have $x_{kj} = 0$ for all $k > i$, so $a_{ii} x_{ij} = 0$, and hence $x_{ij} = 0$. Therefore, X is upper triangular, and $X \in \mathrm{UT}_n(F)$. ■

Exercise 2.1.17

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. We have $I_n \in H$ so that H is nonempty. Suppose $A, B \in H$. By Exercise 2.1.16, $AB \in \mathrm{UT}_n(F)$, so it remains to check that $(AB)_{ii} = 1$ for all i. We have

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}.$$

Since $a_{ik} = 0$ for $k < i$ and $b_{ki} = 0$ for $k > i$, the sum evaluates to $a_{ii} b_{ii} = 1$ for all i, so H is closed under multiplication.

Now let $A \in H$ and $X = A^{-1}$. By Exercise 2.1.16, $X \in \mathrm{UT}_n(F)$, so it remains to check that $x_{ii} = 1$ for all i. Since both A and X are upper triangular, the diagonal computation above gives $(AX)_{ii} = a_{ii} x_{ii} = 1$ for all i. Since $a_{ii} = 1$, we have $x_{ii} = 1$ for all i, and hence $X \in H$. ■

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Exercise 2.2.1

Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Solution. $g \in C_G(A) \iff ag = ga$ for all $a \in A \iff g^{-1}ag = a$ for all $a \in A$. ■

Exercise 2.2.2

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Solution. Let $g \in G$ and $z \in Z(G)$. Then $gz = zg$, so $g \in C_G(Z(G))$. Therefore, $G \subseteq C_G(Z(G))$, so $C_G(Z(G)) = G$. Since $C_G(Z(G)) \leq N_G(Z(G)) \leq G$, $N_G(Z(G)) = G$. ■

Exercise 2.2.3

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 $g \in C_G(B)$, so $gbg^{-1} = b$ for all $b \in B$. In particular, $gag^{-1} = a$ for all $a \in A$ because $A \subseteq B$, so $g \in C_G(A)$, and thus $C_G(B) \subseteq C_G(A)$. Since $C_G(B)$ and $C_G(A)$ are subgroups of G, $C_G(B) \leq C_G(A)$. ■

Exercise 2.2.4

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. Observe that $Z(G) = \bigcap_{g \in G} C_G(g)$ and $C_G(1) = G$. For S_3, let $C = C_{S_3}((1\,2))$. Since $(1\,2)(1\,3) \neq (1\,3)(1\,2)$, we have $C \neq S_3$. Because $\{1, (1\,2)\} \leq C$ and $C \leq S_3$, Lagrange's Theorem gives $|C| \mid 6$ and $2 \mid |C|$, so $|C| = 2$, and therefore $C = \{1, (1\,2)\}$. By symmetry, the same argument holds for $(1\,3)$ and $(2\,3)$, and thus

$$C_{S_3}((1\,2)) = \{1, (1\,2)\}, \quad C_{S_3}((1\,3)) = \{1, (1\,3)\}, \quad C_{S_3}((2\,3)) = \{1, (2\,3)\}.$$

A similar argument for $(1\,2\,3)$, along with $(1\,2\,3)(1\,2) \neq (1\,2)(1\,2\,3)$, shows that $C_{S_3}((1\,2\,3)) = \{1, (1\,2\,3), (1\,3\,2)\}$. Since $C_G(x) = C_G(x^{-1})$, we have $C_{S_3}((1\,3\,2)) = C_{S_3}((1\,2\,3))$. Finally, $Z(S_3) = \{1\}$.

Note that r^2 commutes with r and s, so $r^2 \in Z(D_8)$, and the centralizers of D_8 are:

$$\begin{aligned} C_{D_8}(1) &= D_8 & C_{D_8}(s) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(r) &= \{1, r, r^2, r^3\} & C_{D_8}(sr) &= \{1, r^2, sr, sr^3\} \\ C_{D_8}(r^2) &= D_8 & C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(r^3) &= \{1, r, r^2, r^3\} & C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\}, \end{aligned}$$

and $Z(D_8) = \{1, r^2\}$. Now, -1 commutes with all elements of Q_8, so $-1 \in Z(Q_8)$, and the centralizers of Q_8 are:

$$\begin{aligned} C_{Q_8}(1) &= Q_8 & C_{Q_8}(-1) &= Q_8 \\ C_{Q_8}(i) &= \{1, -1, i, -i\} & C_{Q_8}(-i) &= \{1, -1, i, -i\} \\ C_{Q_8}(j) &= \{1, -1, j, -j\} & C_{Q_8}(-j) &= \{1, -1, j, -j\} \\ C_{Q_8}(k) &= \{1, -1, k, -k\} & C_{Q_8}(-k) &= \{1, -1, k, -k\} \end{aligned}$$

and $Z(Q_8) = \{1, -1\}$.

Let G be any one of S_3, D_8, or Q_8. By Exercise 1.1.35, the cyclic subgroup generated by any $g \in G$ has order $|g|$. Since the cyclic subgroup generated by g and $Z(G)$ are both contained in $C_G(g)$, Lagrange's Theorem gives $\operatorname{lcm}(|g|, |Z(G)|) \mid |C_G(g)|$. Since $|C_G(g)| \mid |G|$ as well, finding an element that does not commute with noncentral g determines the exact order of $C_G(g)$. ■

Exercise 2.2.5

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. Each part will verify $C_G(A) = A$. To show $N_G(A) = G$, we use the fact that $C_G(A) \leq N_G(A)$ and that $|G|/|C_G(A)| = 2$, so $|N_G(A)|$ must be either $|C_G(A)|$ or $|G|$ by Lagrange's Theorem. We then give some $x \in G - A$ such that $xAx^{-1} = A$, so $x \in N_G(A)$ and thus $N_G(A) = G$.
(a) By Exercise 2.2.4, $C_{S_3}(A) = C_{S_3}((1\,2\,3)) \cap C_{S_3}((1\,3\,2)) = A$. Use $x = (1\,2)$.
(b) By Exercise 2.2.4, $C_{D_8}(A) = C_{D_8}(s) \cap C_{D_8}(r^2) \cap C_{D_8}(sr^2) = A$. Use $x = r$.
(c) Observe that A is the cyclic subgroup generated by r. By Lagrange's Theorem, $5 \mid |C_{D_{10}}(A)|$ and $|C_{D_{10}}(A)| \mid 10$. Because $sr \neq rs$, we have $s \notin C_{D_{10}}(A)$, so $C_{D_{10}}(A) = A$. Use $x = s$. ■

Exercise 2.2.6

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) Let $h \in H$. Closure gives $hHh^{-1} \subseteq H$. The same argument applied to h^{-1} gives $h^{-1}Hh \subseteq H$, so $hHh^{-1} = H$ and $h \in N_G(H)$.
As a counterexample, let $G = D_6$ and $H = \{1, r, s\}$. Then
$$rHr^{-1} = \{1, r, sr\} \neq H$$
so that r does not normalize H, and thus $H \not\leq N_G(H)$.
(b) $H \leq C_G(H) \iff hk = kh$ for all $h, k \in H \iff H$ is abelian. ■

Exercise 2.2.7

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.
(a) This follows from Exercise 1.2.5.
(b) This follows from Exercise 1.2.4. ■

Exercise 2.2.8

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 S_n acts on $\{1, 2, \ldots, n\}$ by permutation, the stabilizer of i under this action is a subgroup of S_n, so $G_i \leq G$. For any $\sigma \in G_i$, we have $\sigma(i) = i$ and σ injective, so σ permutes $\{1, 2, \ldots, n\} - \{i\}$. Conversely, any such permutation of $\{1, 2, \ldots, n\} - \{i\}$ extends to a permutation in G_i by fixing i. There are $(n-1)!$ ways to permute these $n-1$ elements, so $|G_i| = (n-1)!$. ■

Exercise 2.2.9

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. We have $N_H(A) = \{h \in H \mid hAh^{-1} = A\} = \{g \in G \mid gAg^{-1} = A\} \cap H = N_G(A) \cap H$. By Exercise 2.1.10, $N_G(A) \cap H \leq G$, and since $N_G(A) \cap H \subseteq H$, we have $N_G(A) \cap H \leq H$. ■

Exercise 2.2.10

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. By assumption, $H = \{1, h\}$ for some $h \in G$ with $h \neq 1$. By the text, $C_G(H) \leq N_G(H)$. Pick $g \in N_G(H)$, so $gHg^{-1} = H$. Then

$$gHg^{-1} = \{g1g^{-1}, ghg^{-1}\} = \{1, ghg^{-1}\} = H = \{1, h\}.$$

Observe $ghg^{-1} \neq 1$, for otherwise $gh = g$, so $h = 1$, contradicting that $h \neq 1$. Then $ghg^{-1} = h$, so $g \in C_G(H)$, and hence $N_G(H) \subseteq C_G(H)$, whence $C_G(H) = N_G(H)$. If $N_G(H) = G$, then $C_G(H) = G$, so every element of H commutes with every $g \in G$, and therefore $H \leq Z(G)$. ■

Exercise 2.2.11

Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Solution. Note that $Z(G) \leq C_G(A)$ and the text gives $C_G(A) \leq N_G(A)$, so $Z(G) \leq N_G(A)$. ■

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 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,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \qquad (*)$$

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

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_3 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

(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 stabilize 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. For parts (c) – (f), let q be the element to be stabilized. The text gives that the stabilizer of any $q \in R$ is a subgroup of S_4, so it remains to be shown that the specific stabilizers have the claimed structure.

(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 $1 \cdot r_1 = r_1$ for any $r_1 \in R$. Let $\alpha, \beta \in S_4$, and put $r_2 = \beta \cdot r_1(x_1, x_2, x_3, x_4)$. Then $\alpha \cdot r_2$ replaces each x_j in r_2 by $x_{\alpha(j)}$, so $x_{\beta(j)}$ becomes $x_{\alpha(\beta(j))}$. Therefore,

$$\begin{aligned} \alpha \cdot r_2 &= \alpha \cdot (\beta \cdot r_1(x_1, x_2, x_3, x_4)) \\ &= \alpha \cdot r_1(x_{\beta(1)}, x_{\beta(2)}, x_{\beta(3)}, x_{\beta(4)}) \\ &= r_1(x_{\alpha(\beta(1))}, x_{\alpha(\beta(2))}, x_{\alpha(\beta(3))}, x_{\alpha(\beta(4))}) \\ &= (\alpha \circ \beta) \cdot r_1(x_1, x_2, x_3, x_4) \end{aligned}$$

(c) We have $\alpha \in G_q$ if and only if $\alpha(4) = 4$, so G_q consists of the permutations of $\{1, 2, 3\}$ extended by fixing 4:

$$G_q = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Restricting α to $\{1, 2, 3\}$ gives a bijection $G_q \to S_3$ defined by $\alpha \mapsto \alpha|_{\{1,2,3\}}$. Moreover, for $\alpha, \beta \in G_q$, we have $(\alpha \circ \beta)|_{\{1,2,3\}} = \alpha|_{\{1,2,3\}} \circ \beta|_{\{1,2,3\}}$, so the bijection is a homomorphism, and thus $G_q \cong S_3$.

(d) We have $\alpha \in G_q$ if and only if $\alpha(\{1, 2\}) = \{1, 2\}$. These are exactly the permutations

$$G_q = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

All nonidentity elements of G_q have order 2, so it is abelian by Exercise 1.1.25.

(e) We have $\alpha \in G_q$ if and only if $\alpha(\{\{1, 2\}, \{3, 4\}\}) = \{\{1, 2\}, \{3, 4\}\}$, so the permutations that satisfy this condition are exactly

$$G_q = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}.$$

Put $\pi = (1\ 2)$ and $\rho = (1\ 3\ 2\ 4)$. The eight elements ρ^k and $\pi\rho^k$ for $0 \le k \le 3$ are all distinct and account for all elements of G_q. By inspection, $\rho^4 = \pi^2 = 1$, and

$$\rho\pi = (1\ 3\ 2\ 4)(1\ 2) = (1\ 4)(2\ 3) = (1\ 2)(1\ 4\ 2\ 3) = \pi\rho^{-1}.$$

Since ρ and π satisfy the same relations as those in D_8, there exists a surjective homomorphism $\varphi\colon D_8 \to G_q$ defined by $\varphi(r) = \rho$ and $\varphi(s) = \pi$. Since $|D_8| = |G_q| = 8$, φ is an isomorphism, so $G_q \cong D_8$.

(f) Rewrite q as

$$q = \sum_{i<j} x_i x_j - (x_1x_2 + x_3x_4) = q_0 - (x_1x_2 + x_3x_4).$$

For any $\alpha \in S_4$, we have $\alpha(\{x_ix_j \mid i < j\}) = \{x_{\alpha(i)}x_{\alpha(j)} \mid i < j\} = \{x_ix_j \mid i < j\}$, so $\alpha \cdot q_0 = q_0$. Moreover, for any $f, g \in R$, we have $\alpha \cdot (f + g) = \alpha \cdot f + \alpha \cdot g$, so $\alpha \cdot q = q_0 - \alpha \cdot (x_1x_2 + x_3x_4)$. Therefore, $\alpha \cdot q = q$ if and only if α fixes $x_1x_2 + x_3x_4$, which is exactly the stabilizer obtained in part (e). ■

Exercise 2.2.13

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

$$\sigma\colon R \to R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Prove that this defines a (left) group action of S_n on R.

Solution. The proof is similar to Exercise 2.2.12(b) but with n in place of 4. ■

Exercise 2.2.14

Let $H(F)$ be the Heisenberg group over the field F introduced in Exercise 1.4.11. 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 $X = (a, b, c) \in Z(H(F))$ and $Y = (d, e, f) \in H(F)$. Then

$$XY = (a + d, b + e + af, c + f), \quad YX = (d + a, e + b + dc, f + c).$$

Since $XY = YX$, the middle entries must be equal, so $af = dc$ for all $d, f \in F$. In particular, $d = 0$ and $f = 1$ gives $a = 0$, and $d = 1$ and $f = 0$ gives $c = 0$. Conversely, any $(0, z, 0) \in H(F)$ commutes with all elements of $H(F)$, so it lies in the center. Therefore,

$$Z(H(F)) = \{(0, z, 0) \mid z \in F\}.$$

The map $z \mapsto (0, z, 0)$ has a two-sided inverse given by $(0, z, 0) \mapsto z$, so it is a bijection. Moreover, for any $x, y \in F$, we have

$$(0, x, 0)(0, y, 0) = (0, x + y, 0),$$

which shows that the map is a homomorphism. Therefore, it is an isomorphism, and $Z(H(F)) \cong F$. ■

2.3 Cyclic Groups and Cyclic Subgroups

Exercise 2.3.1

Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Solution. Recall that $\langle \bar{a} \rangle \leq \langle \bar{b} \rangle$ if and only if $(b, 45) \mid (a, 45)$ for $1 \leq a, b \leq 45$ in $\mathbb{Z}/45\mathbb{Z}$. By Theorem 2.4(1), $Z_{45} \cong \mathbb{Z}/45\mathbb{Z}$, so subgroups and inclusions correspond to those in $\mathbb{Z}/45\mathbb{Z}$. The divisors of 45 are 1, 3, 5, 9, 15, and 45, and Theorem 2.7(3) gives $\langle x^m \rangle = \langle x^{(m,45)} \rangle$, so the full list of subgroups and their inclusions is

$$\begin{aligned} Z_{45} = \langle x \rangle &> \langle x^3 \rangle, \langle x^5 \rangle, \langle x^9 \rangle, \langle x^{15} \rangle, 1 = \langle x^{45} \rangle \\ \langle x^3 \rangle &> \langle x^9 \rangle, \langle x^{15} \rangle, 1 \\ \langle x^5 \rangle &> \langle x^{15} \rangle, 1 \\ \langle x^9 \rangle &> 1 \\ \langle x^{15} \rangle &> 1 \end{aligned}$$

■

Exercise 2.3.2

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. By Proposition 2.2, $|\langle x \rangle| = |x| = |G|$, so $\langle x \rangle = G$. Moreover, this is not true if G is infinite, since $|\mathbb{Z}| = |2| = \infty$, but $\langle 2 \rangle$ is a proper subgroup of $\mathbb{Z}$. ■

Exercise 2.3.3

Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Solution. Proposition 2.6(2) gives $\mathbb{Z}/48\mathbb{Z} = \langle \bar{a} \rangle$ if and only if $(a, 48) = 1$. The integers a with $0 \leq a < 48$ and $(a, 48) = 1$ are precisely 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, and 47. ■

Exercise 2.3.4

Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Solution. By Proposition 2.6(2), $\mathbb{Z}/202\mathbb{Z} = \langle \bar{a} \rangle$ if and only if $(a, 202) = 1$. Since $202 = 2 \cdot 101$, the integers a with $0 \leq a < 202$ and $(a, 202) = 1$ are precisely the odd integers not divisible by 101. ■

Exercise 2.3.5

Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution. By Proposition 2.6(2), the number of generators of $\mathbb{Z}/49000\mathbb{Z}$ is $\varphi(49000)$, so

$$\begin{aligned} \varphi(49000) &= \varphi(2^3)\varphi(5^3)\varphi(7^2) \\ &= 2^2(2-1)5^2(5-1)7(7-1) \\ &= 16800. \end{aligned}$$

■

Exercise 2.3.6

In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \bar{a} \rangle$ for every $\bar{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Solution. We proceed similarly to Exercise 2.3.1, where $\langle \bar{a} \rangle \leq \langle \bar{b} \rangle$ if and only if $(b, 48) \mid (a, 48)$ for $1 \leq a, b \leq 48$. We have $\mathbb{Z}/48\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{46}, \overline{47}\}$. The divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24, and 48, and Theorem 2.7(3) gives $\langle \bar{a} \rangle = \langle \overline{(a, 48)} \rangle$. Therefore, the list of proper subgroups of $\mathbb{Z}/48\mathbb{Z}$ is

$$\begin{aligned}
\langle \bar{2} \rangle &= \{\bar{0}, \bar{2}, \ldots, \overline{44}, \overline{46}\}, & \langle \bar{6} \rangle &= \{\bar{0}, \bar{6}, \ldots, \overline{36}, \overline{42}\}, & \langle \overline{16} \rangle &= \{\bar{0}, \overline{16}, \overline{32}\}, \\
\langle \bar{3} \rangle &= \{\bar{0}, \bar{3}, \ldots, \overline{42}, \overline{45}\}, & \langle \bar{8} \rangle &= \{\bar{0}, \bar{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\}, & \langle \overline{24} \rangle &= \{\bar{0}, \overline{24}\}, \\
\langle \bar{4} \rangle &= \{\bar{0}, \bar{4}, \ldots, \overline{40}, \overline{44}\}, & \langle \overline{12} \rangle &= \{\bar{0}, \overline{12}, \overline{24}, \overline{36}\}, & \langle \bar{0} \rangle &= \{\bar{0}\},
\end{aligned}$$

with the following inclusions:

$$\begin{aligned}
\mathbb{Z}/48\mathbb{Z} = \langle \bar{1} \rangle > \langle \bar{2} \rangle, \langle \bar{3} \rangle, \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle, \langle \overline{48} \rangle = \langle \bar{0} \rangle \\
\langle \bar{2} \rangle > \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \bar{3} \rangle > \langle \bar{6} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \bar{4} \rangle > \langle \bar{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \bar{6} \rangle > \langle \overline{12} \rangle, \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \bar{8} \rangle > \langle \overline{16} \rangle, \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \overline{12} \rangle > \langle \overline{24} \rangle, \langle \bar{0} \rangle \\
\langle \overline{16} \rangle > \langle \bar{0} \rangle \\
\langle \overline{24} \rangle > \langle \bar{0} \rangle.
\end{aligned}$$

■

Exercise 2.3.7

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. Using the isomorphism $\bar{k} \mapsto x^k$ by Theorem 2.4(1), the subgroups $\langle \bar{a} \rangle$ of $\mathbb{Z}/48\mathbb{Z}$ map to $\langle x^a \rangle$, so 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. ■

Exercise 2.3.8

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 $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}?

Solution. If $\langle x^a \rangle = Z_{48}$, then φ_a extends to an isomorphism by Theorem 2.4(1). Conversely, if φ_a extends to an isomorphism, then it is surjective, so $\langle \bar{1} \rangle$ maps to the whole group, i.e., $\langle x^a \rangle = Z_{48}$. By Proposition 2.6(2), $\langle x^a \rangle = Z_{48}$ if and only if $(a, 48) = 1$. Therefore, the integers a for which φ_a extends to an isomorphism are precisely those integers a such that $(a, 48) = 1$. ■

Exercise 2.3.9

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. We have

$$\psi_a : \bar{r} \mapsto x^{ar} \text{ is a well defined homomorphism } \iff x^{48a} = 1 \iff 36 \mid 48a \iff 3 \mid a,$$

where the second equivalence follows from $|x| = 36$ by Propositions 2.2(1) and 2.3. Surjectivity requires $Z_{36} = \langle x^a \rangle$, which occurs if and only if $(36, a) = 1$ by Proposition 2.6(2). Since $3 \mid a$, we have $3 \mid (36, a)$, so ψ_a is never surjective. ■

Exercise 2.3.10

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 2.2 and $\mathbb{Z}/54\mathbb{Z} = \langle \bar{1} \rangle$, $|\bar{1}| = 54$. By Proposition 2.5(2), $|\overline{30}| = \frac{54}{(54,30)} = \frac{54}{6} = 9$. By Theorem 2.7(3), $\langle \overline{30} \rangle = \langle \bar{6} \rangle$, so

$$\langle \overline{30} \rangle = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\},$$

where $\bar{0}$ has order 1, $\overline{18}$ and $\overline{36}$ have order 3, and the remaining elements have order 9. ■

Exercise 2.3.11

Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

Solution. By direct computation, the cyclic subgroups of D_8 are

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle r \rangle = \langle r^3 \rangle &= \{1, r, r^2, r^3\} \\ \langle r^2 \rangle &= \{1, r^2\} \\ \langle sr^k \rangle &= \{1, sr^k\} \quad \text{for } k = 0, 1, 2, 3. \end{aligned}$$

Consider the subset $H = \{1, r^2, s, sr^2\}$ of D_8. Since H is finite and $r^2 s = sr^2 \in H$, it is closed under the group operation, so $H \leq D_8$ by the Subgroup Criterion. Moreover, all elements of H have order at most 2, so H cannot be cyclic by Proposition 2.2. ■

Exercise 2.3.12

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 $Z_2 = \langle x \rangle$, so $Z_2 \times Z_2 = \{(1,1), (1,x), (x,1), (x,x)\}$. Since all elements of $Z_2 \times Z_2$ have order at most 2, it cannot be cyclic by Proposition 2.2.
(b) If (a,b) generated $Z_2 \times \mathbb{Z}$, then $Z_2 \times \mathbb{Z} = \{(a^n, nb) \mid n \in \mathbb{Z}\}$. Since the second component must generate $\mathbb{Z}$, we must have $b = \pm 1$ by Proposition 2.6(1). Then $(x,0) = (a^n, nb)$ for some $n \in \mathbb{Z}$, which implies $nb = 0$ and hence $n = 0$. But then $(a^n, nb) = (1,0) \neq (x,0)$, a contradiction. Therefore, $Z_2 \times \mathbb{Z}$ cannot be cyclic.
(c) A similar argument to part (b) shows that if $\langle (a,b) \rangle = \mathbb{Z} \times \mathbb{Z}$, then $a = \pm 1$ and $b = \pm 1$. Then $\langle (a,b) \rangle = \{(na, nb) \mid n \in \mathbb{Z}\}$, i.e., it only contains elements where the absolute values of the components are equal. Since $(1,0) \notin \langle (a,b) \rangle$, we conclude that $\mathbb{Z} \times \mathbb{Z}$ cannot be cyclic. ■

Exercise 2.3.13

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. Put $Z_2 = \langle x \rangle$.
(a) By Exercise 1.6.2, isomorphisms preserve element orders. Observe that $(0, x) \in \mathbb{Z} \times Z_2$ has order 2. If $n \in \mathbb{Z}$ has order 2, then $2n = 0$, which implies $n = 0$, a contradiction.
(b) The same argument as in part (a) works with $\mathbb{Q}$ in place of $\mathbb{Z}$. ■

Exercise 2.3.14

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. Refer to Exercise 1.3.9 to see the distinct powers of σ. Put $a = 12q + r$ with $0 \leq r < 12$. Because $\sigma^{12} = 1$, we have $\sigma^a = \sigma^r$.

$$\begin{aligned} \sigma^{13} &= \sigma^{12(1)+1} = \sigma^1 & \qquad \sigma^{-6} &= \sigma^{12(-1)+6} = \sigma^6 \\ \sigma^{65} &= \sigma^{12(5)+5} = \sigma^5 & \qquad \sigma^{-81} &= \sigma^{12(-7)+3} = \sigma^3 \\ \sigma^{626} &= \sigma^{12(52)+2} = \sigma^2 & \qquad \sigma^{-570} &= \sigma^{12(-48)+6} = \sigma^6 \\ \sigma^{1195} &= \sigma^{12(99)+7} = \sigma^7 & \qquad \sigma^{-1211} &= \sigma^{12(-101)+1} = \sigma^1 \end{aligned}$$

■

Exercise 2.3.15

Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Solution. Observe that $\mathbb{Z} \times \mathbb{Z} \leq \mathbb{Q} \times \mathbb{Q}$. By Theorem 2.7, $\mathbb{Z} \times \mathbb{Z}$ would have to be cyclic if $\mathbb{Q} \times \mathbb{Q}$ were cyclic, contradicting Exercise 2.3.12(c). ■

Exercise 2.3.16

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 if x and y do *not* commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Solution. Put $\ell = \operatorname{lcm}(m, n)$ and write $\ell = am = bn$ for some $a, b \in \mathbb{Z}$. Then

$$(xy)^\ell = x^\ell y^\ell = x^{bn} y^{am} = 1 \cdot 1 = 1.$$

By Proposition 2.3, $|xy|$ divides ℓ. This need not hold if x and y do not commute. For example, consider $x = rs$ and $y = s$ in D_8. Then $|xy| = |rss| = 4$, but $\operatorname{lcm}(|x|, |y|) = \operatorname{lcm}(2, 2) = 2$. Moreover, if $|x| = 2$ and $y = x$, then $|xy| = |x^2| = 1$, but $\operatorname{lcm}(|x|, |y|) = \operatorname{lcm}(2, 2) = 2$. ■

Exercise 2.3.17

Find a presentation for Z_n with one generator.

Solution. $Z_n = \langle x \mid x^n = 1 \rangle$. ■

Exercise 2.3.18

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. Consider the map $\varphi \colon Z_n \to H$ defined by $\varphi(x^k) = h^k$ for all $k \in \mathbb{Z}$ so that $\varphi(x) = h$. Suppose $x^a = x^b$ for some $a, b \in \mathbb{Z}$, so $x^{a-b} = 1$. By Propositions 2.2 and 2.3, $|x| = n \mid (a - b)$, so $a - b = cn$ for some $c \in \mathbb{Z}$. Therefore,

$$\varphi(x^a) = h^a = h^{b+cn} = h^b (h^n)^c = h^b \cdot 1 = h^b = \varphi(x^b),$$

and thus φ is well defined. Additionally,

$$\varphi(x^a x^b) = \varphi(x^{a+b}) = h^{a+b} = h^a h^b = \varphi(x^a)\varphi(x^b),$$

and hence φ is a homomorphism. Finally, if $\psi \colon Z_n \to H$ is another homomorphism such that $\psi(x) = h$, then by Exercise 1.6.1, $\psi(x^k) = \psi(x)^k = h^k = \varphi(x^k)$ for all $k \in \mathbb{Z}$, so $\psi = \varphi$. ■

Exercise 2.3.19

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. Consider the map $\varphi \colon \mathbb{Z} \to H$ defined by $\varphi(n) = h^n$ for all $n \in \mathbb{Z}$ so that $\varphi(1) = h$. The argument follows similarly to that of Exercise 2.3.18 without the well-definedness check, since φ acts directly on the elements of $\mathbb{Z}$. ■

Exercise 2.3.20

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. By Proposition 2.3, $|x| \mid p^n$. Since p is prime, $|x| = p^m$ for some $m \leq n$. ∎

Exercise 2.3.21

Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution. For $n = 1$, $1 + p \equiv 1 \pmod{p}$, so the order is $1 = p^0$. Now assume $n \geq 2$. Using the notation and additivity fact of $v_p(\cdot)$ from Exercise 0.2.8, let $m \geq 0$ and $2 \leq k \leq p^m$. We claim that $v_p(\binom{p^m}{k} p^k) \geq m + 2$. Indeed, by Exercise 0.2.8,

$$v_p(k!) = \sum_{i \geq 1} \left\lfloor \frac{k}{p^i} \right\rfloor < \sum_{i \geq 1} \frac{k}{p^i} = \frac{k}{p-1} \leq \frac{k}{2},$$

where the last inequality uses the oddness of p, so $p - 1 \geq 2$. In particular, $v_p(k!) < \frac{k}{2}$ gives $v_p(k!) \leq \lceil \frac{k}{2} \rceil - 1 \leq k - 2$. Thus,

$$v_p\left(\binom{p^m}{k} p^k\right) = v_p(p^m(p^m - 1)\cdots(p^m - k + 1)) - v_p(k!) + k \geq m - (k-2) + k = m + 2.$$

By the Binomial Theorem,

$$(1+p)^{p^m} = \sum_{k=0}^{p^m} \binom{p^m}{k} p^k = 1 + p^{m+1} + \sum_{k=2}^{p^m} \binom{p^m}{k} p^k \equiv 1 + p^{m+1} \pmod{p^{m+2}}.$$

Taking $m = n-1$, we get $(1+p)^{p^{n-1}} \equiv 1 + p^n \equiv 1 \pmod{p^n}$. Taking $m = n-2$, we get $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}$, since $0 < p^{n-1} < p^n$. By Proposition 2.3, $|1+p| \mid p^{n-1}$. Since $|1+p| \nmid p^{n-2}$, we must have $|1+p| = p^{n-1}$. ∎

Exercise 2.3.22

Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1 + 2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ but $(1 + 2^2)^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution. We claim for $m \geq 0$ and $2 \leq k \leq 2^m$ that $v_2(\binom{2^m}{k} 2^{2k}) \geq m + 3$, where we again use the notation and additivity fact of $v_2(\cdot)$ from Exercise 0.2.8. Indeed, by Exercise 0.2.8,

$$v_2(k!) = \sum_{i \geq 1} \left\lfloor \frac{k}{2^i} \right\rfloor < \sum_{i \geq 1} \frac{k}{2^i} = k,$$

so $v_2(k!) \leq k - 1$. Thus,

$$v_2\left(\binom{2^m}{k} 2^{2k}\right) = v_2(2^m(2^m - 1)\cdots(2^m - k + 1)) - v_2(k!) + 2k \geq m - (k-1) + 2k = m + k + 1 \geq m + 3.$$

Now, using the Binomial Theorem,

$$(1 + 2^2)^{2^m} = \sum_{k=0}^{2^m} \binom{2^m}{k} 2^{2k} = 1 + 2^{m+2} + \sum_{k=2}^{2^m} \binom{2^m}{k} 2^{2k} \equiv 1 + 2^{m+2} \pmod{2^{m+3}}.$$

Taking $m = n-2$, we get $(1+2^2)^{2^{n-2}} \equiv 1 + 2^n \equiv 1 \pmod{2^n}$. Taking $m = n-3$, we get $(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \not\equiv 1 \pmod{2^n}$, since $0 < 2^{n-1} < 2^n$. By Proposition 2.3, $|5| \mid 2^{n-2}$. Since $|5| \nmid 2^{n-3}$, we must have $|5| = 2^{n-2}$. ∎

Exercise 2.3.23

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. If $(\mathbb{Z}/2^n\mathbb{Z})^\times$ were cyclic, it would have a unique subgroup of order 2 by Theorem 2.7. However,

$$(2^n-1)^2 \equiv (-1)^2 \equiv 1 \pmod{2^n}, \quad \text{and} \quad (2^{n-1}+1)^2 = 2^{2n-2}+2^n+1 \equiv 1 \pmod{2^n}.$$

Since $2 < 2^{n-1}+1 < 2^n-1 < 2^n$, the elements 2^n-1 and $2^{n-1}+1$ are distinct nonidentity elements of order 2, contradicting the uniqueness of the subgroup of order 2. Therefore, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ cannot be cyclic for any $n \geq 3$. ■

Exercise 2.3.24

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 $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x\rangle g^{-1} \leq \langle x\rangle$. If x has order n, show the elements $gx^ig^{-1}, i = 0, 1, \ldots, n-1$ 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 computing 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) If $g \in N_G(\langle x\rangle)$, then $g\langle x\rangle g^{-1} = \langle x\rangle$. In particular, $gxg^{-1} \in \langle x\rangle$, so there exists some $a \in \mathbb{Z}$ such that $gxg^{-1} = x^a$.
(b) Suppose $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. We show that $gx^kg^{-1} = x^{ak}$ for any integer k. If $k = 0$, then $gx^0g^{-1} = gg^{-1} = 1 = x^{a\cdot 0}$. Proceeding by induction on k, the base case $k = 1$ is immediate. If it holds for some $k \geq 1$, then

$$gx^{k+1}g^{-1} = gx^kg^{-1}gxg^{-1} = x^{ak}x^a = x^{a(k+1)}.$$

Moreover, for $k > 0$, we have

$$gx^{-k}g^{-1} = (gx^kg^{-1})^{-1} = (x^{ak})^{-1} = x^{-ak},$$

so $gx^kg^{-1} = x^{ak}$ for all integers k, and hence $g\langle x\rangle g^{-1} \subseteq \langle x\rangle$. Now let $|x| = n$, and suppose $gx^ig^{-1} = gx^jg^{-1}$ for some $0 \leq i < j \leq n-1$. Cancellation gives $x^i = x^j$, contradicting Proposition 2.2(1). Therefore, the elements gx^ig^{-1} for $i = 0, 1, \ldots, n-1$ are distinct, wherefore $|g\langle x\rangle g^{-1}| = n = |\langle x\rangle|$ and $g\langle x\rangle g^{-1} = \langle x\rangle$. Hence, $g \in N_G(\langle x\rangle)$. ■

Exercise 2.3.25

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 (Exercise 1.7.19) to prove 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. Let $G = \langle g\rangle$ for some $g \in G$. By Proposition 2.6(2), $G = \langle g^k\rangle$, so every $y \in G$ can be written as $y = (g^k)^m = (g^m)^k$ for some integer m, and therefore y is a kth power in G.

Let G be a finite group of order n. Let $y \in G$ where $|\langle y\rangle| = \ell$. By Lagrange's Theorem, $\ell \mid n$, so $(k, \ell) = 1$ as well. By the previous part, there exists $z \in \langle y\rangle$ such that $z^k = y$, so y is a kth power in G. ■

Exercise 2.3.26

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 (automorphisms were introduced in Exercise 1.6.20).
(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.
(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 $\bar{a} \mapsto \sigma_a$ 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. Let $Z_n = \langle z\rangle$ for some $z \in Z_n$.

(a) $\boxed{\Rightarrow}$ Suppose $\sigma_a \in \mathrm{Aut}(Z_n)$ and let $d = (n, a)$ with $n = ds$ and $a = dt$ for some integers s and t. We have

$$\sigma_a(z^s) = (z^s)^a = z^{as} = z^{dts} = z^{nt} = 1.$$

Injectivity of σ_a gives $z^s = 1$, so $n \mid s$, forcing $s = n$ and $d = 1$.
$\boxed{\Leftarrow}$ Suppose $(a, n) = 1$. By Exercise 2.3.25, σ_a is surjective. Since Z_n is finite, σ_a is bijective. Moreover, for any $x, y \in Z_n$, we have

$$\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y),$$

where we used the fact that Z_n is abelian in the second equality. Therefore, σ_a is an automorphism of Z_n.

(b) Observe that every σ_c is a homomorphism of Z_n since Z_n is abelian, so

$$\sigma_a = \sigma_b \iff z^a = z^b \iff n \mid (a - b) \iff a \equiv b \pmod{n}.$$

(c) Let $\alpha \in \mathrm{Aut}(Z_n)$. Since Z_n is cyclic, there exists $k \in \mathbb{Z}$ such that $\alpha(z) = z^k$. Then for any integer m, we have $\alpha(z^m) = (z^k)^m = z^{km}$. Therefore, $\alpha = \sigma_k$.

(d) For any $a, b \in \mathbb{Z}$, we have

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x)$$

for all $x \in Z_n$, so $\sigma_a \circ \sigma_b = \sigma_{ab}$.

Define the map

$$\beta \colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n) \quad \text{by} \quad \beta(\bar{a}) = \sigma_a.$$

By definition, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ gives $(a, n) = 1$, so $\sigma_a \in \mathrm{Aut}(Z_n)$ by the backward direction of part (a). If $\bar{a} = \bar{b}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, then $\sigma_a = \sigma_b$ by the backward direction of part (b), so β is well defined. By the forward direction of part (b), $\sigma_a = \sigma_b$ implies $\bar{a} = \bar{b}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, so β is injective. By part (c), every automorphism of Z_n is of the form σ_a for some a, and $(a, n) = 1$ by the forward direction of part (a), so $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and β is surjective. Finally, $\beta(\overline{ab}) = \sigma_{ab} = \sigma_a \circ \sigma_b = \beta(\bar{a}) \circ \beta(\bar{b})$, so β is a homomorphism. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian with order $\varphi(n)$ and $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(Z_n)$ via β, it follows that $\mathrm{Aut}(Z_n)$ is abelian with order $\varphi(n)$. ■

2.4 Subgroups Generated by Subsets of a Group

Exercise 2.4.1

Prove that if H is a subgroup of G then $\langle H \rangle = H$.

Solution. By definition, $\langle H \rangle$ is the intersection of all subgroups of G that contain H, so $H \subseteq \langle H \rangle$. Since $H \leq G$ and $H \subseteq H$, we have $\langle H \rangle \subseteq H$, whence $\langle H \rangle = H$. ■

Exercise 2.4.2

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. Since $B \subseteq \langle B \rangle$ and $A \subseteq B$, we have $A \subseteq \langle B \rangle$. The minimality of $\langle A \rangle$ then yields $\langle A \rangle \leq \langle B \rangle$.
Take $G = \mathbb{Z}$ with $A = \{1\}$ and $B = \{1, 2\}$. Then $A \subseteq B$ with $A \neq B$, but $\langle A \rangle = \langle B \rangle = \mathbb{Z}$. ■

Exercise 2.4.3

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 $x, y \in \langle H, Z(G) \rangle$. By Proposition 2.9, write x and y as

$$x = x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}, \quad y = y_1^{\delta_1} \cdots y_n^{\delta_n},$$

where $\varepsilon_i, \delta_j \in \{\pm 1\}$ and $x_i, y_j \in H \cup Z(G)$ for all i and j. Because elements of H commute amongst themselves, elements of $Z(G)$ commute with every element of G, and both H and $Z(G)$ are closed under inverses, we obtain

$$xy = x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m} y_1^{\delta_1} \cdots y_n^{\delta_n} = y_1^{\delta_1} \cdots y_n^{\delta_n} x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m} = yx,$$

and thus $\langle H, Z(G) \rangle$ is abelian.
For the explicit example, put $G = D_8$ with $H = 1$. Then $C_G(H) = G$, but $\langle H, C_G(H) \rangle = G$, which is non-abelian. ■

Exercise 2.4.4

Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Solution. Let $K = H - \{1\}$. Every nonidentity element in H belongs to $K \subseteq \langle K \rangle$, and $1 \in \langle K \rangle$ because $\langle K \rangle \leq G$, so $H \subseteq \langle K \rangle$. By Exercise 2.4.2, Exercise 2.4.1, and $K \subseteq H$, we have $\langle K \rangle \subseteq \langle H \rangle = H$, so $H = \langle K \rangle$. ■

Exercise 2.4.5

Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Solution. Observe that the elements of order 2 in S_3 are exactly its three 2-cycles. Any two distinct 2-cycles $\sigma, \tau \in S_3$ share exactly one point, so $\sigma\tau$ is a 3-cycle. Thus, $\langle \sigma, \tau \rangle$ contains $\langle \sigma\tau \rangle$, along with σ, τ, and $\sigma\tau\sigma$ (which is the third 2-cycle). These are six distinct elements, so $\langle \sigma, \tau \rangle = S_3$. ■

Exercise 2.4.6

Prove that the subgroup of S_4 generated by (1 2) and (1 2)(3 4) is a noncyclic group of order 4.

Solution. Put $\sigma = (1\,2)$ and $\tau = (3\,4)$. Since $\tau = \sigma(\sigma\tau)$ and $\sigma\tau \in \langle \sigma, \tau \rangle$, we have $\langle \sigma, \sigma\tau \rangle = \langle \sigma, \tau \rangle$. Additionally, σ and τ are disjoint 2-cycles, so they commute. Moreover, $|\sigma| = |\tau| = 2$, so $\langle \sigma, \tau \rangle = \{\sigma^i \tau^j \mid i, j \in \{0, 1\}\} = \{1, \sigma, \tau, \sigma\tau\}$. Since $|\langle \sigma, \tau \rangle| = 4$ and it has no element of order 4, it is not cyclic. ■

Exercise 2.4.7

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 $\sigma = (1\ 2)$ and $\tau = (1\ 3)(2\ 4)$, and let $\rho = \sigma\tau$. Because $\rho = \sigma\tau$ and $\tau = \sigma\rho$, we have $\langle \sigma, \rho \rangle = \langle \sigma, \tau \rangle$. Note that $|\sigma| = |\tau| = 2$ and $|\rho| = 4$. Using Exercise 1.2.6 with $x = \sigma$ and $y = \tau$, there exists a surjective homomorphism $\varphi : D_8 \to \langle \sigma, \rho \rangle$ with $r \mapsto \rho$ and $s \mapsto \sigma$. Since φ is surjective, $|\langle \sigma, \rho \rangle| \leq 8$. Moreover, $\langle \rho \rangle \leq \langle \sigma, \rho \rangle$ and $\sigma \notin \langle \rho \rangle$. Because the elements $\sigma\rho^i$ for $i = 0, 1, 2, 3$ are all distinct by cancellation and in $\langle \sigma, \rho \rangle$, we have $|\langle \sigma, \rho \rangle| \geq 8$, so $|\langle \sigma, \rho \rangle| = 8$ and φ is an isomorphism. ■

Exercise 2.4.8

Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$.

Solution. Let $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (1\ 2\ 4\ 3)$. Observe that $\sigma\tau = (1\ 3\ 2) \in \langle \sigma, \tau \rangle$. Moreover, $\sigma^2 = (1\ 3)(2\ 4)$ and $\sigma^3\tau\sigma^3 = (1\ 2)$, so $\langle \sigma, \tau \rangle$ contains a subgroup of order 8 by Exercise 2.4.7. By Lagrange's Theorem, $\operatorname{lcm}(8, 3) \mid |\langle \sigma, \tau \rangle|$, so $S_4 = \langle \sigma, \tau \rangle$. ■

Exercise 2.4.9

Prove that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

[Recall from Exercise 2.1.9 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 and B be the two matrices given in the exercise. Note that $\langle A, B \rangle \leq \mathrm{SL}_2(\mathbb{F}_3)$. Consider the 12 distinct matrices in $\langle A, B \rangle$ along with I_2:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
$$B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$
$$(AB)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad ABA^2 = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix} \quad A^2B = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$$
$$B^2A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \quad ABA = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \quad BAB = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

Since $|\langle A, B \rangle| > 12$, $\langle A, B \rangle \leq \mathrm{SL}_2(\mathbb{F}_3)$, and $|\langle A, B \rangle| \mid |\mathrm{SL}_2(\mathbb{F}_3)| = 24$ by Lagrange's Theorem, $|\langle A, B \rangle| = 24$, so $\langle A, B \rangle = \mathrm{SL}_2(\mathbb{F}_3)$. ■

Exercise 2.4.10

Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]

Solution. Let A and B be the matrices given in the exercise. Direct computation gives $A^4 = I_2$ and $A^2 = B^2 = (AB)^2 = -I_2$, which are exactly the relations given in Exercise 1.5.3 for Q_8. Therefore, there exists a surjective homomorphism $\varphi : Q_8 \to \langle A, B \rangle$ defined by $i \mapsto A$ and $j \mapsto B$, where surjectivity yields $|\langle A, B \rangle| \leq 8$. Because $A^2 = -I_2$ and $A^4 = I_2$, we have $|A| = 4$, so $\langle A \rangle = \{I_2, A, -I_2, -A\}$, which doesn't contain B. By Lagrange's Theorem, $4 \mid |\langle A, B \rangle|$ and $4 < |\langle A, B \rangle| \leq 8$, so $|\langle A, B \rangle| = 8$. Thus, $\langle A, B \rangle \cong Q_8$. ■

Exercise 2.4.11

Show that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Solution. Note that $|S_4| = 24$ and Exercise 2.4.9 assumes $|\mathrm{SL}_2(\mathbb{F}_3)| = 24$. Suppose

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_3)$$

has order 2. Then $\det A = 1$ and $A^2 = I_2$, giving the equations

$$\begin{cases} 1 = ad - bc \\ 1 = a^2 + bc \\ 0 = ab + bd \\ 0 = ac + cd. \end{cases}$$

Suppose $a + d \neq 0$. Then $b = c = 0$, which gives $1 = ad$, so $a = d = \pm 1$, and $A = \pm I_2$. If $a + d = 0$, then $a = -d = 2d$ in $\mathbb{F}_3$. This yields $1 = 2d^2 - bc$ and $1 = (2d)^2 + bc = d^2 + bc$. Adding these two equations yields $2 = 3d^2 = 0$ in $\mathbb{F}_3$, which is a contradiction. Therefore, the only element of order 2 is $-I_2$, while (1 2) and (1 3) are two elements of order 2 in S_4, so $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are not isomorphic. ■

Exercise 2.4.12

Prove that the subgroup of upper triangular matrices in $\mathrm{GL}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8 (cf. Exercise 2.1.16). [First find the order of this subgroup.]

Solution. Any matrix in $\mathrm{UT}_3(\mathbb{F}_2)$ must have nonzero determinant. Since an upper triangular matrix's determinant is the product of its diagonal entries, it must have 1's on the diagonal, so $\mathrm{UT}_3(\mathbb{F}_2) = H(\mathbb{Z}/2\mathbb{Z})$. By Exercise 1.4.11(c), $|\mathrm{UT}_3(\mathbb{F}_2)| = 8$. Put $A = (1, 0, 1)$ and $B = (1, 0, 0)$. By Exercise 1.4.11(b) and (d), $A^{-1} = (1, 1, 1)$, $|A| = 4$, and $|B| = 2$. Direct computation gives $AB = BA^{-1}$ and

$$A^2 = (0, 1, 0), \quad BA = (0, 1, 1), \quad BA^2 = (1, 1, 0), \quad BA^3 = (0, 0, 1).$$

Along with I_3, A, A^{-1}, and B, there are 8 distinct elements in $\langle A, B\rangle \leq \mathrm{UT}_3(\mathbb{F}_2)$. Because $|\mathrm{UT}_3(\mathbb{F}_2)| = 8$, we have $\langle A, B\rangle = \mathrm{UT}_3(\mathbb{F}_2)$. Given that A and B satisfy the relations of D_8, there exists a surjective homomorphism $\varphi : D_8 \to \mathrm{UT}_3(\mathbb{F}_2)$ with $r \mapsto A$ and $s \mapsto B$. Since $|\mathrm{UT}_3(\mathbb{F}_2)| = 8 = |D_8|$, φ is an isomorphism. ■

Exercise 2.4.13

Prove that the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.

Solution. Let P be the set in question and let $\mathbb{Q}_+^\times$ be the multiplicative group of positive rational numbers. By definition, $\langle P\rangle \leq \mathbb{Q}_+^\times$. For any prime p, we have $(1/p)^{-1} = p \in \langle P\rangle$, so $p^k \in \langle P\rangle$ for any integer k. Let $q \in \mathbb{Q}_+^\times$ with $q = m/n$ for some $m, n \in \mathbb{Z}^+$. By the Fundamental Theorem of Arithmetic, m and n can be written as products of primes. Hence, $q = m/n$ can be expressed as a product of powers of primes, all of which are in $\langle P\rangle$. Therefore, $q \in \langle P\rangle$, so $\mathbb{Q}_+^\times \leq \langle P\rangle$, and thus $\mathbb{Q}_+^\times = \langle P\rangle$. ■

Exercise 2.4.14

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 $H \leq \langle \frac{1}{k}\rangle$, where k is the product of all the denominators which appear in a set of generators for H.]
(d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution.

(a) Let G be a finite group. Since G is a subgroup containing itself, $G = \langle G\rangle$.
(b) $\mathbb{Z} = \langle 1\rangle$.

(c) Let $H = \langle A \rangle$, where

$$A = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n} \right\}.$$

Define the quantities

$$k = \prod_{i=1}^{n} q_i, \quad k_j = \frac{k}{q_j}.$$

Observe that $p_j/q_j = p_j k_j / k \in \langle \frac{1}{k} \rangle$ for each j, so $A \subseteq \langle 1/k \rangle$. By minimality, $H = \langle A \rangle \leq \langle 1/k \rangle$. By Theorem 2.7(1), every subgroup of a cyclic group is cyclic, so H is cyclic.

(d) For any $p/q \in \mathbb{Q}$ and for every $n \in \mathbb{Z}$, $2q \cdot np/q = 2np$ is even, so $np/q \neq 1/(2q)$. Therefore, $1/(2q) \notin \langle p/q \rangle$, which implies that $\mathbb{Q}$ is not cyclic. By the contrapositive of part (c), $\mathbb{Q}$ is not finitely generated. ■

Exercise 2.4.15

Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Solution. Consider the set

$$A = \left\{ \frac{1}{2^k} \,\middle|\, k \in \mathbb{Z}^+ \cup \{0\} \right\}.$$

Each element of $\langle A \rangle$ is a $\mathbb{Z}$-combination of the $1/2^k$ for $k \in \mathbb{Z}^+ \cup \{0\}$, so every element of $\langle A \rangle$ is of the form $m/2^k$ for some $m \in \mathbb{Z}$ and $k \geq 0$. If $m/2^k = 1/3$, then $3m = 2^k$, which is impossible, so $1/3 \notin \langle A \rangle$, wherefore $\langle A \rangle < \mathbb{Q}$. Moreover, for every $m/2^k \in \langle A \rangle$, we have $1/2^{k+1} \in \langle A \rangle$. Because $n \cdot m/2^k = 1/2^{k+1}$ yields $2nm = 1$, which is impossible for $n, m \in \mathbb{Z}$, we see that $1/2^{k+1} \notin \langle m/2^k \rangle$, and therefore $\langle A \rangle$ cannot be cyclic. ■

Exercise 2.4.16: Maximal Subgroups

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 $H = \langle x^p \rangle$ for some prime p dividing n.

Solution.

(a) Observe that the set of proper subgroups containing H is nonempty and finite. Take M to have maximal order in this set. If $M \leq K < G$, then K is in the set of proper subgroups containing H with $|K| \leq |M|$, so $|K| = |M|$, whence $K = M$. Therefore, M is maximal.

(b) Let $G = D_{2n} = \langle r, s \rangle$. Because $s \notin \langle r \rangle$, $\langle r \rangle < G$. Let $\langle r \rangle < H \leq G$. Then H contains some sr^k for $0 \leq k < n$, so $s = sr^k r^{n-k} \in H$. Therefore, $H = G$, and $\langle r \rangle$ is maximal.

(c) $\boxed{\Rightarrow}$ Suppose H is maximal. By Theorem 2.7(1) and (3), $H = \langle x^d \rangle$ for some $d \mid n$. Since $H \neq G$, $d > 1$ by Proposition 2.6(2). Let p be a prime such that $p \mid d$. By Proposition 2.6(2), $(p, n) = p$ gives $\langle x^p \rangle < G$. Because $p \mid d$, $H \leq \langle x^p \rangle$, whereby maximality of H forces $H = \langle x^p \rangle$. By Theorem 2.7(3), $d = p$.
$\boxed{\Leftarrow}$ Suppose that $H = \langle x^p \rangle$ for some prime $p \mid n$. Since $(p, n) = p$, Proposition 2.6(2) gives $H \neq G$. Suppose $H \leq K \leq G$ for some subgroup K. Then $K = \langle x^d \rangle$ for some $d \mid n$ by Theorem 2.7(1) and (3). Since $H \leq K$, we have $d \mid p$. Primality of p gives $d = 1$ or $d = p$, so $K = G$ or $K = H$, whence H is maximal. ■

Exercise 2.4.17

This is an exercise involving Zorn's Lemma (see Appendix I) to 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 $\mathcal{C}$ be a chain in $\mathcal{S}$.

(a) Prove that the union, H, of all the subgroups in $\mathcal{C}$ is a subgroup of G.

(b) Prove that H is a *proper* subgroup. [If not, each g_i must lie in H and so must lie in some element of the chain $\mathcal{C}$. Use the definition of a chain to arrive at a contradiction.]

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Solution. For parts (a) and (b), assume $\mathcal{C} \neq \emptyset$.

(a) Since $1 \in K$ for every $K \in \mathcal{C}$, we have $1 \in H$. Suppose $g, h \in H$. Then $g \in K_1$ and $h \in K_2$ for some $K_1, K_2 \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, either $K_1 \leq K_2$ or $K_2 \leq K_1$. Without loss of generality, suppose $K_1 \leq K_2$. Then $g \in K_2$ as well, so $gh^{-1} \in K_2 \subseteq H$, and therefore $H \leq G$.

(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 $1 \leq i \leq n$. The set $\{K_1, \ldots, K_n\}$ is a finite totally ordered set under inclusion, so it has a largest element K that contains all generators g_i. Therefore, $K = G$, contradicting that $\mathcal{C}$ consists of proper subgroups of G.

(c) Because G is nontrivial, $1 \in \mathcal{S}$ so that $\mathcal{S}$ is nonempty. If $\mathcal{C} = \emptyset$, then 1 is an upper bound for $\mathcal{C}$. Otherwise, $H \in \mathcal{S}$ by parts (a) and (b), and for any $K \in \mathcal{C}$, we have $K \leq H$ so that H is an upper bound for $\mathcal{C}$. Then every chain in $\mathcal{S}$ has an upper bound, so by Zorn's Lemma, $\mathcal{S}$ must have a maximal element. ■

Exercise 2.4.18: The Prüfer p-group

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 the following:

(a) $H_k \leq H_m$ if and only if $k \leq m$

(b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi i t/n} \mid t = 0, 1, \ldots, n-1\}$ is the set of all n^{th} roots of 1 in $\mathbb{C}$)

(c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every proper subgroup of Z is finite and cyclic)

(d) Z is not finitely generated.

Manual Remark. *This group is known as the Prüfer p-group, a prototypical example of an infinite abelian group that is not finitely generated.*

Solution. Extend the convention that $H_0 = 1$. Moreover, $|H_k| = p^k$ for all $k \geq 0$ as there are exactly p^k p^kth roots of unity.

(a) $\boxed{\Rightarrow}$ If $H_k \leq H_m$, then $p^k \mid p^m$ by Lagrange's Theorem, and thus $k \leq m$.
$\boxed{\Leftarrow}$ Suppose $k \leq m$, so $m - k \geq 0$. Then for any $z \in H_k$, we have

$$z^{p^m} = (z^{p^k})^{p^{m-k}} = 1$$

so that $z \in H_m$, and thus $H_k \leq H_m$.

(b) Let $\theta = e^{2\pi i/p^k}$. By part (a), $|H_k| = p^k = |\theta|$, and since $\langle\theta\rangle \subseteq H_k$, we have $\langle\theta\rangle = H_k$.

(c) Let H be a proper subgroup of Z. Note that every element in Z has order p^i for some $i \in \mathbb{Z}^+$. Define the set

$$S = \{n \in \mathbb{Z}^+ \mid |h| = p^n \text{ for some } h \in H\}.$$

Since $1 \in H$ has order p^0, $0 \in S$. If $n \in S$, then there exists $h \in H$ with $|h| = p^n$, so $\langle h\rangle \leq H_n$. Since $|\langle h\rangle| = p^n = |H_n|$, we have $\langle h\rangle = H_n \leq H$. Note that S must be finite, for otherwise

$$Z = \bigcup_{n \in S} H_n \subseteq H,$$

contradicting that $H \neq Z$. Put $s = \max S$.

We claim that $H = H_s$. Indeed, $H_s \leq H$ by the beginning observation. Conversely, let $h \in H$ with $|h| = p^k$. Then $k \in S$ and $k \leq s$, so by part (a), $H_k \leq H_s$. Since $h \in H_k$, we have $h \in H_s$. Therefore, $H \subseteq H_s$, so $H = H_s$. In particular, H is cyclic of order p^s by part (b).

(d) Suppose $Z = \langle z_1, z_2, \ldots, z_n\rangle$ for some $n \in \mathbb{Z}^+$. Let $|z_i| = p^{x_i}$ for some $x_i \in \mathbb{Z}^+$, and put $x = \max_i x_i$. Then $z_i \in H_x$ for every $1 \leq i \leq n$ so that $Z \leq H_x$. However, H_x is finite by the preliminary observation, while Z is infinite, contradicting the assumption that Z is finitely generated. ■

Exercise 2.4.19: Divisibility

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 $x^k = a$, i.e., each element has a kth root in A (in additive notation, each element is the kth multiple of some element of 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 $p/q \in \mathbb{Q}$ and let n be a nonzero integer. Then $n \cdot p/(qn) = p/q$, where $p/(qn) \in \mathbb{Q}$.

(b) Let G be finite abelian with $|G| = n$. If $G = 1$, then G cannot be divisible by definition. Otherwise, fix $g \in G$ with $g \neq 1$. By Lagrange's Theorem, $x^n = 1 \neq g$ for all $x \in G$, so G is not divisible. ■

Exercise 2.4.20

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 groups.

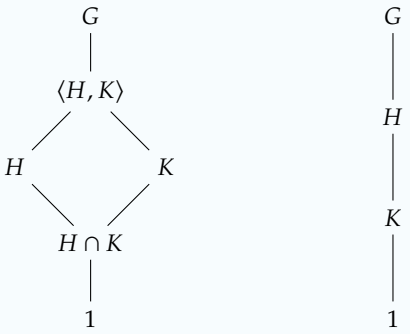
Solution. Since $A \neq 1$, $A \times B \neq 1$. For a fixed nonzero integer k and fixed $a \in A$ and $b \in B$, there exists $(c, d) \in A \times B$ such that $(c, d)^k = (c^k, d^k) = (a, b)$ if and only if there exist $c \in A$ and $d \in B$ such that $c^k = a$ and $d^k = b$. Quantifying over all nonzero integers k and all elements $a \in A$ and $b \in B$, we see that $A \times B$ is divisible if and only if both A and B are divisible. ■

2.5 The Lattice of Subgroups of a Group

Exercise 2.5.1

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 and neither is contained in the other, then the sublattice is a diamond shape. Otherwise, one of H or K is contained in the other, or they are equal, leading to a chain structure.



■

Exercise 2.5.2

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. Using the subgroup lattice of D_{16}, we find:
(a) $\langle sr^2, r^4\rangle, \langle sr^6\rangle, \langle sr^2\rangle, \langle r^4\rangle, 1$.
(b) $\langle sr^3, r^4\rangle, \langle r^4\rangle, \langle sr^3\rangle, \langle sr^7\rangle, 1$.
(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) $\langle s\rangle, \langle s, r^4\rangle, \langle s, r^2\rangle, D_{16}$. ■

Exercise 2.5.3

Show that the subgroup $\langle s, r^2\rangle$ of D_8 is isomorphic to V_4.

Solution. Note that $\langle s, r^2\rangle = \{1, s, r^2, sr^2\}$. Consider the mapping $\varphi\colon V_4 \to \langle s, r^2\rangle$ defined by

$$\varphi(1) = 1, \quad \varphi(a) = s, \quad \varphi(b) = r^2, \quad \varphi(c) = sr^2.$$

To see that φ is a homomorphism, we can check a pair of nonidentity elements, for example:

$$\varphi(a)\varphi(b) = s \cdot r^2 = sr^2 = \varphi(c) = \varphi(ab).$$

Similar checks for the other pairs show that φ preserves the group operation. Since $\langle s, r^2\rangle$ has order 4 and φ is surjective, it follows that φ is also injective, and hence an isomorphism. Therefore, $\langle s, r^2\rangle \cong V_4$. ■

Exercise 2.5.4

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:

$$\langle s, r\rangle, \langle s, r^3\rangle, \langle s, rs\rangle, \langle s, r^3s\rangle, \langle r^2s, r\rangle, \langle r^2s, r^3\rangle, \langle r^2s, rs\rangle, \langle r^2s, r^3s\rangle, \langle r, rs\rangle, \langle r^3, rs\rangle, \langle r, r^3s\rangle, \langle r^3, r^3s\rangle$$ ■

Exercise 2.5.5

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}: $x = r, r^3, r^5, r^7, sr, sr^3, sr^5, sr^7$. ■

Exercise 2.5.6

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 find $C_G(a)$ for some $a \in G$, we look for elements in $g \in G$ such that $g \notin \langle a\rangle$, but $ga = ag$, then look for the smallest subgroup containing both $\langle a\rangle$ and g.

$$\begin{aligned} C_{D_8}(1) &= D_8 & C_{D_8}(s) &= \langle s, r^2\rangle \\ C_{D_8}(r) &= \langle r\rangle & C_{D_8}(rs) &= \langle rs, r^2\rangle \\ C_{D_8}(r^2) &= D_8 & C_{D_8}(r^2s) &= \langle s, r^2\rangle \\ C_{D_8}(r^3) &= \langle r\rangle & C_{D_8}(r^3s) &= \langle sr, r^2\rangle \end{aligned}$$

(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) Note that no element of S_3 commutes with other elements, then $C_{S_3}(a) = \langle a\rangle$ for $a \in S_3 - \{1\}$.
(d) Use similar reasoning as in part (a) to obtain the centralizers:

$$\begin{aligned} C_{D_{16}}(1) = C_{D_{16}}(r^4) &= D_{16} \\ C_{D_{16}}(r^k) &= \langle r\rangle \text{ for all } k = 1, 2, 3, 5, 6, 7 \\ C_{D_{16}}(s) = C_{D_{16}}(sr^4) &= \langle s, r^4\rangle \\ C_{D_{16}}(sr) = C_{D_{16}}(sr^5) &= \langle sr^5, r^4\rangle \\ C_{D_{16}}(sr^2) = C_{D_{16}}(sr^6) &= \langle sr^2, r^4\rangle \\ C_{D_{16}}(sr^3) = C_{D_{16}}(sr^7) &= \langle sr^3, r^4\rangle \end{aligned}$$ ■

Exercise 2.5.7

Find the center of D_{16}.

Solution. $Z(D_{16}) = \{1, r^4\}$ by Exercise 2.2.7. ■

Exercise 2.5.8

In each of the following groups find the normalizer of each subgroup:
(a) S_3 (b) Q_8.

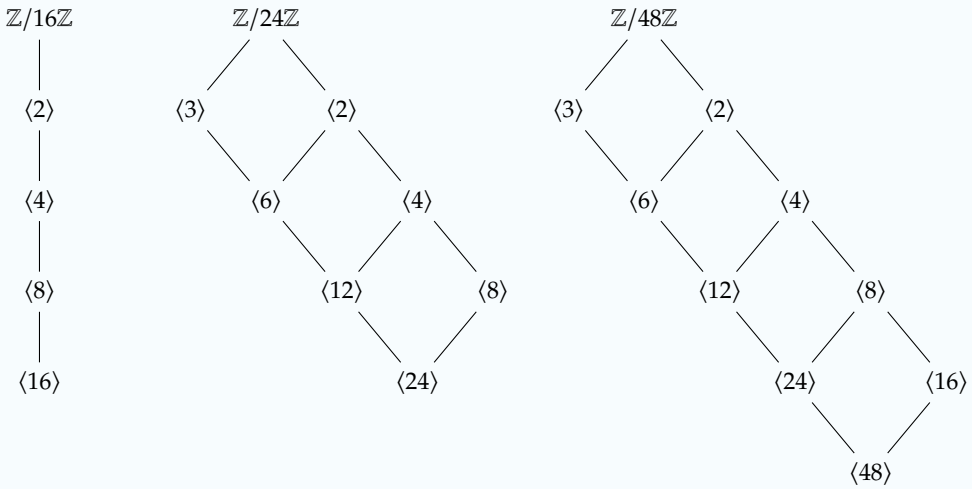
Solution.

(a) From the subgroup lattice of S_3, each nontrivial subgroup is cyclic and maximal. Then $N_{S_3}(\langle\alpha\rangle) = \langle\alpha\rangle$ or S_3. For any 2-cycle α, note that $\alpha\beta \neq \beta\alpha$ for any other 2-cycle β, hence $N_{S_3}(\langle\alpha\rangle) = \langle\alpha\rangle$. For the 3-cycle $\alpha = (1\ 2\ 3)$, any 2-cycle β satisfies $\beta\alpha\beta^{-1} \in \langle\alpha\rangle$, so $N_{S_3}(\langle\alpha\rangle) = S_3$.
(b) Since $Z(Q_8) = \langle -1\rangle$, $N_{Q_8}(\langle -1\rangle) = Q_8$. Similarly, $N_{Q_8}(\{1\}) = Q_8$. For the subgroups of order 4, note that $ji(-j) = -i$ and $j(-i)(-j) = i$, so that $j \in N_{Q_8}(\langle i\rangle)$. Then $N_{Q_8}(\langle i\rangle) = Q_8$. By symmetry, the same holds for $\langle j\rangle$ and $\langle k\rangle$. ■

Exercise 2.5.9

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.



■

Exercise 2.5.10

Classify groups of order 4 by proving that if $|G| = 4$, then $G \cong Z_4$ or $G \cong V_4$. [cf. Exercise 1.1.36.]

Solution. Let $G = \{1, a, b, c\}$. If G has an element of order 4, then $G \cong Z_4$ by Theorem 2.4.

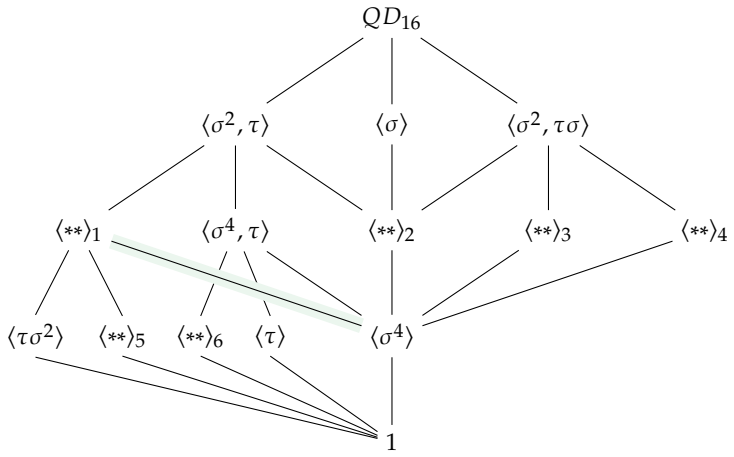
Suppose G is not cyclic. Then every nonidentity element has order 2 by Lagrange's Theorem. In particular, $a^2 = b^2 = c^2 = 1$. Note that $ab \neq 1$, since otherwise $b = a^{-1} = a$. Similarly, $ab \neq a$ and $ab \neq b$, so that $ab = c$. By similar reasoning, we have $bc = a$ and $ca = b$. This is precisely the definition of V_4, so that $G \cong V_4$. ■

Exercise 2.5.11

Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

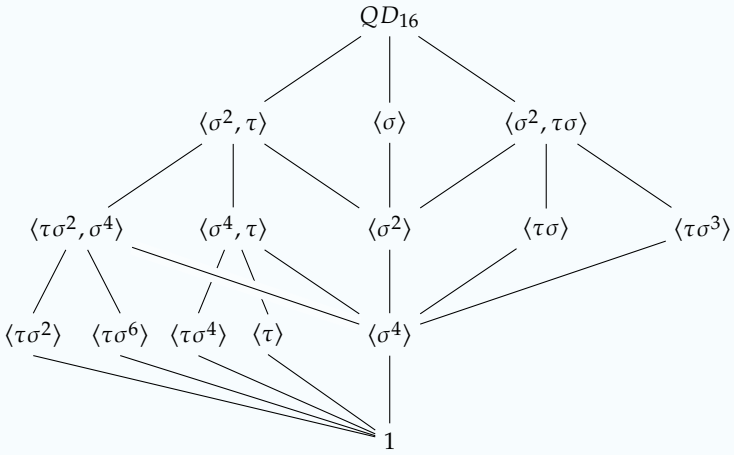
(called the **quasidihedral** or **semidihedral** group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8, \langle \sigma \rangle \cong Z_8$, and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$, and every proper subgroup is contained in one of these three 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. The above has had subscripts added to distinguish the unknown subgroups. It is clear that $\langle ** \rangle_2$ must be $\langle \sigma^2 \rangle$ since it is the only subgroup contained in both $\langle \sigma \rangle$ and $\langle \sigma^2, \tau \rangle$. To find the other subgroups, we calculate the cyclic subgroups of the form $\langle \tau\sigma^k \rangle$:

$$\langle \tau\sigma \rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\} \qquad \langle \tau\sigma^3 \rangle = \{1, \tau\sigma^3, \sigma^4, \tau\sigma^7\}$$
$$\langle \tau\sigma^4 \rangle = \{1, \tau\sigma^4\} \qquad \langle \tau\sigma^6 \rangle = \{1, \tau\sigma^6\}$$

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



■

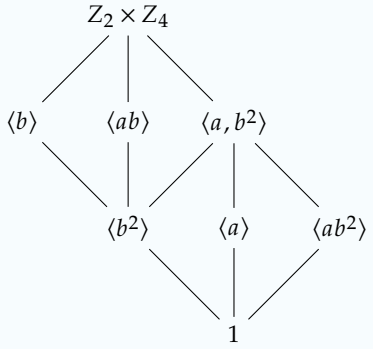
Exercise 2.5.12

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. Since A is the direct product of two abelian groups, it itself is abelian, and we may write:

$$A = \{1, b, b^2, b^3, a, ab, ab^2, ab^3\}$$

Using the isomorphisms given, we construct the lattice.

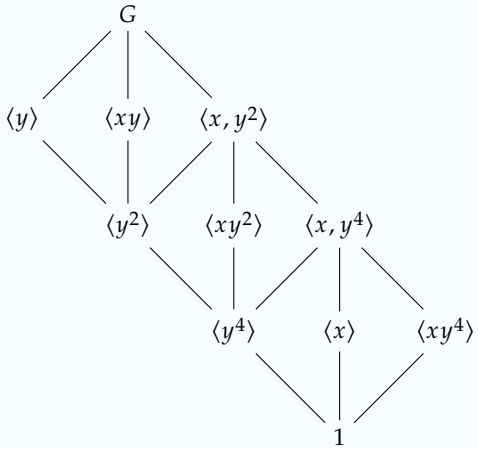


■

Exercise 2.5.13

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 2.5.12).

Solution. Put $x = a$ and $y^2 = b$, where $\langle a, b \rangle$ is Exercise 2.5.12. Then G contains a copy of $Z_2 \times Z_4$, with the necessary appending of $\langle y \rangle$ and $\langle xy \rangle$ to the lattice:



■

Exercise 2.5.14

Let M be the **modular group** of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle.$$

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 2.5.13) but that these two groups are not isomorphic.

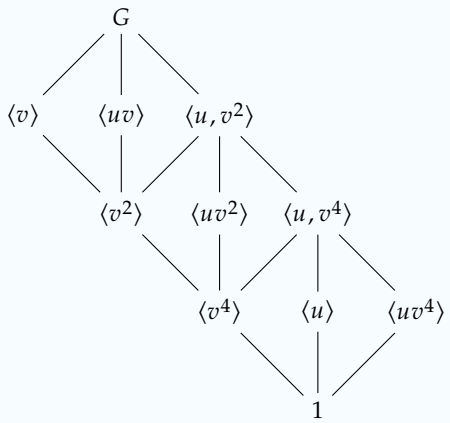
Solution. Since $|v| = |uv| = 8$, $\langle v \rangle \cong \langle uv \rangle \cong Z_8$. One can apply the second relation to obtain $v^2u = uv^2$, hence we deduce that $\langle u, v^2 \rangle$ is abelian. We may write

$$\langle u, v^2 \rangle = \{1, v^2, v^4, v^6, u, uv^2, uv^4, uv^6\}$$

From the enumeration of $\langle u, v^2 \rangle$, we have the map $\varphi \colon Z_2 \times Z_4 \to \langle u, v^2 \rangle$ defined by

$$\varphi(a) = u, \quad \varphi(b) = v^2.$$

This extends to a homomorphism. Moreover, $|\langle u, v^2 \rangle| = |Z_2 \times Z_4| = 8$. Since φ sends distinct elements of $Z_2 \times Z_4$ to distinct elements of $\langle u, v^2 \rangle$, it is injective. Being a homomorphism between two groups of the same finite order, it is also surjective, hence an isomorphism. We have the following lattice for M:



Since $vu = uv^5 \neq uv$, M is not abelian, and therefore cannot be isomorphic to $Z_2 \times Z_8$. ■

Exercise 2.5.15

Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

Solution. From $|r| = 8$, we deduce $\langle r \rangle \cong Z_8$. The remaining subgroups $\langle s, r^2 \rangle$ and $\langle sr, r^2 \rangle$ can be shown to be isomorphic to D_8 as follows:

- For the subgroup $\langle s, r^2 \rangle$, observe that $(r^2)^4 = s^2 = 1$, and $sr^2 = r^6 s = (r^2)^{-1} s$. Use r^2 in place of r and s in place of s to see that the relations match those of D_8.
- For the subgroup $\langle sr, r^2 \rangle$, observe that $(r^2)^4 = (sr)^2 = 1$, and

  $$(sr)r^2 = sr^3 = r^5 s = r^6 r^7 s = (r^2)^{-1}(sr).$$

  Use r^2 in place of r and sr in place of s to see that the relations match those of D_8. ■

Exercise 2.5.16

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 2.5.11).

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. ■

Exercise 2.5.17

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 2.5.14).

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, $\langle u, v^4 \rangle \cong V_4$. ■

Exercise 2.5.18

Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 2.5.11).

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

$$\begin{aligned} C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) &= QD_{16} \\ C_{QD_{16}}(\langle \sigma^k \rangle) &= \langle \sigma \rangle \text{ for } k = 1, 2, 3, 5, 6, 7 \\ C_{QD_{16}}(\langle \tau\sigma \rangle) = C_{QD_{16}}(\langle \tau\sigma^5 \rangle) &= \langle \tau\sigma \rangle \\ C_{QD_{16}}(\langle \tau\sigma^3 \rangle) = C_{QD_{16}}(\langle \tau\sigma^7 \rangle) &= \langle \tau\sigma^3 \rangle \\ C_{QD_{16}}(\langle \tau \rangle) = C_{QD_{16}}(\langle \tau\sigma^4 \rangle) &= \langle \sigma^4, \tau \rangle \\ C_{QD_{16}}(\langle \tau\sigma^2 \rangle) = C_{QD_{16}}(\langle \tau\sigma^6 \rangle) &= \langle \tau\sigma^2, \sigma^4 \rangle \end{aligned}$$

■

Exercise 2.5.19

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 $rsr^{-1} = r^2s \neq r$, $r \notin N_{D_{16}}(\langle s, r^4 \rangle)$ so that $N_{D_{16}}(\langle s, r^4 \rangle) = \langle s, r^2 \rangle$. ■

Exercise 2.5.20

Use the lattice of subgroups of QD_{16} (cf. Exercise 2.5.11) 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

$$\sigma^2\langle \tau\sigma \rangle\sigma^6 = \{1, \tau\sigma^5, \sigma^4, \tau\sigma\} = \langle \tau\sigma \rangle$$

and $\sigma(\tau\sigma)\sigma^7 = \tau\sigma^3 \neq \tau\sigma$ so that $\sigma \notin N_{QD_{16}}(\langle \tau\sigma \rangle)$. Then $N_{QD_{16}}(\langle \tau\sigma \rangle) = \langle \sigma^2, \tau\sigma \rangle$.

(b) $\langle \tau, \sigma^4 \rangle = \{1, \tau, \sigma^4, \tau\sigma^4\}$, and

$$\sigma^2\langle \tau, \sigma^4 \rangle\sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\}$$

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.

Exercise 3.1.1

Let $\varphi\colon G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker(\varphi) \trianglelefteq G$.

Solution. Observe that $1_G \in \varphi^{-1}(E)$ since $\varphi(1_G) = 1_H \in E$. Let $x, y \in \varphi^{-1}(E)$ so that $\varphi(x), \varphi(y) \in E$. Since $E \leq H$, $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} \in E$, hence $xy^{-1} \in \varphi^{-1}(E)$. Therefore, $\varphi^{-1}(E) \leq G$.

Suppose $E \trianglelefteq H$. Then $heh^{-1} \in E$ for all $h \in H$ and $e \in E$. Let $x \in \varphi^{-1}(E)$ and $g \in G$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in E,$$

so that $gxg^{-1} \in \varphi^{-1}(E)$. Therefore, $\varphi^{-1}(E) \trianglelefteq G$. Then $\ker\varphi = \varphi^{-1}(1_H) \trianglelefteq G$ since $\{1_H\} \trianglelefteq H$. ■

Exercise 3.1.2

Let $\varphi\colon G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Fix an element $u \in X$ (so $\varphi(u) = a$). 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. Let $w \in Z$, and define $v = u^{-1}w$. Then

$$\varphi(v) = \varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}(ab) = b$$

so that $v \in Y$ and $uv = w$. ■

Exercise 3.1.3

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 obtain abelian quotient groups, consider non-abelian groups and their centers. Put $G = D_8$ and $N = Z(D_8) = \langle r^2 \rangle$. Then $G/N \cong V_4$ is abelian. ■

Exercise 3.1.4

Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Solution. Inducting on α, the base case $\alpha = 0$ is clear since $(gN)^0 = N = g^0N$. Suppose the statement holds for some $\alpha \in \mathbb{Z}$. Then

$$(gN)^{\alpha+1} = (gN)^\alpha(gN) = g^\alpha NgN = g^{\alpha+1}N.$$

Hence, the statement holds for all $\alpha \in \mathbb{Z}^+ \cup \{0\}$. The case of $\alpha = -1$ is handled by Proposition 3.5. For all negative α, utilize $\alpha = -1$ and the positive case to obtain the result. ■

Exercise 3.1.5

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 there exists some $n \in \mathbb{Z}^+$ such that $g^n \in N$, then Exercise 3.1.4 shows that $(gN)^n = g^nN = N$, so that the order of gN is at most n. If there exists some $m < n$ such that $(gN)^m = N$, then Exercise 3.1.4 shows that $g^m \in N$, contradicting the minimality of n. Hence, the order of gN is exactly n. If no such positive integer exists, then $(gN)^m \neq N$ for all $m \in \mathbb{Z}^+$. If $|gN|$ were finite, then there would exist some $m \in \mathbb{Z}^+$ such that $(gN)^m = N$, contradicting the assumption. Hence, $|gN|$ is infinite.

Put $G = Z_4 = \langle x \rangle$ and $N = \langle x^2 \rangle$. Then $|x| = 4$, but $|xN| = 2$ since $(xN)^2 = x^2N = N$. ■

Exercise 3.1.6

Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Solution. $\varphi^{-1}(+1)$ consists of positive reals and $\varphi^{-1}(-1)$ negative reals. Let $x, y \in \mathbb{R}^\times$. Then

$$\varphi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \varphi(x)\varphi(y)$$

■

Exercise 3.1.7

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

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

hence π is a homomorphism. Moreover, π is surjective since $\pi((a, 0)) = a$ for all $a \in \mathbb{R}$. We have $\ker \pi$ as the line $y = -x$, and $\pi^{-1}(a)$ as $y = a - x$, which is $\ker \pi$ translated up by a. ■

Exercise 3.1.8

Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ 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

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$$

so that φ is a homomorphism. Note that $|x| > 0$ for any $x \in \mathbb{R}^\times$, so $\operatorname{im}(\varphi) = \mathbb{R}^+$. $\ker(\varphi) = \{-1, 1\}$, and the fiber of φ over some $a \in \mathbb{R}^+$ is simply $\{-a, a\}$. ■

Exercise 3.1.9

Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. 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

$$\begin{aligned}
\varphi((a + bi)(c + di)) &= \varphi((ac - bd) + (ad + bc)i) \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= \varphi(a + bi)\varphi(c + di)
\end{aligned}$$

so that φ is a homomorphism. Observe that $a^2 + b^2 > 0$ for any $a + bi \in \mathbb{C}^\times$, so that $\operatorname{im}(\varphi) = \mathbb{R}^+$. $\ker \varphi$ is the unit circle in the complex plane, and the fiber of φ over some $r \in \mathbb{R}^+$ is the circle of radius $\sqrt{r}$ centered at the origin. ■

Exercise 3.1.10

Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\bar{a}) = \bar{a}$. 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 $\bar{a}$ has a different meaning in the domain and range of φ).

Solution. To show that φ is well defined, suppose $\bar{a} = \bar{b}$ in $\mathbb{Z}/8\mathbb{Z}$. Then $8 \mid (a-b)$, so that $a - b = 8k$ for some $k \in \mathbb{Z}$. Then $a - b = 4(2k)$, so that $4 \mid (a-b)$ and $\bar{a} = \bar{b}$ in $\mathbb{Z}/4\mathbb{Z}$. Hence, φ is well defined. Moreover, for any $\bar{a}, \bar{b} \in \mathbb{Z}/8\mathbb{Z}$, then

$$\varphi(\bar{a} + \bar{b}) = \varphi(\overline{a+b}) = \overline{a+b} = \bar{a} + \bar{b} = \varphi(\bar{a}) + \varphi(\bar{b})$$

so that φ is a homomorphism. Note that for any $\bar{c} \in \mathbb{Z}/4\mathbb{Z}$, then $\varphi(\bar{c}) = \bar{c}$, so φ is surjective. The fibers of φ:

$$\begin{aligned}
\varphi^{-1}(\bar{0}) &= \{\bar{0}, \bar{4}\} \\
\varphi^{-1}(\bar{1}) &= \{\bar{1}, \bar{5}\} \\
\varphi^{-1}(\bar{2}) &= \{\bar{2}, \bar{6}\} \\
\varphi^{-1}(\bar{3}) &= \{\bar{3}, \bar{7}\}
\end{aligned}$$

with $\ker \varphi = \varphi^{-1}(\bar{0}) = \{\bar{0}, \bar{4}\}$. ■

Exercise 3.1.11

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) Observe 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) To show that ψ is surjective is similar as the previous exercise. 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 $\pi_1 \colon H \to F$ given by

$$\pi_1\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = b$$

Define another map $\pi_2 \colon F \to H$ given by

$$\pi_2(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

It is clear that π_2 is a two-sided inverse of π_1. For any $b, c \in F$, we have

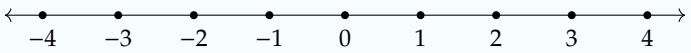
$$\pi_1\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) = \pi_1\left(\begin{pmatrix} 1 & b+c \\ 0 & 1 \end{pmatrix}\right) = b + c = \pi_1\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) + \pi_1\left(\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right)$$

so that π_1 is a homomorphism. Then π_1 is an isomorphism, and $H \cong F$. ■

Exercise 3.1.12

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 $\varphi \colon G \to H$ be the homomorphism $\varphi \colon r \mapsto e^{2\pi i r}$. 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 $e^{2\pi i r} = 1$ if and only if r is an integer, $\ker(\varphi) = \mathbb{Z}$. 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 $4\pi i/3 = 2/3(2\pi i)$:

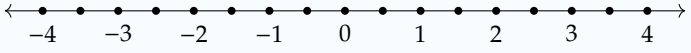
$$\begin{aligned} \varphi^{-1}(-1) &= \frac{1}{2} + \mathbb{Z} = \left\{ \frac{1}{2} + n \,\middle|\, n \in \mathbb{Z} \right\} \\ \varphi^{-1}(i) &= \frac{1}{4} + \mathbb{Z} = \left\{ \frac{1}{4} + n \,\middle|\, n \in \mathbb{Z} \right\} \\ \varphi^{-1}(e^{4\pi i/3}) &= \frac{2}{3} + \mathbb{Z} = \left\{ \frac{2}{3} + n \,\middle|\, n \in \mathbb{Z} \right\} \end{aligned}$$

■

Exercise 3.1.13

Repeat the preceding exercise with the map φ replaced by the map $\varphi \colon r \mapsto e^{4\pi i r}$.

Solution. The kernel of φ is $\frac{1}{2}\mathbb{Z}$, or



Moreover, the fibers are just all halved, so

$$\begin{aligned} \varphi^{-1}(-1) &= \frac{1}{4} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{4} + \frac{n}{2} \,\middle|\, n \in \mathbb{Z} \right\} \\ \varphi^{-1}(i) &= \frac{1}{8} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{8} + \frac{n}{2} \,\middle|\, n \in \mathbb{Z} \right\} \\ \varphi^{-1}(e^{4\pi i/3}) &= \frac{1}{3} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{3} + \frac{n}{2} \,\middle|\, n \in \mathbb{Z} \right\} \end{aligned}$$

■

Exercise 3.1.14

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 $0 \leq q < 1$.
(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 2.1.6).
(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of roots of unity in $\mathbb{C}^\times$.

Solution.

(a) Suppose $a/b \in \mathbb{Q}$ with $(a,b) = 1$. By the Division Algorithm, there exist unique integers q, r such that $a = bq + r$ for $0 \leq r < b$, or equivalently, $a/b = q + r/b$. Then $a/b + \mathbb{Z} = r/b + \mathbb{Z}$. If there exists some other representative s/t in $0 \leq s/t < 1$ such that $a/b + \mathbb{Z} = s/t + \mathbb{Z}$, then $r/b + \mathbb{Z} = s/t + \mathbb{Z}$, or that $r/b - s/t \in \mathbb{Z}$. Then there exists some integer k such that $rt - sb = kbt$. Since $0 \leq r < b$ and $0 \leq s < t$, $0 \leq rt < bt$ and $0 \leq sb < bt$. Combining these two inequalities, we get $-bt < rt - sb < bt$, so that $-1 < k < 1$. Since k is an integer, $k = 0$, and $rt - sb = 0$, or $r/b = s/t$. Hence, the representative in $0 \leq q < 1$ is unique.

(b) Let $a/b \in \mathbb{Q}$. Then $b(a/b + \mathbb{Z}) = ab + \mathbb{Z} = \mathbb{Z}$, so that $a/b + \mathbb{Z}$ has finite order. Moreover, $1/k + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has order k, and since k can be made arbitrarily large, there are elements of arbitrarily large order.

(c) By the previous exercise, $\mathbb{Q}/\mathbb{Z} \subseteq \mathrm{Tor}(\mathbb{R}/\mathbb{Z})$. Let $x + \mathbb{Z} \in \mathrm{Tor}(\mathbb{R}/\mathbb{Z})$. Then $|x + \mathbb{Z}|$ is finite, so there exists some $n \in \mathbb{Z}$ such that $n(x + \mathbb{Z}) = nx + \mathbb{Z} = \mathbb{Z}$. Then $nx \in \mathbb{Z}$, so that $x = m/n$ for some $m \in \mathbb{Z}$. Hence, $x + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, and $\mathrm{Tor}(\mathbb{R}/\mathbb{Z}) \subseteq \mathbb{Q}/\mathbb{Z}$. Therefore, $\mathrm{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

(d) By Exercise 3.1.12, we have $\mathbb{R}/\mathbb{Z} \cong S^1$. By definition, $\mathrm{Tor}(S^1)$ consists of $z \in \mathbb{C}^\times$ such that $z^n = 1$ for some $n \in \mathbb{Z}^+$. This is precisely the set of roots of unity. Since $\mathrm{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the set of roots of unity. ■

Exercise 3.1.15

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. Since A is abelian, any proper subgroup B of A is normal. To that end, let $aB \in A/B$, and let $n \in \mathbb{Z}^+$. Since A is divisible, there exists some $x \in A$ such that $x^n = a$. Then

$$(xB)^n = x^n B = aB$$

so that A/B is divisible. Observe that $\mathbb{Q}$ is divisible, since for any $q \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$, there exists $p \in \mathbb{Q}$ such that $np = q$, namely $p = q/n$. Moreover, $\mathbb{Z}$ is a proper subgroup of $\mathbb{Q}$, so by the first part, $\mathbb{Q}/\mathbb{Z}$ is divisible. ■

Exercise 3.1.16

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. We prove the general case. Since $G = \langle S \rangle$, for any $g \in G$, we have

$$g = s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}, \quad s_i \in S, \alpha_i \in \mathbb{Z}$$

Observe that $\overline{S} = \{\overline{s} \mid s \in S\}$. Then for any $\overline{g} \in \overline{G}$, we have

$$\overline{g} = \overline{s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}} = \overline{s}_1^{\alpha_1} \overline{s}_2^{\alpha_2} \cdots \overline{s}_k^{\alpha_k}$$

so that $\overline{g} \in \langle \overline{S} \rangle$. Hence, $\overline{G} \subseteq \langle \overline{S} \rangle$. Since $\overline{s} \in \overline{G}$ for any $s \in S$, $\langle \overline{S} \rangle \subseteq \overline{G}$. Therefore, $\overline{G} = \langle \overline{S} \rangle$.

The case of $G = \langle x, y \rangle$ is a special case where $S = \{x, y\}$. ■

Exercise 3.1.17

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

$$\begin{aligned} \overline{r^k r^2 r^{-k}} &= \bar{r}^2 \in \overline{H} \\ \overline{r^k s r^{-k}} &= \overline{s(r^2)^{-k}} \in \overline{H} \end{aligned}$$

If it is of the latter, then

$$\begin{aligned} \overline{(sr^k)r^2(r^{-k}s)} &= \overline{r^{-2}} \in H \\ \overline{(sr^k)s(r^{-k}s)} &= \overline{s(r^2)^k} \in H \end{aligned}$$

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 $\pi\colon G \to \overline{G}$ 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 $\varphi\colon D_8 \to \pi^{-1}(\overline{H})$ 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 $\bar{s}$, $\bar{r}^2 \in Z(\overline{G})$. However, $\overline{rs} \neq \overline{sr}$ and $\overline{r^3s} \neq \overline{sr^3}$. 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:

$$\begin{aligned} \widehat{1} &= \{\bar{1}, \bar{r}^2\} & \widehat{s} &= \{\bar{s}, \overline{sr^2}\} \\ \widehat{r} &= \{\bar{r}, \bar{r}^3\} & \widehat{sr} &= \{\overline{sr}, \overline{sr^3}\} \end{aligned}$$

One can see that each nonidentity element of $\widehat{G}$ has order 2 so that $\widehat{G} \cong V_4$. ∎

Exercise 3.1.18

Let G be the quasidihedral group of order 16 (whose lattice was computed in Exercise 2.5.11): $G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle$, 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

$$\begin{aligned} \overline{1} &= \{1, \sigma^4\} & \overline{\tau} &= \{\tau, \tau\sigma^4\} \\ \overline{\sigma} &= \{\sigma, \sigma^5\} & \overline{\tau\sigma} &= \{\tau\sigma, \tau\sigma^5\} \\ \overline{\sigma}^2 &= \{\sigma^2, \sigma^6\} & \overline{\tau\sigma^2} &= \{\tau\sigma^2, \tau\sigma^6\} \\ \overline{\sigma}^3 &= \{\sigma^3, \sigma^7\} & \overline{\tau\sigma^3} &= \{\tau\sigma^3, \tau\sigma^7\} \end{aligned}$$

(c) The orders are

$\overline{x}$	$\overline{1}$	$\overline{\sigma}$	$\overline{\sigma}^2$	$\overline{\sigma}^3$	$\overline{\tau}$	$\overline{\tau\sigma}$	$\overline{\tau\sigma^2}$	$\overline{\tau\sigma^3}$
$\lvert\overline{x}\rvert$	1	4	2	4	2	2	2	2

(d) $\overline{\sigma\tau} = \overline{\tau\sigma^3}$, $\overline{\tau\sigma^{-2}\tau} = \overline{\sigma}^2$, $\overline{\tau^{-1}\sigma^{-1}\tau\sigma} = \overline{\sigma}^2$.
(e) Note that $\overline{\sigma}^4 = \overline{\tau}^2 = \overline{1}$, and $\overline{\sigma\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^7} = \overline{\tau\sigma}$ so that $\overline{G}$ satisfies the same relations in D_8. Then the mapping $\varphi\colon \overline{G} \to D_8$ given by $\varphi(\overline{\sigma}) = r$ and $\varphi(\overline{\tau}) = s$ extends to a surjective homomorphism, hence $\overline{G} \cong D_8$. ■

Exercise 3.1.19

Let G be the modular group of order 16 (whose lattice was computed in Exercise 2.5.14): $G = \langle u, v \mid u^2 = v^8 = 1,\ vu = uv^5 \rangle$, and let $\overline{G} = G/\langle v^4 \rangle$ 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 $\overline{G}$ is 8.
(b) Exhibit each element of $\overline{G}$ in the form $\overline{u}^a \overline{v}^b$, 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 $\overline{u}^a \overline{v}^b$, for some integers a and b as in (b): $\overline{vu}$, $\overline{uv^{-2}u}$, $\overline{u^{-1}v^{-1}uv}$.
(e) Prove that $\overline{G}$ 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 $|\overline{G}| = 8$.
(b) The elements are

$$\begin{aligned} \overline{1} &= \{1, v^4\} & \overline{u} &= \{u, uv^4\} \\ \overline{v} &= \{v, v^5\} & \overline{uv} &= \{uv, uv^5\} \\ \overline{v}^2 &= \{v^2, v^6\} & \overline{uv^2} &= \{uv^2, uv^6\} \\ \overline{v}^3 &= \{v^3, v^7\} & \overline{uv^3} &= \{uv^3, uv^7\} \end{aligned}$$

(c) The orders are

$\overline{x}$	$\overline{1}$	$\overline{v}$	$\overline{v}^2$	$\overline{v}^3$	$\overline{u}$	$\overline{uv}$	$\overline{uv^2}$	$\overline{uv^3}$
$\lvert\overline{x}\rvert$	1	4	2	4	2	4	2	4

(d) $\overline{vu} = \overline{uv^5} = \overline{uv}$, $\overline{uv^{-2}u} = \overline{v^2}$, $\overline{u^{-1}v^{-1}uv} = \overline{v^2}$.

(e) Since $\overline{vu} = \overline{uv^5} = \overline{uv}$, $\overline{G}$ is abelian. Moreover, using the presentation of $Z_2 \times Z_4$ in Exercise 2.5.12, we see that $\overline{u}^2 = \overline{v}^4 = 1$ so that $\overline{G}$ satisfies the same relations. Then $\varphi\colon \overline{G} \to Z_2 \times Z_4$ given by $\varphi(\overline{u}) = a$ and $\varphi(\overline{v}) = b$ is a surjective homomorphism, hence $\overline{G} \cong Z_2 \times Z_4$. ■

Exercise 3.1.20

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 $\widetilde{\overline{a}}$ 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 $\widetilde{x} = \overline{x}\langle 12\rangle = \{\overline{x}, \overline{x+12}\}$. 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 $\varphi\colon \widetilde{G} \to \mathbb{Z}/12\mathbb{Z}$ given by $\varphi(\widetilde{x}) = \overline{x}$. This map is trivially a bijection, and for any $\widetilde{x}, \widetilde{y} \in \widetilde{G}$, then

$$\varphi(\widetilde{x} + \widetilde{y}) = \varphi(\widetilde{x+y}) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(\widetilde{x}) + \varphi(\widetilde{y})$$

so that φ is a homomorphism. Then $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. ■

Exercise 3.1.21

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 $\overline{x}^a\overline{y}^b$ for some integers a and b.
(c) Find the order of each element 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 $\overline{x}^2\overline{y}^2 = \overline{1}$ in $\overline{G}$, we have $\overline{x}^2 = \overline{y}^2$. Then we have the elements

$$\begin{aligned} \overline{1} &= \{1, x^2y^2\} & \overline{y} &= \{y, x^2y^3\} \\ \overline{x} &= \{x, x^3y^2\} & \overline{xy} &= \{xy, x^3y^3\} \\ \overline{x}^2 &= \{x^2, y^2\} & \overline{x^2y} &= \{x^2y, y^3\} \\ \overline{x}^3 &= \{x^3, xy^2\} & \overline{x^3y} &= \{x^3y, xy^3\} \end{aligned}$$

(c) The orders are

$\overline{g}$	$\overline{1}$	$\overline{x}$	$\overline{x}^2$	$\overline{x}^3$	$\overline{y}$	$\overline{xy}$	$\overline{x^2y}$	$\overline{x^3y}$
$\lvert\overline{g}\rvert$	1	4	2	4	4	2	4	2

(d) Using the presentation of $Z_2 \times Z_4$ in Exercise 2.5.12, and noting that $\overline{xy}^2 = \overline{x}^4 = 1$ then the mapping $\varphi\colon Z_2 \times Z_4 \to \overline{G}$ given by

$$\varphi(a) = \overline{xy}, \quad \varphi(b) = \overline{x}$$

extends to a unique homomorphism. Now suppose $\varphi(a^sb^t) = \varphi(a^ub^v)$. Then $\overline{xy}^s\overline{x}^t = \overline{xy}^u\overline{x}^v$. Since $\langle\overline{xy}\rangle \cap \langle\overline{x}\rangle$ is trivial, $\overline{xy}^{s-u} = \overline{x}^{v-t}$ imply that both quantities must be one. Then $\overline{xy}^s = \overline{xy}^u$ and $\overline{x}^v = \overline{x}^t$. Then $s \equiv u \pmod 2$ and $v \equiv t \pmod 4$, 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 $\overline{G} \cong Z_2 \times Z_4 \cong Z_4 \times Z_2$. ■

Exercise 3.1.22

(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 $K \trianglelefteq G$, $gxg^{-1} \in H$ 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 $gNg^{-1} \subseteq N$. ■

Exercise 3.1.23

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 $N_i \trianglelefteq G$, $gn_ig^{-1} \in N_i$ 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 $N \trianglelefteq G$. ■

Exercise 3.1.24

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 $N \trianglelefteq G$, $hxh^{-1} \in N$. Since $H \leq G$, $hxh^{-1} \in H$ so that $hxh^{-1} \in N \cap H$. Then $N \cap H \trianglelefteq H$. ■

Exercise 3.1.25

(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) $\boxed{\Rightarrow}$ If $N \trianglelefteq G$, then $gNg^{-1} \subseteq N$ holds true for all $g \in G$.
$\boxed{\Leftarrow}$ Suppose $gNg^{-1} \subseteq N$ for every $g \in G$, and let $n \in N$. For some $g \in G$, we have $g^{-1}Ng \subseteq N$ so that $g^{-1}ng \in N$. Then $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$. Hence, $N \subseteq gNg^{-1}$, and $N = gNg^{-1}$. Therefore, $N \trianglelefteq G$.

(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. ■

Exercise 3.1.26

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) Observe that $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$. To see that the orders are the same, refer to 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 $N = \langle \varnothing \rangle = 1$ is trivial. Otherwise, suppose S is nonempty, and let $n \in N$. Since $N = \langle S \rangle$,

$$n = s_1 s_2 \cdots s_k, \quad s_i \in S \text{ for all } i = 1, 2, \ldots, k.$$

Since

$$gng^{-1} = g(s_1 s_2 \cdots s_k)g^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_kg^{-1})$$

for every $g \in G$ and $gSg^{-1} \subseteq N$, it follows that $gng^{-1} \in N$. Hence, $gNg^{-1} \subseteq N$ for every $g \in G$, so that $N \trianglelefteq G$.
(d) $\boxed{\Rightarrow}$ Immediate from the definition of a normal subgroup.
$\boxed{\Leftarrow}$ Let $S = \langle x \rangle$, and use part (c).
(e) Let $S = \{g \in G \mid |g| = n\}$. Let $N = \langle S \rangle$. If S is empty, then N is again trivial, hence is normal. Suppose S is nonempty. By part (a), then $|gsg^{-1}| = |s| = n$ for any $g \in G$ and $s \in S$, so that $gsg^{-1} \in S \subseteq N$. Then $gSg^{-1} \subseteq N$, hence $N \trianglelefteq G$ by part (c). ■

Exercise 3.1.27

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.

$\boxed{\Rightarrow}$ Suppose $gNg^{-1} \subseteq N$. Let $\varphi \colon N \to gNg^{-1}$ be the conjugation map. By Exercise 1.7.17, we know that this map is defined to be an isomorphism, hence $|gNg^{-1}| = |N|$. Since $gNg^{-1} \subseteq N$ and both sets are finite with the same cardinality, it follows that $gNg^{-1} = N$.
$\boxed{\Leftarrow}$ Immediate.

By the previous part, we have that $g \in N_G(N)$ if and only if $gNg^{-1} = N$, which holds if and only if $gNg^{-1} \subseteq N$. Then $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$. ■

Exercise 3.1.28

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.
$\boxed{\Rightarrow}$ Immediate, since $gSg^{-1} \subseteq gNg^{-1} = N$ because $g \in N_G(N)$.
$\boxed{\Leftarrow}$ If S is empty, then N is trivial, hence is normal. Otherwise, suppose S is nonempty, and let $n \in N$. Since $N = \langle S \rangle$,

$$n = s_1 s_2 \cdots s_k, \quad s_i \in S \text{ for all } i = 1, 2, \ldots, k.$$

Since

$$gng^{-1} = g(s_1 s_2 \cdots s_k)g^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_kg^{-1})$$

for every $g \in G$ and $gSg^{-1} \subseteq N$, it follows that $gng^{-1} \in N$. Thus, $gNg^{-1} \subseteq N$. Since N is finite, we may use the previous exercise to conclude that $g \in N_G(N)$. ■

Exercise 3.1.29

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.
$\boxed{\Rightarrow}$ Immediate, since $gNg^{-1} = N$ for every $g \in G$, so $tSt^{-1} \subseteq N$.
$\boxed{\Leftarrow}$ Let S and T be nonempty subsets of G, and let $g \in G$. By assumption, $g \in \langle T \rangle$ implies that

$$g = t_1 t_2 \ldots t_k, \quad t_i \in T \text{ for each } i = 1, 2, \ldots, k.$$

We proceed by induction on the word length of $g \in \langle T \rangle$. The base case of $t_1 S t_1^{-1} \subseteq N$ is satisfied by assumption. Assume now that $gSg^{-1} \subseteq N$ for k-length words made up of elements from T. Consider a word of length $k+1$ given by

$$g = t_1 t_2 \ldots t_k t_{k+1}, \quad t_i \in T \text{ for each } i = 1, 2, \ldots, k+1.$$

Let $\widehat{t} = t_1 t_2 \ldots t_k$ so that $g = \widehat{t} t_{k+1}$. By the induction assumption, $\widehat{t} S \widehat{t}^{-1} \subseteq N$. For any $s \in S$, then

$$gsg^{-1} = \widehat{t} t_{k+1} s t_{k+1}^{-1} \widehat{t}^{-1} = \widehat{t}(t_{k+1} s t_{k+1}^{-1})\widehat{t}^{-1}$$

where $t_{k+1} s t_{k+1}^{-1} \in N$ because $tSt^{-1} \subseteq N$ for every $t \in T$. Since $N = \langle S \rangle$,

$$t_{k+1} s t_{k+1}^{-1} = s_1 s_2 \ldots s_m, \quad s_i \in S \text{ for each } i = 1, 2, \ldots, m.$$

Then

$$\widehat{t}(t_{k+1} s t_{k+1}^{-1})\widehat{t}^{-1} = (\widehat{t} s_1 \widehat{t}^{-1})(\widehat{t} s_2 \widehat{t}^{-1}) \cdots (\widehat{t} s_m \widehat{t}^{-1}) \in N$$

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 $N \trianglelefteq G$. ■

Exercise 3.1.30

Let $N \leq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

Solution.
$\boxed{\Rightarrow}$ Suppose $gN = Ng$, and let $n \in N$. Then there exists $n' \in N$ such that $gn = n'g$. Then $gng^{-1} = n' \in N$, hence $gNg^{-1} \subseteq N$. Similarly, there exists $n'' \in N$ such that $ng = gn''$, so that $n = gn''g^{-1} \in gNg^{-1}$, hence $N \subseteq gNg^{-1}$. Then $gNg^{-1} = N$, so that $g \in N_G(N)$.
$\boxed{\Leftarrow}$ Suppose $g \in N_G(N)$. Let $n \in N$. Since $n \in gNg^{-1}$, there exists $n' \in N$ such that $n = gn'g^{-1}$. Then $ng = gn'$, hence $n \in gN$, and $Ng \subseteq gN$. By symmetry, we have $gN \subseteq Ng$, hence $gN = Ng$. ■

Exercise 3.1.31

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 $N_G(N)$, $N_G(N)$ is the largest subgroup in which N is normal. ■

Exercise 3.1.32

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 $j\langle i\rangle(-j) = \langle i\rangle$, $j \in N_{Q_8}(\langle i\rangle)$ 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.

Observe that $Q_8/Z(Q_8) = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$. It is clear that $\bar{i}^2 = \bar{j}^2 = \bar{k}^2 = \bar{1}$, so that $Q_8/Z(Q_8) \cong V_4$. Moreover, each of the maximal subgroups $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$ are of order 4, which means their corresponding quotient groups will have order 2, hence $Q_8/\langle i\rangle \cong Q_8/\langle j\rangle \cong Q_8/\langle k\rangle \cong Z_2$. ■

Exercise 3.1.33

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 $N_{D_8}(\langle s, r^2\rangle) = N_{D_8}(\langle r\rangle) = N_{D_8}(\langle rs, r^2\rangle) = D_8$. Moreover, each of these maximal subgroups are of order 4, which means their corresponding quotient groups will have order 2, hence $D_8/\langle s, r^2\rangle \cong D_8/\langle r\rangle \cong D_8/\langle rs, r^2\rangle \cong Z_2$.

Now we examine $\langle r^2\rangle = Z(D_8)$, which is 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. ■

Exercise 3.1.34

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 $r, s \in N_{D_{2n}}(\langle r^k\rangle)$, $\langle r^k\rangle \trianglelefteq D_{2n}$.

(b) Consider $D_{2n}/\langle r^k\rangle$. Since $k \mid n$, 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 $D_{2n}/\langle r^k\rangle \cong D_{2k}$. ■

Exercise 3.1.35

Prove that $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$ and describe the isomorphism type of the quotient group (cf. Exercise 2.1.9).

Solution. Since $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$ by Exercise 2.1.9, it remains to be shown that $\mathrm{SL}_n(F)$ is normal in $\mathrm{GL}_n(F)$. Let $S \in \mathrm{SL}_n(F)$ and $X \in \mathrm{GL}_n(F)$. Then

$$\det(XSX^{-1}) = \det(X)\det(S)\det(X^{-1}) = 1$$

so that $XSX^{-1} \in \mathrm{SL}_n(F)$. Then $X\,\mathrm{SL}_n(F)X^{-1} \subseteq \mathrm{SL}_n(F)$ for every $X \in \mathrm{GL}_n(F)$, and since conjugation is an isomorphism, $X\,\mathrm{SL}_n(F)X^{-1} = \mathrm{SL}_n(F)$. Hence, $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$.

Observe that a normal subgroup corresponds to the kernel of some homomorphism. It is clear that the mapping $\det\colon \mathrm{GL}_n(F) \to F^\times$ is a homomorphism, and the elements that map to the identity in $F^\times$ are precisely those matrices with determinant 1, i.e. $\mathrm{SL}_n(F)$. Then we may consider the mapping $\varphi\colon \mathrm{GL}_n(F)/\mathrm{SL}_n(F) \to F^\times$ given by $\varphi(\overline{X}) = \det(X)$.

We now show that φ is well defined. Suppose $\overline{A} = \overline{B}$ for some $\overline{A}, \overline{B} \in \mathrm{GL}_n(F)/\mathrm{SL}_n(F)$. Then for some $AS \in \overline{A}$ for $S \in \mathrm{SL}_n(F)$, there exists $S' \in \mathrm{SL}_n(F)$ such that $AS = BS'$. Then

$$\varphi(\overline{A}) = \det(A) = \det(AS) = \det(BS') = \det(B) = \varphi(\overline{B})$$

so that φ is well defined.

Suppose $\varphi(\overline{A}) = \varphi(\overline{B})$ for $\overline{A}, \overline{B} \in \mathrm{GL}_n(F)/\mathrm{SL}_n(F)$. Then $\det(A) = \det(B)$. Let $AS \in \overline{A}$ for some $S \in \mathrm{SL}_n(F)$. Note that B^{-1} exists since $B \in \mathrm{GL}_n(F)$. Then

$$\det(B^{-1}AS) = \det(B^{-1})\det(A)\det(S) = \det(A)^{-1}\det(A)\det(S) = 1$$

so that $B^{-1}AS \in \mathrm{SL}_n(F)$, hence $B^{-1}AS = S'$ for some $S' \in \mathrm{SL}_n(F)$. It follows that $AS = BS'$ so that $AS \in \overline{B}$, hence $\overline{A} \subseteq \overline{B}$. 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 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$. ∎

Exercise 3.1.36

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 $G/Z(G)$ is cyclic with generator $xZ(G)$. Let $g, h \in G$. Then there exist integers $a, b \in \mathbb{Z}$ and elements $z_1, z_2 \in Z(G)$ such that

$$g = x^a z_1 \quad \text{and} h = x^b z_2$$

Then

$$gh = (x^a z_1)(x^b z_2) = (x^b z_2)(x^a z_1) = hg$$

since $z_1, z_2 \in Z(G)$. Hence, G is abelian. ∎

Exercise 3.1.37

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 given set. It is clear that $C \leq A \times B$. To show that $C \trianglelefteq A \times B$, let $(a, b) \in A \times B$. Then for any $(a', 1) \in C$, we have

$$(a, b)(a', 1)(a, b)^{-1} = (aa'a^{-1}, b1b^{-1}) = (aa'a^{-1}, 1) \in C$$

hence, $C \trianglelefteq A \times B$.

Let $\varphi\colon A \times B/C \to B$ be given by $\varphi((a, b)C) = b$. To show that this is well defined, suppose $(a, b)C = (a', b')C$. Then $C = (a^{-1}, b^{-1})(a', b')C$, or that $(a^{-1}a', b^{-1}b') \in C$. Then $b^{-1}b' = 1$, or $b = b'$ so that φ is well defined.

Suppose $\varphi((a, b)C) = \varphi((a', b')C)$. Then $b = b'$ so that $(a, b)C = (a', b')C$, hence φ is injective. Moreover, $\varphi((1, b)C) = b$ so that φ is surjective. Lastly, for $(a, b)C, (a', b')C \in A \times B/C$, then

$$\varphi((a, b)C(a', b')C) = \varphi((aa', bb')C) = bb' = \varphi((a, b)C)\varphi((a', b')C)$$

so that φ is a bijective homomorphism. Hence, $A \times B/C \cong B$. ∎

Exercise 3.1.38

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. By Exercise 1.1.29, $A \times A$ is abelian since A is abelian, hence every subgroup of $A \times A$ is normal, including D.

Let $\varphi\colon (A\times A)/D \to A$ be given by $\varphi((a,b)D) = ab^{-1}$. To show that this is well defined, suppose $(a_1,b_1)D = (a_2,b_2)D$. Then $D = (a_1^{-1},b_1^{-1})(a_2,b_2)D$, or that $(a_1^{-1}a_2, b_1^{-1}b_2) \in D$. Then $a_1^{-1}a_2 = b_1^{-1}b_2$, or $a_2b_2^{-1} = a_1b_1^{-1}$ so that φ is well defined. We may follow this argument backwards to show that φ is injective. Moreover, $\varphi((a,1)D) = a$ so that φ is surjective. Lastly, for $(a_1,b_1)D, (a_2,b_2)D \in (A\times A)/D$, then

$$\varphi((a_1,b_1)D(a_2,b_2)D) = \varphi((a_1a_2,b_1b_2)D) = a_1a_2(b_1b_2)^{-1} = (a_1b_1^{-1})(a_2b_2^{-1}) = \varphi((a_1,b_1)D)\varphi((a_2,b_2)D)$$

so that φ is a bijective homomorphism. Hence, $(A \times A)/D \cong A$. ■

Exercise 3.1.39

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 $S_3 \times S_3$. ■

Exercise 3.1.40

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.

$\boxed{\Rightarrow}$ 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 $x^{-1}y^{-1}xy \in N$.

$\boxed{\Leftarrow}$ 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, $\overline{xy} = \overline{yx}$. ■

Exercise 3.1.41

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 $[x,y] \in N$. ■

Exercise 3.1.42

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 $H \trianglelefteq G$, $y^{-1}xy \in H$, hence $[x,y] \in H$. Since $K \trianglelefteq G$, $x^{-1}y^{-1}x \in K$, 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 $xy = yx$. ■

Exercise 3.1.43

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 $\widetilde{g} \in \mathcal{P}$ denote the element such that $g \in \widetilde{g}$. We now show that $\widetilde{1} \leq G$. Since $1 \in \widetilde{1}$, $\widetilde{1}$ is nonempty. Suppose $g, h \in \widetilde{1}$. Then

$$\widetilde{gh} = \widetilde{g} \cdot \widetilde{h} = \widetilde{1} \cdot \widetilde{1} = \widetilde{1}$$

so that $gh \in \widetilde{1}$. Lastly, if $g \in \widetilde{1}$, then

$$\widetilde{g^{-1}} = \widetilde{g^{-1}} \cdot \widetilde{1} = \widetilde{g^{-1}} \cdot \widetilde{g} = \widetilde{g^{-1}g} = \widetilde{1}$$

so that $g^{-1} \in \widetilde{1}$. Hence, $\widetilde{1} \leq G$.

To show that $\widetilde{1} \trianglelefteq G$, let $g \in G$ and $x \in \widetilde{1}$. Then

$$\widetilde{gxg^{-1}} = \widetilde{g} \cdot \widetilde{x} \cdot \widetilde{g^{-1}} = \widetilde{g} \cdot \widetilde{1} \cdot \widetilde{g^{-1}} = \widetilde{gg^{-1}} = \widetilde{1}$$

so that $gxg^{-1} \in \widetilde{1}$, hence $\widetilde{1} \trianglelefteq G$.

To show that the elements of $\mathcal{P}$ are the cosets of $\widetilde{1}$, let $g \in G$ with $\overline{g} \in G/\widetilde{1}$. We show that $\overline{g} = \widetilde{g}$. For any $x \in \overline{g}$, then $x \in g\widetilde{1}$, or $x = gh$ for some $h \in \widetilde{1}$. Then

$$\widetilde{x} = \widetilde{gh} = \widetilde{g} \cdot \widetilde{h} = \widetilde{g} \cdot \widetilde{1} = \widetilde{g}$$

so that $x \in \widetilde{g}$, hence $\overline{g} \subseteq \widetilde{g}$. Similarly, for any $y \in \widetilde{g}$, consider the element $g^{-1}y \in G$. Then

$$\widetilde{g^{-1}y} = \widetilde{g^{-1}} \cdot \widetilde{y} = \widetilde{g^{-1}} \cdot \widetilde{g} = \widetilde{g^{-1}g} = \widetilde{1}$$

so that $g^{-1}y \in \widetilde{1}$, or $y \in g\widetilde{1} = \overline{g}$. Hence, $\widetilde{g} \subseteq \overline{g}$, and $\overline{g} = \widetilde{g}$. ∎

3.2 More on Cosets and Lagrange's Theorem

Let G be a group.

Exercise 3.2.1

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, 15, and 60 are permissible orders for subgroups of a group of order 120. The corresponding indices are 120, 60, 24, 8, and 2, respectively. ■

Exercise 3.2.2

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. Recall that $|S_3| = 6$. By Lagrange's Theorem, the possible orders of nontrivial subgroups are 2 and 3. Any subgroup of order 2 must be cyclic, and these are the subgroups $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, and $\langle(2\ 3)\rangle$. Similarly, any subgroup of order 3 must be cyclic. Since $\langle(1\ 2\ 3)\rangle$ contains both elements of order 3 in S_3, it is the only subgroup of order 3. Since no subgroup of order 2 can be contained in the subgroup of order 3, and the subgroup of order 3 is maximal as there are no other divisors to consider except 6 (which is S_3 itself), the lattice contains all subgroups of S_3.

We now consider the joins of the subgroups. By Exercise 2.4.5, the join of any two elements of order 2 is S_3. The join of the subgroup of order 3 with any subgroup of order 2 is also S_3: for example, $(1\ 2\ 3)(1\ 2) = (1\ 3) \in \langle(1\ 2\ 3), (1\ 2)\rangle$. Then $(1\ 3)$ and $(1\ 2)$ generate S_3. We may similarly argue for the other two elements of order 2.

Lastly, observe that any two distinct subgroups of order 2 intersect trivially, and the intersection of any subgroup of order 2 with the subgroup of order 3 is also trivial since none of the elements of order 2 are contained in the subgroup of order 3. Hence, the lattice is correct. ■

Exercise 3.2.3

Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

Solution. Recall that $|Q_8| = 8$. By Lagrange's Theorem, the possible orders of nontrivial subgroups are 2 and 4. Any subgroup of order 2 must be cyclic, and the only element of order 2 in Q_8 is -1, hence $\langle -1\rangle$ is the only subgroup of order 2. There are 6 elements of order 4 in Q_8, and each of them is contained in one of the three subgroups of order 4: $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$. Moreover, the subgroups of order 4 are maximal since no other divisor exists between 4 and 8.

We consider the joins of the subgroups. By the presentation for Q_8, we have the join of any 2 subgroups of order 4 is Q_8. The join of the subgroup of order 2 with any subgroup of order 4 is the subgroup of order 4 itself since $\langle -1\rangle$ is contained in each subgroup of order 4.

The intersection of any two distinct subgroups of order 4 is $\langle -1\rangle$. The intersection of the subgroup of order 2 with any subgroup of order 4 is also $\langle -1\rangle$. Hence, the lattice is correct. ■

Exercise 3.2.4

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, so that $Z(G)$ is a proper subgroup of G. Suppose $Z(G) \neq 1$. By Lagrange's Theorem, the possible orders of $Z(G)$ are p or q. Without loss of generality, assume $|Z(G)| = p$. Then $|G/Z(G)| = |G|/|Z(G)| = pq/p = q$, which is prime. By Corollary 3.10, $G/Z(G) \cong Z_q$, which is cyclic. By Exercise 3.1.36, G is abelian, a contradiction. Hence, $Z(G) = 1$. ■

Exercise 3.2.5

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) We first show that $gHg^{-1} \leq G$. Note that $1 \in H$, hence $g1g^{-1} = 1 \in gHg^{-1}$ so that gHg^{-1} is nonempty. Suppose $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ for some $h_1, h_2 \in H$. Then

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$$

since $h_1h_2^{-1} \in H$. Then $gHg^{-1} \leq G$.

To show that gHg^{-1} has the same order as H, consider the mapping $\varphi: H \to gHg^{-1}$ given by $\varphi(h) = ghg^{-1}$. For $h_1, h_2 \in H$ such that $\varphi(h_1) = \varphi(h_2)$, then $gh_1g^{-1} = gh_2g^{-1}$, or $h_1 = h_2$, hence φ is injective. Moreover, for any $ghg^{-1} \in gHg^{-1}$, then $\varphi(h) = ghg^{-1}$, so that φ is surjective. Hence, φ is a bijection, and $|gHg^{-1}| = |H|$.

(b) Let H be the unique subgroup of G of order n. For any $g \in G$, consider the subgroup gHg^{-1}. By part (a), gHg^{-1} is a subgroup of G of order n. Since H is the unique subgroup of order n, $gHg^{-1} = H$ for every $g \in G$, hence $H \trianglelefteq G$. ■

Exercise 3.2.6

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 $g \in N_G(H)$. ■

Exercise 3.2.7

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 $a, b, c \in G$. To show that $\sim$ is an equivalence relation, we check the three properties:

- Reflexive: $a \sim a$ since $a^{-1}a = 1 \in H$.
- Symmetric: If $a \sim b$, then $b^{-1}a \in H$. Then $(b^{-1}a)^{-1} = a^{-1}b \in H$, hence $b \sim a$.
- Transitive: If $a \sim b$ and $b \sim c$, then $b^{-1}a, c^{-1}b \in H$. Then $(c^{-1}b)(b^{-1}a) = c^{-1}a \in H$, hence $a \sim c$.

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. By Proposition 0.2, the equivalence classes partition G. Since the equivalence classes are precisely the left cosets of H in G, the left cosets of H partition G. ■

Exercise 3.2.8

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 $H \cap K \leq K$, by Lagrange's Theorem, $\ell \mid m$ and $\ell \mid n$. It follows that $\ell \mid (m, n) = 1$, hence $\ell = 1$. ■

Exercise 3.2.9

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 are 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) Let $\mathcal{S}'$ denote the set of $(p-1)$-tuples of elements of G. Observe that $|\mathcal{S}'| = |G|^{p-1}$. Define the mapping

$$\varphi : \mathcal{S}' \to \mathcal{S} \quad \text{by} \quad \varphi(x_1, x_2, \ldots, x_{p-1}) = (x_1, x_2, \ldots, x_{p-1}, (x_1 x_2 \cdots x_{p-1})^{-1})$$

To show that φ is injective, suppose $\varphi(x_1, \ldots, x_{p-1}) = \varphi(y_1, \ldots, y_{p-1})$. Then $x_i = y_i$ for all $1 \le i \le p-1$, 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 shifts the i-th coordinate of α to the $(i+k)$-th coordinate of β for some fixed k, where the indices are taken modulo p when $i + k > p$. Explicitly, $\beta = (x_k, x_{k+1}, \ldots, x_p, x_1, x_2, \ldots, x_{k-1})$ for some $1 \le k \le p$. Observe that these consist of the same elements as α, just in a different order. Moreover, observe that if $x_1 x_2 \cdots x_p = 1$, then $x_1 x_2 \cdots x_{k-1} = (x_k x_{k+1} \cdots x_p)^{-1}$. It follows that

$$x_k x_{k+1} \cdots x_p x_1 x_2 \cdots x_{k-1} = x_k x_{k+1} \cdots x_p (x_k x_{k+1} \cdots x_p)^{-1} = 1$$

so that $\beta \in \mathcal{S}$.

(c) Let $\alpha, \beta, \gamma \in \mathcal{S}$. We check the three properties of an equivalence relation:

- Reflexive: Since α shifted by 0 is itself, $\alpha \sim \alpha$.
- Symmetric: If $\alpha \sim \beta$, then β is a shift of α by some k. Then shifting β by $p - k$ returns α, hence $\beta \sim \alpha$.
- Transitive: If $\alpha \sim \beta$ and $\beta \sim \gamma$, then β is a shift of α by some k_1, and γ is a shift of β by some k_2. Then shifting α by $(k_1 + k_2) \pmod p$ returns γ, hence $\alpha \sim \gamma$.

$\boxed{\Rightarrow}$ Let $[\alpha]$ denote the equivalence class of $\sim$ that contains α, and let $\alpha = (x_1, x_2, \ldots, x_p)$. If $[\alpha]$ contains a single element, then every cyclic permutation of α is equal to α. In particular, the cyclic permutation that shifts each coordinate by 1 must be equal to α, hence $x_2 = x_1, x_3 = x_2, \ldots, x_p = x_{p-1}, x_1 = x_p$. It follows that $\alpha = (x, x, \ldots, x)$ for some $x \in G$. Since $\alpha \in \mathcal{S}$, $x^p = 1$.

$\boxed{\Leftarrow}$ 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.

(d) 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. Let $[\alpha]$ have n elements. Note that for any two coordinates x_i and x_j, if there exists some $k \in \mathbb{Z}$ such that $i + kn \equiv j \pmod p$, then $x_i = x_j$ since shifting α by kn returns α as there are only n distinct cyclic permutations in $[\alpha]$.

There are two cases to discuss, either $n = p$ or $1 \le n < p$. If $n = p$, then all cyclic permutations of α are distinct, and we are done. Suppose $1 \le n < p$. Since p is prime, $(n, p) = 1$, hence there exists some $k \in \mathbb{Z}$ such that $kn \equiv 1 \pmod p$. In particular, $i + kn \equiv i + 1 \equiv j \pmod p$ implies $x_{i+1} = x_j$. It follows that $x_i = x_j$ for all $1 \le i, j \le p$, 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.

(e) Note that $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, hence $k \ge 1$. From part (d), we have $|\mathcal{S}| = |G|^{p-1} = k + pd$. Since p divides $|G|$, it divides $|G|^{p-1}$, hence it divides $k + pd$. It follows that p divides k. Since $k \ge 1$, $k \ge p > 1$. In particular, there exists some equivalence class of size 1 that is not $\{(1, 1, \ldots, 1)\}$, hence by part (c), there exists some $x \in G$ with $x^p = 1$ and $x \ne 1$. Thus, G contains an element of order p. ∎

Exercise 3.2.10

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 $\text{lcm}(m, n) \leq |G : H \cap K| \leq mn$. 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, 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, 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, $(gh)^{-1}(gh') = h^{-1}h' \in H \cap K$, 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, $\ell = m|H : H \cap K|$, hence $m \mid \ell$. Similarly, $n \mid \ell$. Since ℓ is a multiple of both m and n, $\text{lcm}(m, n) \mid \ell$, hence $\text{lcm}(m, n) \leq \ell$, and we have the desired inequality $\text{lcm}(m, n) \leq \ell \leq mn$.

Lastly, if $(m, n) = 1$, then $\text{lcm}(m, n) = mn$ so that $\ell = mn$. ∎

Exercise 3.2.11

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, there are $|G : K| \cdot |K : H|$ distinct cosets of H in G, hence $|G : H| = |G : K| \cdot |K : H|$. ∎

Exercise 3.2.12

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 $\varphi(xH) = Hx^{-1}$. We claim that this map is well defined. Suppose $xH = yH$. Then

$$y^{-1}x \in H \implies (y^{-1}x)^{-1} = x^{-1}y \in H \implies Hx^{-1} = Hy^{-1}.$$

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 $|L| = |R|$. ∎

Exercise 3.2.13

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 $(1\,2\,3)(1\,2\,3\,4) = (1\,3\,4\,2) \neq (1\,3\,2\,4) = (1\,2\,3\,4)(1\,2\,3)$. Since $(1\,2\,3\,4) \in D_8$ and $(1\,2\,3) \in \langle(1\,2\,3)\rangle$, it follows that there exists elements of D_8 and $\langle(1\,2\,3)\rangle$ that do not commute in S_4. ∎

Exercise 3.2.14

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 $N \trianglelefteq S_4$, $N\langle\sigma\rangle \leq S_4$. Since $\sigma \notin S_4$, $N \cap \langle\sigma\rangle = 1$, 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. ■

Exercise 3.2.15

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 $G_i \cong S_{n-1}$. ■

Exercise 3.2.16

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 $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Solution. Let p be a prime. For any $a \in \mathbb{Z}$, then we either have $p \mid a$ or $p \nmid a$. If $p \mid a$, then $a \equiv 0 \pmod{p}$, hence $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's Theorem and Corollary 3.9, $|\overline{a}|$ divides $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, hence $\overline{a}^{p-1} = \overline{1}$. Then $a^{p-1} \equiv 1 \pmod{p}$, so $a^p \equiv a \pmod{p}$. ■

Exercise 3.2.17

Let p be a prime and let n be a positive integer. Find the order of $\overline{p}$ 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 $p^n \equiv 1 \pmod{}(p^n - 1)$, $|\overline{p}| \leq n$. Suppose $d < n$ such that $p^d \equiv 1 \pmod{}(p^n - 1)$. Then $p^n - 1 \mid p^d - 1$ so that $p^n - 1 \leq p^d - 1$, a contradiction. It follows that $|\overline{p}| = n$. By Lagrange's Theorem, $|\overline{p}| = n$ divides $|(\mathbb{Z}/(p^n - 1)\mathbb{Z})^\times| = \varphi(p^n - 1)$. ■

Exercise 3.2.18

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 $N \trianglelefteq G$, $HN \leq G$. 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 $(|H|, |G : N|) = 1$, $n = 1$ so that $|H| = |H \cap N|$. It follows that $H = H \cap N$, hence $H \leq N$. ■

Exercise 3.2.19

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, $M = N$. ■

Exercise 3.2.20

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. Let $x \in A \cap B$ and $ab \in AB$ where $a \in A$ and $b \in B$. Note that

$$(ab)(x)(ab)^{-1} = a(bxb^{-1})a^{-1}$$

Since $A \trianglelefteq G$, $bxb^{-1} \in A$. Moreover, since A is abelian, $a(bxb^{-1})a^{-1} = bxb^{-1} \in A$. Also, since $x, b \in B$ and $B \leq G$, $bxb^{-1} \in B$. It follows that $(ab)x(ab)^{-1} \in A \cap B$, hence $A \cap B \trianglelefteq AB$. ■

Exercise 3.2.21

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. ■

Exercise 3.2.22

Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\phi(n)} \equiv 1 \pmod{n}$ 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 $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, $|\bar{a}|$ divides $\varphi(n)$, hence $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Exercise 3.2.23

Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \pmod{\varphi}(100)$ 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 $3^4 \pmod 4 0 = 81 \pmod 4 0 \equiv 1 \pmod 4 0$, $3^{100} \pmod 4 0 \equiv 1 \pmod 4 0$. It follows that $3^{100} = 1 + 40k = 1 + \varphi(100)k$ for some $k \in \mathbb{Z}$, hence

$$3^{3^{100}} = 3^{1+\varphi(100)k} = 3 \cdot 3^{\varphi(100)^k} \equiv 3 \cdot 1^k \pmod 1 00 = 3 \pmod 1 00$$

so that the last two digits of $3^{3^{100}}$ are 03. ■

3.3 The Isomorphism Theorems

Let G be a group.

Exercise 3.3.1

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, $|F^\times| = q - 1$. We then have that $|\mathrm{GL}_n(F) : \mathrm{SL}_n(F)| = |F^\times| = q - 1$. ■

Exercise 3.3.2

Prove all parts of the Lattice Isomorphism Theorem.

Solution. Let $\mathcal{A} = \{A \leq G \mid N \subseteq A\}$ be the set of subgroups of G containing N. Let $\overline{\mathcal{A}} = \{\overline{A} \leq \overline{G}\}$ be the set of subgroups of $\overline{G} = G/N$. Define the map

$$\varphi \colon \mathcal{A} \to \overline{\mathcal{A}} \quad \text{by} \quad \varphi(A) = \overline{A} = A/N$$

We first show that $\varphi(A) \leq \overline{G}$. Since $1 \in A$ for any $A \in \mathcal{A}$, $1N = N \in \overline{A}$ so that $\overline{1} \in \overline{A}$, hence $\overline{A}$ is nonempty. Let $\overline{a}, \overline{b} \in \overline{A}$, where $a, b \in A$. Since $A \leq G$, $ab^{-1} \in A$, hence

$$\overline{a}\overline{b}^{-1} = \overline{ab^{-1}} \in \overline{A}$$

so that $\overline{A} \leq \overline{G}$.

Next, we show that φ is surjective. Let $\overline{A} \in \overline{\mathcal{A}}$, and let $\pi \colon G \to \overline{G}$ be the natural projection homomorphism. Consider $\pi^{-1}(\overline{A})$. Since π is a homomorphism, $\pi^{-1}(\overline{A}) \leq G$. Moreover, since $\overline{1} \in \overline{A}$, $N = \pi^{-1}(\overline{1}) \subseteq \pi^{-1}(\overline{A})$ so that $\pi^{-1}(\overline{A}) \in \mathcal{A}$. Note that

$$\varphi(\pi^{-1}(\overline{A})) = \pi^{-1}(\overline{A})/N = \overline{A}$$

so that φ is surjective. To show that φ is injective, 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) $\boxed{\Rightarrow}$ Suppose $A \leq B$ for $A, B \in \mathcal{A}$. Let $\overline{a} \in \overline{A}$ for some $a \in A$. Since $A \leq B$, $a \in B$ so that $\overline{a} \in \overline{B}$, hence $\overline{A} \leq \overline{B}$.
$\boxed{\Leftarrow}$ Suppose $\overline{A} \leq \overline{B}$ for $A, B \in \mathcal{A}$. Let $a \in A$ 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) Define the map

$$\psi \colon B/A \to \overline{B}/\overline{A} \quad \text{by} \quad \psi(bA) = \overline{b}\,\overline{A}$$

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 $\overline{b_2^{-1}b_1} \in \overline{A}$. Then $\overline{b_1}\,\overline{A} = \overline{b_2}\,\overline{A}$, hence $\psi(b_1A) = \psi(b_2A)$.

Suppose $bA \in \ker\psi$. Then $\psi(bA) = \overline{A}$ so that $\overline{b}\,\overline{A} = \overline{A}$. Then $\overline{b} \in \overline{A}$, hence $bN \in A/N$, and $b \in A$. Then $bA = A$ which is the identity in B/A so that $\ker\psi = 1$, hence ψ is injective. To show that ψ is surjective, let $\overline{b}\,\overline{A} \in \overline{B}/\overline{A}$ for $\overline{b} \in B$. By definition of $\overline{B}$, there exists $b \in B$ such that $\overline{b} = bN$. Then $\psi(bA) = \overline{b}\,\overline{A}$, hence ψ is surjective. Lastly, for any $b_1A, b_2A \in B/A$,

$$\psi(b_1A \cdot b_2A) = \psi(b_1b_2A) = \overline{b_1b_2}\,\overline{A} = \overline{b}_1\overline{b}_2\overline{A} = \psi(b_1A) \cdot \psi(b_2A)$$

so that ψ is a homomorphism. Therefore, ψ is an isomorphism and $|B : A| = |B/A| = |\overline{B}/\overline{A}| = |\overline{B} : \overline{A}|$.

(3) Let $\overline{x} \in \overline{\langle A, B\rangle}$. Then $x \in \langle A, B\rangle$ so that $x = x_1x_2 \dots x_n$ where $x_i \in A \cup B$ for each $1 \leq i \leq n$. It follows that

$$\overline{x} = \overline{x_1x_2 \dots x_n}$$

where $\overline{x_i} \in \overline{A} \cup \overline{B}$ for each $1 \leq i \leq n$, hence $\overline{x} \in \langle \overline{A}, \overline{B}\rangle$, and $\overline{\langle A, B\rangle} \subseteq \langle \overline{A}, \overline{B}\rangle$.

Conversely, let $\overline{x} \in \langle \overline{A}, \overline{B}\rangle$. Then $\overline{x} = \overline{x_1x_2 \dots x_n}$ where $\overline{x_i} \in \overline{A} \cup \overline{B}$ for each $1 \leq i \leq n$. It follows that $x = x_1x_2 \dots x_n$ where $x_i \in A \cup B$ for each $1 \leq i \leq n$, hence $x \in \langle A, B\rangle$ so that $\overline{x} \in \overline{\langle A, B\rangle}$. Therefore, $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.

(4) Let $\overline{x} \in \overline{A \cap B}$. Then $x \in A \cap B$ so that $x \in A$ and $x \in B$, hence $\overline{x} \in \overline{A}$ and $\overline{x} \in \overline{B}$, so that $\overline{x} \in \overline{A} \cap \overline{B}$. It follows that $\overline{A \cap B} \subseteq \overline{A} \cap \overline{B}$.

Conversely, let $\overline{x} \in \overline{A} \cap \overline{B}$. Then $\overline{x} \in \overline{A}$ and $\overline{x} \in \overline{B}$, so that $x \in A$ and $x \in B$, hence $x \in A \cap B$ so that $\overline{x} \in \overline{A \cap B}$. Therefore, $\overline{A \cap B} = \overline{A} \cap \overline{B}$.

(5) $\boxed{\Rightarrow}$ Suppose $A \trianglelefteq G$ for some $A \in \mathcal{A}$. Let $\overline{g} \in \overline{G}$ and $\overline{a} \in \overline{A}$ for some $g \in G$ and $a \in A$. Note that

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

Since $A \trianglelefteq G$, $gag^{-1} \in A$, hence $\overline{gag^{-1}} \in \overline{A}$. It follows that $(\overline{g})(\overline{a})(\overline{g})^{-1} \in \overline{A}$, hence $\overline{A} \trianglelefteq \overline{G}$.
$\boxed{\Leftarrow}$ Suppose $\overline{A} \trianglelefteq \overline{G}$ for some $A \in \mathcal{A}$. Let $g \in G$ and $a \in A$. Since $\overline{gag^{-1}} = (\overline{g})(\overline{a})(\overline{g})^{-1} \in \overline{A}$, $gag^{-1}N \in A/N$, hence $gag^{-1} \in A$. It follows that $A \trianglelefteq G$. ■

Exercise 3.3.3

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 $H \trianglelefteq G$ and $K \leq G$, $HK \leq G$ by Corollary 3.15. By Proposition 3.14, $HK = KH$. By Exercise 3.2.11, we have

$$|G : H| = |G : HK| \cdot |HK : H|.$$

Since $|G : H| = p$ is prime, we have two cases:
(1) If $|G : HK| = 1$, then $G = HK$. By the Second Isomorphism Theorem, we have

$$K/(K \cap H) \cong KH/H = G/H$$

so that $|K : K \cap H| = |KH : H| = |G : H| = p$.
(2) If $|G : HK| = p$, then $|HK : H| = 1$, hence $HK = H$. It follows that $K \leq H$. ■

Exercise 3.3.4

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. Define the map

$$\varphi : A \times B \to (A/C) \times (B/D) \quad \text{by} \quad \varphi(a, b) = (aC, bD)$$

for $a \in A$ and $b \in B$. It is easy to see that φ is well defined. Moreover, for any $(a_1, b_1), (a_2, b_2) \in A \times B$,

$$\varphi((a_1, b_1)(a_2, b_2)) = \varphi(a_1a_2, b_1b_2) = (a_1a_2C, b_1b_2D) = (a_1C, b_1D)(a_2C, b_2D) = \varphi(a_1, b_1)\varphi(a_2, b_2)$$

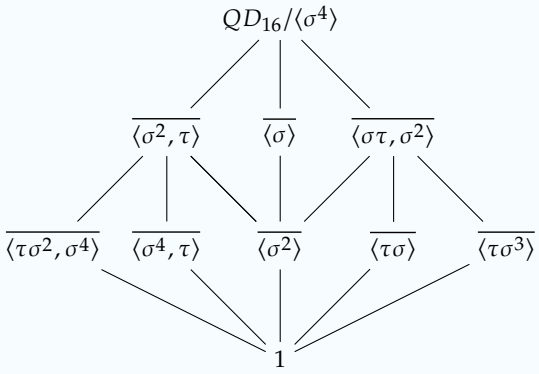
so that φ is a homomorphism. To show that φ is surjective, let $(aC, bD) \in (A/C) \times (B/D)$ for some $a \in A$ and $b \in B$. Then $\varphi(a, b) = (aC, bD)$, hence φ is surjective. Lastly, suppose $(a, b) \in \ker \varphi$. Then $\varphi(a, b) = (C, D)$ so that $aC = C$ and $bD = D$. It follows that $a \in C$ and $b \in D$, hence $(a, b) \in C \times D$. Therefore, $\ker \varphi = C \times D$, so that by the First Isomorphism Theorem, $C \times D \trianglelefteq A \times B$ and

$$(A \times B)/(C \times D) \cong (A/C) \times (B/D).$$ ■

Exercise 3.3.5

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:

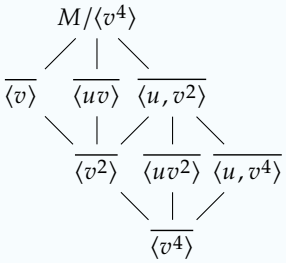


Moreover, $\overline{\sigma^4} = \overline{\tau^2} = \overline{1}$ and $\overline{\tau\sigma} = \overline{\sigma^3\tau} = \overline{\sigma^{-1}\tau}$, then the generators $\overline{\sigma}$ and $\overline{\tau}$ satisfy the relations as r and s do in D_8, hence $QD_{16}/\langle\sigma^4\rangle \cong D_8$. ■

Exercise 3.3.6

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:

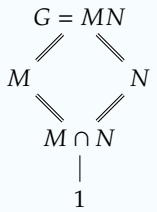


Moreover, $\overline{v^4} = \overline{u^2} = \overline{1}$ and $\overline{vu} = \overline{uv^5} = \overline{uv}$ so that the generators of $M/\langle v^4\rangle$ satisfy the relations as a and b do in $Z_2 \times Z_4$, whose presentation is given in Exercise 2.5.12. Then $M/\langle v^4\rangle \cong Z_2 \times Z_4$. ■

Exercise 3.3.7

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 $G/(M \cap N)$:



Consider the mapping

$$\varphi : G \to (G/M) \times (G/N) \quad \text{by} \quad \varphi(g) = (gM, gN)$$

for $g \in G$. It is easy to see that φ is well defined. Moreover, for any $g_1, g_2 \in G$,

$$\varphi(g_1g_2) = (g_1g_2M, g_1g_2N) = (g_1M, g_1N)(g_2M, g_2N) = \varphi(g_1)\varphi(g_2)$$

so that φ is a homomorphism. To show that φ is surjective, let $(g_1M, g_2N) \in (G/M) \times (G/N)$ for some $g_1, g_2 \in G$. Since $G = MN = NM$, there exists $m, m' \in M$ and $n, n' \in N$ such that $g_1 = nm$ and $g_2 = m'n'$. Then $g_1M = nM$ and $g_2N = m'N$, so that

$$\varphi(nm') = (nm'M, nm'N) = (nM, m'N) = (g_1M, g_2N)$$

so that φ is surjective. Lastly, suppose $g \in \ker\varphi$. Then $\varphi(g) = (M, N)$ so that $gM = M$ and $gN = N$. It follows that $g \in M$ and $g \in N$, hence $g \in M \cap N$. Therefore, $\ker\varphi = M \cap N$, so that by the First Isomorphism Theorem, we have

$$G/(M \cap N) \cong (G/M) \times (G/N). \qquad \blacksquare$$

Exercise 3.3.8

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. Suppose $y \in G$. Then y is a p^n-th root of unity for some $n \in \mathbb{Z}^+$, so that $y = e^{2\pi ik/p^n}$ for some $k \in \mathbb{Z}$. Let $z = e^{2\pi ik/p^{n+1}}$, so that $z^p = e^{2\pi ik/p^n} = y$. Then because $z \in G$, φ is surjective.

Now $\ker\varphi = \{z \in G \mid z^p = 1\} = \{e^{2\pi ik/p} \mid k = 0, 1, \ldots, p-1\}$, which is a nontrivial subgroup of G. By the First Isomorphism Theorem, we have $G/\ker\varphi \cong \varphi(G) = G$, hence G is isomorphic to a proper quotient of itself. $\blacksquare$

Exercise 3.3.9

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 $P \cap N \leq P$, $|P \cap N|$ divides $|P| = p^a$. Similarly, since $P \cap N \leq N$, $|P \cap N|$ divides $|N| = p^b n$. It follows that $|P \cap N|$ divides $\gcd(p^a, p^b n) = p^b$, hence $|P \cap N| = p^c$ for some $c \leq b$. By the Second Isomorphism Theorem, we have

$$PN/N \cong P/(P \cap N)$$

so that $|PN/N| = |P|/|P \cap N| = p^{a-c}$. Since $PN/N \leq G/N$, $|PN/N|$ divides $|G/N|$. It follows that p^{a-c} divides $|G|/|N| = (p^a m)/(p^b n) = p^{a-b}(m/n)$. Since p does not divide m/n, p^{a-c} divides p^{a-b}, hence $c \geq b$. Therefore, $c = b$ so that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. $\blacksquare$

Exercise 3.3.10

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. $\blacksquare$

3.4 Composition Series and the Hölder Program

Exercise 3.4.1

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 abelian, every subgroup of G is normal. Moreover, simplicity of G implies that its only subgroups are 1 and G. If G is the trivial group, then $G \cong Z_1$. Suppose G is nontrivial, and let $g \in G$ be nonidentity. Then $\langle g \rangle \leq G$. Since $g \neq 1$ and G is simple, $\langle g \rangle = G$, hence G is cyclic.

Assume, by way of contradiction, that $|G|$ is not prime. We have two cases:

- Suppose $|G|$ is infinite. Then $G \cong \mathbb{Z}$ has infinitely many proper nontrivial subgroups, contradicting the simplicity of G.
- Suppose $|G|$ is finite and composite. Then there exists some divisor d of $|G|$ such that $1 < d < |G|$. Since G is cyclic, there exists a unique subgroup of G of order d, contradicting the simplicity of G.

Therefore, $|G|$ is prime, and $G \cong Z_p$ for some prime p. ■

Exercise 3.4.2

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. ■

Exercise 3.4.3

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, QD_{16} is solvable. ■

Exercise 3.4.4

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. We now proceed by induction on m.

Suppose that every finite abelian group of order strictly less than m has a subgroup of order n for each positive divisor n of its order. 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.

If 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 n divides m, k divides m/p. By the inductive hypothesis, there exists a subgroup $\overline{H}$ of $G/\langle h \rangle$ such that $|\overline{H}| = k$. 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. ■

Exercise 3.4.5

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. Define the subgroups

$$H_i = H \cap G_i \quad \text{for each } 0 \leq i \leq n$$

Then $H_0 = H \cap G_0 = 1$ and $H_n = H \cap G_n = H$. It is clear that $H_i \leq H_{i+1}$ for each $0 \leq i \leq n-1$. To show that $H_i \trianglelefteq H_{i+1}$, let $g \in H_{i+1}$ and $x \in H_i$. Then $g \in G_{i+1}$ and $x \in G_i$. Since $G_i \trianglelefteq G_{i+1}$, $gxg^{-1} \in G_i$. Since $g, x \in H$, $gxg^{-1} \in H$, hence $gxg^{-1} \in H_i$. It follows that $H_i \trianglelefteq H_{i+1}$. By the Second Isomorphism Theorem, we have

$$H_{i+1}/H_i \cong H_{i+1}G_i/G_i \leq G_{i+1}/G_i$$

Since G_{i+1}/G_i is abelian, 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

$$N_i = G_iN \quad \text{for each } 0 \leq i \leq n$$

Since it is clear that $N_i \leq N_{i+1}$, we need to show that $N_i \trianglelefteq N_{i+1}$. Let $g \in G_{i+1}$, $h \in G_i$, and $n_1, n_2 \in N$. Then

$$(gn_1)(hn_2)(gn_1)^{-1} = gn_1hn_2n_1^{-1}g^{-1} = g(n_1hn_2n_1^{-1})g^{-1}$$

Note that $n_1hn_2n_1^{-1} \in N_i$ since $h \in G_i \leq G$ and $N \trianglelefteq G$. Since $G_i \trianglelefteq G_{i+1}$, $g(n_1hn_2n_1^{-1})g^{-1} \in G_i \subseteq N_i$. It follows that $N_i \trianglelefteq N_{i+1}$.

Lastly, by the Lattice Isomorphism Theorem, then $N_i/N \trianglelefteq N_{i+1}/N$, and the Third Isomorphism Theorem concludes that

$$(N_{i+1}/N)/(N_i/N) \cong N_{i+1}/N_i \cong G_{i+1}/(G_iN \cap G_{i+1}) = G_{i+1}/G_i$$

Since G_{i+1}/G_i is abelian, so is $(N_{i+1}/N)/(N_i/N)$. Therefore, G/N is solvable with the chain

$$1 = N_0/N \trianglelefteq N_1/N \trianglelefteq \cdots \trianglelefteq N_n/N = G/N.$$ ■

Exercise 3.4.6

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, 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. ■

Exercise 3.4.7

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, $|H| < |G|$, 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 $|G/H| < |G|$, 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, 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. ■

Exercise 3.4.8

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, $0 \le i \le s-1$.

(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, $0 \le i \le t-1$.

[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) $\boxed{\Rightarrow}$ (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 $|A/\langle a \rangle| < |A|$, 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, 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) $\boxed{\Rightarrow}$ (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, $G/H_{s-1} \cong Z_n$ for some $n \in \mathbb{Z}^+$. If n is prime, then the composition factors of G/H_{s-1} are of prime order. Since $|H_{s-1}| < |G|$, 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 $\pi\colon G \to G/H_{s-1}$ 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) $\boxed{\Rightarrow}$ (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, 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) $\boxed{\Rightarrow}$ (i): This implication is immediate from the definition of solvable groups. ∎

Exercise 3.4.9

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, 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:

$$G/N_{r-1} \cong M_1/(N_{r-1} \cap M_1) \cong M_1 \quad \text{and} \quad N_{r-1}/1 \cong N_{r-1} \cong G/M_1$$ ∎

Exercise 3.4.10

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 $\min\{r-1, s-1\} = k-1 < k$, 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. ■

Exercise 3.4.11

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 $H_n = H$, 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

$$H_k \cong H_k/1 = H_k/(H_k \cap G_{k-1}) \cong H_kG_{k-1}/G_{k-1} \leq G_k/G_{k-1}$$

Since G_k/G_{k-1} is abelian, so is H_k. Therefore, $A = H_k$ is a nontrivial, abelian normal subgroup of G contained in H. ■

Exercise 3.4.12

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)** $\boxed{\Rightarrow}$ **(ii)** Suppose every group of odd order is solvable. Let G be a simple group of odd order. Since G is solvable, by the characterization of solvable groups, all composition factors of G are of prime order. Since G is simple, its only composition series is $1 \trianglelefteq G$, hence G is of prime order.
(ii) $\boxed{\Rightarrow}$ **(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

Exercise 3.5.1

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 $\sigma\tau$, while even permutations are σ, σ^2, and $\tau^2\sigma$. ■

Exercise 3.5.2

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. ■

Exercise 3.5.3

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 $n \ge 1$. ■

Exercise 3.5.4

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 $S_n = \langle (1\ 2), (1\ 2\ 3\ ldots\ n)\rangle$. ■

Exercise 3.5.5

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 $S_p = \langle \sigma, \tau\rangle$. ■

Exercise 3.5.6

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 $\varphi\colon D_8 \to \langle\sigma, \tau\rangle$ 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, $\langle\sigma, \tau\rangle \cong D_8$. ■

Exercise 3.5.7

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. ■

Exercise 3.5.8

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. ■

Exercise 3.5.9

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 $H = \langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is isomorphic to V_4. Moreover, H is generated by all elements of order 2 in A_4. By Exercise 3.1.26, this subgroup is normal in A_4. ■

Exercise 3.5.10

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. ■

Exercise 3.5.11

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. ■

Exercise 3.5.12

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 map 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 $\varphi(\sigma) = \varphi(\tau)$, 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}. ■

Exercise 3.5.13

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. ■

Exercise 3.5.14

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, $\langle\sigma, \tau\rangle = A_4$. ■

Exercise 3.5.15

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 $\langle x, y\rangle = A_4$. ■

Exercise 3.5.16

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 $\{1, \ldots, 5\}$, then $\langle x, y\rangle \cong A_4$.
(b) Prove that if x and y do not fix a common element of $\{1, \ldots, 5\}$, 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 $\varphi\colon \langle x,y\rangle \to S_4$ 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 Lagrange's Theorem then $\langle x,y\rangle$ must have order of at least 60, hence $\langle x,y\rangle = A_5$. ■

Exercise 3.5.17

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 $\varphi\colon \langle x,y\rangle \to Z_3 \times Z_3$ 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.

Exercise 4.1.1

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

$$\bigcap_{b \in A} G_b = \bigcap_{g \in G} gG_ag^{-1}.$$

■

Exercise 4.1.2

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

$$\bigcap_{b \in A} G_b = \bigcap_{\sigma \in G} \sigma G_a\sigma^{-1} = 1.$$

■

Exercise 4.1.3

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, 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. ■

Exercise 4.1.4

Let S_3 act on the set Ω of ordered pairs $\{(i,j) \mid 1 \le i,j \le 3\}$ 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 $\mathcal{O}$ of S_3 acting on these nine points, pick some $a \in \mathcal{O}$ 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

$$\mathcal{O}_1 = \{(i,i) \mid i \in \{1,2,3\}\} \quad \text{and} \quad \mathcal{O}_2 = \{(i,j) \mid i \neq j\}$$

of S_3 acting on Ω. Note that $|\mathcal{O}_1| = 3$ and $|\mathcal{O}_2| = 6$. 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 $\mathcal{O}_1$, 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 $|G_a||\mathcal{O}_1| = 2 \cdot 3 = 6 = |S_3|$ as expected. For $\mathcal{O}_2$, 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, $|G_a||\mathcal{O}_2| = 1 \cdot 6 = 6 = |S_3|$. ■

Exercise 4.1.5

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 $\{(i,j,k) \mid 1 \le i,j,k \le 3\}$

(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 combining 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:

- $\mathcal{O}_1 = \{(i,i,i) \mid i \in \{1,2,3\}\}$ with order 3.
- $\mathcal{O}_2 = \{(i,i,j) \mid i \neq j\}$ with order 6.
- $\mathcal{O}_3 = \{(i,j,i) \mid i \neq j\}$ with order 6.
- $\mathcal{O}_4 = \{(j,i,i) \mid i \neq j\}$ with order 6.
- $\mathcal{O}_5 = \{(i,j,k) \mid i,j,k \text{ distinct}\}$ 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 $\mathcal{O}_1$, 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 $|G_a||\mathcal{O}_1| = 2 \cdot 3 = 6 = |S_3|$. 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 $\mathcal{O}_2$, 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 $|G_a||\mathcal{O}_2| = 1 \cdot 6 = 6 = |S_3|$. The same logic applies to $\mathcal{O}_3$, $\mathcal{O}_4$, and $\mathcal{O}_5$.

(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 $\mathcal{P}(\{1,2,3\}) - \{\varnothing\}$:

- $\mathcal{O}_1 = \{\{1\},\{2\},\{3\}\}$ with order 3.
- $\mathcal{O}_2 = \{\{1,2\},\{1,3\},\{2,3\}\}$ with order 3.
- $\mathcal{O}_3 = \{\{1,2,3\}\}$ 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 $|G_a||O_3| = 6 \cdot 1 = 6 = |S_3|$. ■

Exercise 4.1.6

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

$$(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3).$$ ■

Exercise 4.1.7

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 $\sigma(B) \cap B = \varnothing$ (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 $1(B) = B$, $1 \in G_B$, 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 $a \in B$, $\sigma(a) \in \sigma(B)$. But $\sigma(a) = a \in B$, so $\sigma(B) \cap B \neq \varnothing$. 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 $\sigma_i(B) \cap \sigma_j(B) \neq \varnothing$. Then there are $b, b' \in B$ such that $\sigma_i(b) = \sigma_j(b')$, or $(\sigma_j^{-1}\sigma_i)(b) = b'$, hence $\sigma_j^{-1}\sigma_i(B) \cap B \neq \varnothing$. Since B is a block, $\sigma_j^{-1}\sigma_i(B) = B$, 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 $\sigma(B) \cap B \neq \varnothing$ 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 $\sigma(B) \cap B = \varnothing$. Thus, B is a nontrivial block, and D_8 is not primitive in its action on the four vertices of a square.

(d) $\boxed{\Rightarrow}$ 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 $H \leq G$, $1 \cdot a = a \in B$. 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 $G_a \leq H$, $H = G_a$. 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. $\boxed{\Leftarrow}$ 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 $a \in B$, $\sigma(a) \in \sigma(B)$, so $\sigma(a) \in B$. Therefore, $\sigma(a) = a \in B$, and it follows that $\sigma(B) \cap B \neq \varnothing$. 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 $\sigma \in G_B$, $\sigma(B) = B$, 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. ■

Exercise 4.1.8

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 $n - 1 \geq 1$, 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 $\sigma \in G_a$, $\sigma(B) = B$, 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), it is not doubly transitive. ■

Exercise 4.1.9

[4.1.9] Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$, in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$ (i.e., in the notation of Exercise 7 the sets $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are blocks). Prove that G is transitive on $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.

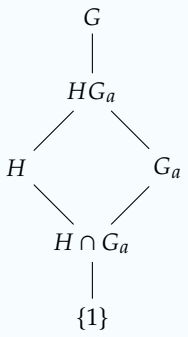
(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$. [Draw the sublattice describing the Second Isomorphism Theorem for the subgroups H and G_a of G. Note that $H \cap G_a = H_a$.]

Solution.

(a) Let $g \in G$ and $\mathcal{O}_i$ be an orbit of H on A. Let $a \in \mathcal{O}_i$ so that $\mathcal{O}_i = H \cdot a = \{h \cdot a \mid h \in H\}$. Consider the set $g\mathcal{O}_i = \{g \cdot (h \cdot a) \mid h \in H\}$. Since H is normal in G, for any $h \in H$, we have $ghg^{-1} \in H$. Then $g\mathcal{O}_i = H \cdot (g \cdot a)$, which is the orbit of H containing $g \cdot a$. Therefore, there exists some j such that $g\mathcal{O}_i = \mathcal{O}_j$.

To show that G is transitive on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$, let $\mathcal{O}_i$ and $\mathcal{O}_j$ be any two orbits of H on A. Since G is transitive on A, for some $a \in \mathcal{O}_i$ and $b \in \mathcal{O}_j$, there exists some $g \in G$ such that $g \cdot a = b$. Then $g\mathcal{O}_i$ is the orbit of H containing b, hence $g\mathcal{O}_i = \mathcal{O}_j$. Therefore, G is transitive on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$. Since G is transitive on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$, all orbits of H on A have the same cardinality.

(b) Suppose $a \in \mathcal{O}_1$. By Proposition 4.2, we have $|\mathcal{O}_1| = |H : H_a|$. Since $H_a = H \cap G_a$, $|\mathcal{O}_1| = |H : H \cap G_a|$. Moreover, the orbits of H partition A and have the same size by the previous solution, so we have $|A| = r|\mathcal{O}_1|$. By applying Proposition 4.2 again, we have $|A| = |G : G_a|$. Therefore, $|G : G_a| = r|\mathcal{O}_1| = r|H : H \cap G_a|$. 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:



■

Exercise 4.1.10

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 $x_1K, \dots, x_nK$ where $\{x_1K, \dots, x_nK\}$ 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 $\{x_1K, \dots, x_nK\}$ 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 $x_iK \in \mathcal{O}$, 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 $x_1K, \dots, x_nK$.

(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, 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 Multiplication–Cayley's Theorem

Exercise 4.2.1

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 labelling).

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). ■

Exercise 4.2.2

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:

$$\begin{aligned}
(1\,2) \cdot 1 &= (1\,2) & \sigma_{(1\,2)}(1) &= 2 \\
(1\,2) \cdot (1\,2) &= 1 & \sigma_{(1\,2)}(2) &= 1 \\
(1\,2) \cdot (2\,3) &= (1\,2\,3) & \sigma_{(1\,2)}(4) &= 5 \\
(1\,2) \cdot (1\,3) &= (1\,3\,2) & \sigma_{(1\,2)}(3) &= 6 \\
(1\,2) \cdot (1\,2\,3) &= (2\,3) & \sigma_{(1\,2)}(5) &= 3 \\
(1\,2) \cdot (1\,3\,2) &= (1\,3) & \sigma_{(1\,2)}(6) &= 4
\end{aligned}$$

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 $(1\,2)(2\,3) = (1\,2\,3)$,

$$(1\,2\,3) \mapsto (1\,2)(3\,6\,4\,5)(1\,3\,5\,2)(4\,6) = (1\,5\,6)(2\,4\,3)$$

Continuing in this way, we find that the images of the elements of S_3 under the left regular representation are as follows:

$$\begin{aligned}
1 &\mapsto 1 \\
(1\,2) &\mapsto (1\,2)(3\,6\,4\,5) \\
(2\,3) &\mapsto (1\,3\,5\,2)(4\,6) \\
(1\,3) &\mapsto (1\,4)(2\,6)(3\,5) \\
(1\,2\,3) &\mapsto (1\,5\,6)(2\,4\,3) \\
(1\,3\,2) &\mapsto (1\,6\,5)(2\,3\,4)
\end{aligned}$$

■

Exercise 4.2.3

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. ■

Exercise 4.2.4

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

$$\begin{aligned} i &\mapsto \sigma_i = (1\,3\,2\,4)(5\,7\,6\,8) \\ j &\mapsto \sigma_j = (1\,5\,2\,6)(3\,8\,4\,7) \end{aligned}$$

Hence $Q_8 \cong \langle \sigma_i, \sigma_j \rangle \leq S_8$. ■

Exercise 4.2.5

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, 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, $\widehat{H} = \widehat{K}$. ■

Exercise 4.2.6

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, 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. ■

Exercise 4.2.7

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 $\mathcal{O}_a$ of a under this action. By Proposition 4.2, we have $|\mathcal{O}_a| = |Q_8 : (Q_8)_a|$, where $(Q_8)_a$ is the stabilizer of a in Q_8. Since $|\mathcal{O}_a|$ divides $|A| \leq 7$, $|\mathcal{O}_a|$ must be 1, 2, 4, or 7. However, since Q_8 has no subgroup of index 7, $|\mathcal{O}_a|$ cannot be 7. If $|\mathcal{O}_a| = 4$, then $(Q_8)_a$ has order 2, but the only subgroup of order 2 in Q_8 is $\langle -1\rangle$. If $|\mathcal{O}_a| = 2$, 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 $|\mathcal{O}_a| = 1$, 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 $a \in A$, $\langle -1\rangle$ 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 $n \leq 7$. ■

Exercise 4.2.8

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 $\varphi\colon G \to S_n$, which is the permutation representation of G on G/H. Let $K = \ker(\varphi) \subseteq H$, since $g \in K$ if and only if $gxH = xH$ for all $x \in G$. Taking $x = 1$, we have $gH = H$, so that $g \in H$. By the First Isomorphism Theorem, we have $G/K \cong \varphi(G) \leq S_n$, so that $|G : K| = |G/K| = |\varphi(G)|$ divides $|S_n| = n!$. Therefore, $|G : K| \leq n!$. ■

Exercise 4.2.9

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 $\varphi\colon G \to S_p$. Since $|G| = p^\alpha$, 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, $\varphi(G)$ 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, by the First Isomorphism Theorem, we have $|G : \ker(\varphi)| = p$. But since $\ker(\varphi) \subseteq H$ and both have index p, $\ker(\varphi) = H$. 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. ■

Exercise 4.2.10

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 $H \trianglelefteq G$, $gHg^{-1} = H$. 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, $G = hk$ 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 $\varphi\colon G \to S_3$. Since H is not normal in G, the action is nontrivial, so φ is injective. Therefore, $G \cong \varphi(G) \leq S_3$. Since $|G| = 6 = |S_3|$, $\varphi(G) = S_3$, and hence $G \cong S_3$. ■

Exercise 4.2.11

Let G be a finite group and let $\pi\colon G \to S_G$ 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 $|x| = n$, $|O_g| = n$ 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 $|O_g| = n$, $(\langle x \rangle)_g$ 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. ■

Exercise 4.2.12

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 $\varepsilon \circ \pi\colon G \to \{\pm 1\}$. Since $\pi(G)$ contains an odd permutation, $\varepsilon \circ \pi$ is surjective. By the First Isomorphism Theorem, we have $G/\ker(\varepsilon \circ \pi) \cong \{\pm 1\}$, so that $|\ker(\varepsilon \circ \pi)| = |G|/2$. Therefore, $\ker(\varepsilon \circ \pi)$ is a subgroup of G of index 2. ■

Exercise 4.2.13

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, 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. ■

Exercise 4.2.14

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.

Exercise 4.3.1

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. ■

Exercise 4.3.2

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. ■

Exercise 4.3.3

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 $C_{S_3}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$, 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. ■

Exercise 4.3.4

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 $n \in N_G(S)$, 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 $n \in C_G(S)$, 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, $gC_G(S)g^{-1} = C_G(gSg^{-1})$. ■

Exercise 4.3.5

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, $|\mathcal{K}_g| \leq n$. ■

Exercise 4.3.6

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, $Z(G) \neq G$. 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 $\langle g \rangle \leq C_G(g)$, $|C_G(g)|$ 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 $15 = 1 + 3 + 3 + 3 + 5$. ■

Exercise 4.3.7

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)

■

Exercise 4.3.8

Prove that $Z(S_n) = 1$ for all $n \geq 3$.

Solution. Suppose $\sigma \in Z(S_n)$ for some $n \geq 3$. Pick some $a \in \{1, 2, \ldots, n\}$. Pick some $b, c \in \{1, 2, \ldots, n\} - \{a\}$ with $b \neq c$. Then $\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b)) = (a\ b)$, so $\{\sigma(a), \sigma(b)\} = \{a, b\}$. Moreover, $\sigma(a\ c)\sigma^{-1} = (\sigma(a)\ \sigma(c)) = (a\ c)$, so $\{\sigma(a), \sigma(c)\} = \{a, c\}$. Then $\sigma(a) \in \{a, b\}$ and $\sigma(a) \in \{a, c\}$, so $\sigma(a) = a$. Since a was arbitrary, σ fixes all elements of $\{1, 2, \ldots, n\}$. ■

Exercise 4.3.9

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 $n \geq 4$. ■

Exercise 4.3.10

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 $\tau = (2\,4\,5\,3)$. ■

Exercise 4.3.11

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 $\tau = (1\,2\,3\,4\,5)$. ■

Exercise 4.3.12

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)

■

Exercise 4.3.13

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, $|\mathcal{K}| = |G| - 1$. Therefore, $|G : C_G(g)| = |G| - 1$, which implies that $|C_G(g)| = |G|/(|G| - 1)$. Since $|C_G(g)|$ is an integer, $|G| - 1$ 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. ■

Exercise 4.3.14

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 $\tau \circ \pi_1(a) \circ \tau^{-1} = (2\ 4)(1\ 2)(3\ 4)(2\ 4) = (1\ 4)(2\ 3) = \pi_2(a)$. ■

Exercise 4.3.15

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 $\tau = (5\ 2\ 3)(6\ 4\ 7)$. ■

Exercise 4.3.16

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 $\tau = (2\ 3)$. ■

Exercise 4.3.17

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, $M(\tau\sigma\tau^{-1})$ is finite. Therefore, $\tau\sigma\tau^{-1} \in D$. ■

Exercise 4.3.18

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 $A - F(H)$. ■

Exercise 4.3.19

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 $|S_n : A_n| = 2$, 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. ■

Exercise 4.3.20

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.
$\boxed{\Rightarrow}$ 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.
$\boxed{\Leftarrow}$ 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. ■

Exercise 4.3.21

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.
$\boxed{\Rightarrow}$ 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, 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.
$\boxed{\Leftarrow}$ 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. ■

Exercise 4.3.22

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. ■

Exercise 4.3.23

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 $(|M| - 1)|G : M|$. ■

Exercise 4.3.24

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, $|G:M| \geq 2$, 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

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

■

Exercise 4.3.25

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,

$$G = \bigcup_{g \in G} gHg^{-1}.$$

■

Exercise 4.3.26

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 $a \in A$. ■

Exercise 4.3.27

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. It is clear that $g_i \in C_G(g_j)$ for any two representatives g_i and g_j. Let S be the set of class representatives, so that we may write $S \subseteq C_G(g_i)$. Then $|C_G(g_i)| \geq |S| = r$ for all i. From the class equation, we get that

$$|G| = \sum_{i=1}^{r} |G : C_G(g_i)| \leq \sum_{i=1}^{r} \frac{|G|}{r} = |G|$$

Each term in the sum must be equal to $|G|/r$ so that $|C_G(g_i)| = r$ for all i. Therefore, $C_G(g_i) = S$ for all i. Recall that one of the g_i must be 1, so that $C_G(1) = G$. Therefore, $G = S$, so that G is abelian. ■

Exercise 4.3.28

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 $\pi\colon G \to S_q$. 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 $(1\ 2\ cdots\ q)$. ■

Exercise 4.3.29

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 $\alpha \geq 0$. ■

Exercise 4.3.30

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, $G/C_G(x)$ 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. ■

Exercise 4.3.31

Using the usual generators and relations for the dihedral group D_{2n}, show that for $n = 2k$ an even integer, the conjugacy classes in D_{2n} are the following:

$$\{1\}, \{r^k\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \ldots, k\}, \{sr^{2b-1} \mid b = 1, \ldots, k\}.$$

Give the class equation for D_{2n}.

Solution. We immediately have two conjugacy classes, $\{1\}$ and $\{r^k\}$, 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

$$|D_{2n}| = 1 + 1 + 2(k-1) + k + k. \qquad \blacksquare$$

Exercise 4.3.32

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

$$|D_{2n}| = 1 + 2k + n. \qquad \blacksquare$$

Exercise 4.3.33

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. $\blacksquare$

Exercise 4.3.34

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

$$|N_{S_p}(P)| = \frac{|S_p|}{k} = \frac{p!}{(p-2)!} = p(p-1). \qquad \blacksquare$$

Exercise 4.3.35

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 $1 \leq k \leq \lfloor n/p \rfloor$, hence the number of conjugacy classes of elements of order p in S_n is given by $\lfloor n/p \rfloor$. $\blacksquare$

Exercise 4.3.36

Let $\pi \colon G \to S_G$ 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 $\lambda \colon G \to S_G$ 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 $h = g^{-1}$, 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, $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$. $\blacksquare$

4.4 Automorphisms

Exercise 4.4.1

Let G be a group. If $\sigma \in \text{Aut}(G)$ and ϕ_g is conjugation by g, prove that $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Deduce that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. (The group $\text{Aut}(G)/\text{Inn}(G)$ 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 $\varphi_g \in \text{Inn}(G)$ and any $\sigma \in \text{Aut}(G)$, we have $\sigma\varphi_g\sigma^{-1} \in \text{Inn}(G)$, so that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. ■

Exercise 4.4.2

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 $|gh| = \text{lcm}(|g|, |h|) = \text{lcm}(p, q) = pq$. Therefore, $G = \langle gh \rangle$ is cyclic. ■

Exercise 4.4.3

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 $|\text{Aut}(D_8)| \leq 8$.

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 $|\text{Aut}(D_8)| \leq 8$. ■

Exercise 4.4.4

Use arguments similar to those in the preceding exercise to show that $|\text{Aut}(Q_8)| \leq 24$.

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 $|\text{Aut}(Q_8)| \leq 24$. ■

Exercise 4.4.5

Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\text{Aut}(D_8) \cong D_8$.

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 $\text{Aut}(H)$ when acted on by conjugation. By Exercise 4.4.3, we know that $|\text{Aut}(D_8)| \leq 8$, so that $\text{Aut}(H) \cong D_8$. Therefore, $\text{Aut}(D_8) \cong D_8$. ■

Exercise 4.4.6

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 $\varphi \in \text{Aut}(G)$. In particular, this holds for every $\varphi_g \in \text{Inn}(G)$ so that $\varphi_g(H) = gHg^{-1} = H$ for every $g \in G$. Therefore, $H \trianglelefteq G$.

Consider the abelian group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 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 $\sigma\colon G \to G$ 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. ■

Exercise 4.4.7

If H is the unique subgroup of a given order in a group G, prove that H is characteristic in G.

Solution. For any $\sigma \in \text{Aut}(G)$, 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. ■

Exercise 4.4.8

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, $H \trianglelefteq V_4$. 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. ■

Exercise 4.4.9

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 $\langle r\rangle \trianglelefteq D_{2n}$, by Exercise 4.4.8, every subgroup of $\langle r\rangle$ is normal in D_{2n}. ■

Exercise 4.4.10

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 $\overline{g} \cdot a = gag^{-1}$, where g is any representative of the coset $\overline{g}$ (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 $\overline{g}$ and $\overline{h}$ 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

$$\overline{g} \cdot a = gag^{-1} = gaa_0a_0^{-1}g^{-1} = ga_0a(ga_0)^{-1} = hah^{-1} = \overline{h} \cdot a$$

since A is abelian. Therefore, the action is well defined.

Consider $G = S_3$ and $A = S_3$ itself. Then $\overline{1} = \overline{(1\ 2)}$ in $\overline{G}$. However, for $a = (1\ 3)$, we have $\overline{1} \cdot a = a = (1\ 3)$ 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. ■

Exercise 4.4.11

If p is a prime and P is a subgroup of S_p of order p, prove that $N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P)$. (Use Exercise 4.3.34).

Solution. By Exercise 4.3.34, we know that $|N_{S_p}(P)| = p(p-1)$. Moreover, since P is cyclic of order p, we have $\mathrm{Aut}(P) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ by Proposition 4.16, so that $|\mathrm{Aut}(P)| = p-1$. Let N_{S_p} act on P by conjugation. Then we have the map

$$\varphi \colon N_{S_p}(P) \to \mathrm{Aut}(P), \quad \varphi(g)(x) = gxg^{-1}$$

for all $g \in N_{S_p}(P)$ and $x \in P$. Recall that $\ker \varphi = C_{S_p}(P)$ by Proposition 4.13. Therefore, by the First Isomorphism Theorem, we have

$$N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{im}\, \varphi \leq \mathrm{Aut}(P).$$

Since P is cyclic, the only permutations that centralize P are the elements of P itself, so that $C_{S_p}(P) = P$. Therefore,

$$|N_{S_p}(P)/C_{S_p}(P)| = \frac{|N_{S_p}(P)|}{|C_{S_p}(P)|} = \frac{p(p-1)}{p} = p-1 = |\mathrm{Aut}(P)|.$$

Hence, $\mathrm{im}\, \varphi = \mathrm{Aut}(P)$ so that $N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P)$. ■

Exercise 4.4.12

Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.

Solution. Observe that $3825 = 15^2 \cdot 17$. Since $|H| = 17$ a prime, H is cyclic. Moreover, we have $\mathrm{Aut}(H) \cong (\mathbb{Z}/17\mathbb{Z})^\times$ by Proposition 4.16, so that $|\mathrm{Aut}(H)| = 16$. Now consider the action of G on H by conjugation. This gives the map

$$\varphi \colon G \to \mathrm{Aut}(H), \quad \varphi(g)(x) = gxg^{-1}$$

for all $g \in G$ and $x \in H$. Recall that $\ker \varphi = C_G(H)$ by Proposition 4.13. Therefore, by the First Isomorphism Theorem, we have

$$G/C_G(H) \cong \mathrm{im}\, \varphi \leq \mathrm{Aut}(H).$$

Hence, $|G/C_G(H)|$ divides $|\mathrm{Aut}(H)| = 16$. However, $|G| = 3825$ is relatively prime to 16, so that $|G/C_G(H)| = 1$. Therefore, $G = C_G(H)$, so that $H \leq Z(G)$. ■

Exercise 4.4.13

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.

Solution. Note that $203 = 7 \cdot 29$. The proof of showing that $H \leq Z(G)$ is similar to the previous exercise. To see that G is abelian, consider the quotient group G/H. Since $|G/H| = 29$ is prime, G/H is cyclic. By Exercise 3.1.36, we have that G is abelian. ■

Exercise 4.4.14

Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.

Solution. This exercise is similar to the previous two. Following the proofs, we will find that $|G/C_G(H)|$ divides $|\mathrm{Aut}(H)| = 6$ or 48. However, $1575 = 3^2 \cdot 5^2 \cdot 7$ results in $(|G|, |\mathrm{Aut}(H)|) = 1$ or 3. If the latter is true, then $|C_G(H)| = 525$. However, this is impossible since $H \leq C_G(H)$ and $|H| = 9$ does not divide 525. Therefore, we must have $|G/C_G(H)| = 1$, so that $G = C_G(H)$ and hence $H \leq Z(G)$. ■

Exercise 4.4.15

Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$, and $(\mathbb{Z}/18\mathbb{Z})^\times$.

Solution. Since $|(\mathbb{Z}/5\mathbb{Z})^\times| = 4$, $(\mathbb{Z}/5\mathbb{Z})^\times$ is isomorphic to either Z_4 or V_4. However, $\bar{2} \in (\mathbb{Z}/5\mathbb{Z})^\times$ has order 4, so that $(\mathbb{Z}/5\mathbb{Z})^\times \cong Z_4$ is cyclic.

Observe that $|(\mathbb{Z}/9\mathbb{Z})^\times| = |(\mathbb{Z}/18\mathbb{Z})^\times| = 6$. By Exercise 4.2.10, groups of order 6 are isomorphic to either Z_6 or S_3. However, both groups are abelian, so that $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$ must be isomorphic to Z_6. Therefore, both groups are cyclic. ■

Exercise 4.4.16

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 $n \mid 24$.)

Solution. We first prove the lemma: let $a, b, m, n \in \mathbb{Z}$ such that $(m, n) = 1$. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{mn}$. Indeed, we have that

$$a - b = xm \quad \text{and} \quad a - b = yn$$

for some $x, y \in \mathbb{Z}$. Therefore, $xm = yn$, so that $m \mid yn$. Since $(m, n) = 1$, $m \mid y$. Letting $y = km$ for some $k \in \mathbb{Z}$, we have

$$a - b = yn = kmn,$$

so that $a \equiv b \pmod{mn}$.

Let $x \in (\mathbb{Z}/24\mathbb{Z})^\times$. Note that x is always odd. Then $\gcd(x, 24) = 1$, hence $(x, 3) = (x, 8) = 1$. Since $(x, 3) = 1$, $x \equiv 1$ or $2 \pmod{3}$. Then $x^2 \equiv 1 \pmod{3}$. Since $(x, 8) = 1$, let $x = 2k + 1$ for some $k \in \mathbb{Z}$. Then

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

Since one of k or $k + 1$ is even, $4k(k + 1)$ is divisible by 8, so that $x^2 \equiv 1 \pmod{8}$. By the lemma above, we have $x^2 \equiv 1 \pmod{2}4$. Therefore, every element of $(\mathbb{Z}/24\mathbb{Z})^\times$ has order dividing 2, so that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group. ■

Exercise 4.4.17

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).

Solution.

- $n = 2$: $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$. Then $\psi_1 \colon x^k \mapsto x^{1 \cdot k} = x^k$ for $k = 0, 1$. Therefore, $\mathrm{Aut}(G) = \{\mathrm{id}\}$.
- $n = 3$: $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$. Then
$$\psi_1 \colon x^k \mapsto x^{1 \cdot k} = x^k, \quad \psi_2 \colon x^k \mapsto x^{2 \cdot k}$$
for $k = 0, 1, 2$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_2\}$.
- $n = 4$: $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$. Then
$$\psi_1 \colon x^k \mapsto x^{1 \cdot k} = x^k, \quad \psi_3 \colon x^k \mapsto x^{3 \cdot k}$$
for $k = 0, 1, 2, 3$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_3\}$.
- $n = 5$: $(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Then
$$\psi_1 \colon x^k \mapsto x^{1 \cdot k}, \quad \psi_2 \colon x^k \mapsto x^{2 \cdot k}, \quad \psi_3 \colon x^k \mapsto x^{3 \cdot k}, \quad \psi_4 \colon x^k \mapsto x^{4 \cdot k}$$
for $k = 0, 1, 2, 3, 4$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_2, \psi_3, \psi_4\}$.
- $n = 6$: $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$. Then
$$\psi_1 \colon x^k \mapsto x^{1 \cdot k} = x^k, \quad \psi_5 \colon x^k \mapsto x^{5 \cdot k}$$
for $k = 0, 1, 2, 3, 4, 5$. Therefore, $\mathrm{Aut}(G) = \{\psi_1, \psi_5\}$. ■

Exercise 4.4.18

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 4.3.33.)

(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 $n \neq 6$.

Solution.

(a) Let $\mathcal{K}$ be a conjugacy class of G and let $\sigma \in \mathrm{Aut}(G)$. For any $x \in \mathcal{K}$, we have $\sigma(x) \in G$. Consider the conjugacy class $\mathcal{K}'$ of $\sigma(x)$ in G. For any $y \in \mathcal{K}$, there exists some $g \in G$ such that $y = gxg^{-1}$. Then

$$\sigma(y) = \sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g)^{-1} \in \mathcal{K}'.$$

Therefore, $\sigma(\mathcal{K}) \subseteq \mathcal{K}'$.

Now let $z \in \mathcal{K}'$. Then there exists some $h \in G$ such that $z = h\sigma(x)h^{-1}$. Since σ is an automorphism, there exists some $g \in G$ such that $\sigma(g) = h$. Then

$$z = h\sigma(x)h^{-1} = \sigma(g)\sigma(x)\sigma(g)^{-1} = \sigma(gxg^{-1}) \in \sigma(\mathcal{K}).$$

Therefore, $\mathcal{K}' \subseteq \sigma(\mathcal{K})$. Hence, $\sigma(\mathcal{K}) = \mathcal{K}'$, so that $\mathrm{Aut}(G)$ permutes the conjugacy classes of G.

(b) By Exercise 4.3.33, the formulas for each conjugacy class is given by

$$|\mathcal{K}| = \binom{n}{2} = \frac{n(n-1)}{2}, \quad \text{and} \quad |\mathcal{K}'| = \frac{n!}{2^k k!(n-2k)!}$$

for some $k \geq 2$. Assume, by way of contradiction, that $|\mathcal{K}| = |\mathcal{K}'|$. Equating the two expressions and cancellation, we obtain

$$(n-2)(n-3)\cdots(n-2k+1) = 2^k k!.$$

Observe that the left-hand side contains $2k-2$ consecutive integers, which has at most $k-1$ powers of 2. The right-hand side has at least k powers of 2, so that the two sides cannot be equal. Therefore, $|\mathcal{K}| \neq |\mathcal{K}'|$. Hence, by (a), any automorphism of S_n sends transpositions to transpositions.

(c) Let $\sigma \in \mathrm{Aut}(S_n)$. By (b), we know that σ sends transpositions to transpositions. In particular,

$$\sigma((1\,2)) = (a\,b_2), \quad \sigma((1\,3)) = (c\,d_3)$$

for distinct integers. Note that if $\{a, b_2\} \cap \{c, d_3\} = \varnothing$, then

$$\sigma((1\,2)(1\,3)) = \sigma((1\,2))\sigma((1\,3)) = (a\,b_2)(c\,d_3)$$

is a product of two disjoint transpositions. However, $(1\,2)(1\,3) = (1\,3\,2)$ is a 3-cycle, so this is impossible. Therefore, $\{a, b_2\} \cap \{c, d_3\} \neq \varnothing$. Without loss of generality, assume that $a = c$ since we may interchange the order within the transposition. Repeating this argument for all transpositions $(1\,k)$ for $k = 4, \ldots, n$, we obtain the desired result. Moreover, these integers must be distinct since σ is injective.

(d) Note that $(1\,2), (1\,3), \ldots, (1\,n)$ generate S_n since any transposition $(i\,j)$ can be written as

$$(i\,j) = (1\,i)(1\,j)(1\,i).$$

Therefore, any automorphism of S_n is uniquely determined by its action on these elements. By (c), there are at most $n!$ ways to assign images to these transpositions since there are n choices for the image of $(1\,2)$, $n-1$ choices for the image of $(1\,3)$, and so on. Therefore, $|\mathrm{Aut}(S_n)| \leq n!$. However, $|\mathrm{Inn}(S_n)| = |S_n/Z(S_n)| = n!$ since $Z(S_n)$ is trivial for $n \geq 3$. Since $\mathrm{Inn}(S_n) \leq \mathrm{Aut}(S_n)$, we must have $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$. ∎

Exercise 4.4.19

This exercise shows that $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$ (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 $\text{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.

(b) Prove that $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$. (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.)

Solution.

(a) This is similar to (b) in the previous exercise. By Exercise 4.3.33, the formulas for each conjugacy class is given by

$$|\mathcal{K}| = \binom{6}{2} = 15, \quad \text{and} \quad |\mathcal{K}'| = \frac{6!}{2^k k!(6-2k)!}$$

for some $k \geq 2$. Since we are working in S_6, we only need to check $k = 2$ and $k = 3$. For $k = 2$, we have

$$|\mathcal{K}'| = \frac{6!}{2^2 \cdot 2! \cdot 2!} = 45 \neq 15 = |\mathcal{K}|.$$

For $k = 3$, we have

$$|\mathcal{K}'| = \frac{6!}{2^3 \cdot 3! \cdot 0!} = 15 = |\mathcal{K}|.$$

Therefore, $|\mathcal{K}| \neq |\mathcal{K}'|$ unless $\mathcal{K}'$ is the conjugacy class of products of three disjoint transpositions. Hence, by (a) in the previous exercise, $\text{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.

(b) Following the same steps as in (c) and (d) of the previous exercise, we can show that any automorphism that sends transpositions to transpositions is inner. Therefore, by (a), we have $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$. ■

Exercise 4.4.20

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 2.5.11). (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 $J(P) \trianglelefteq G$.

Solution.

(a) Let $\sigma \in \text{Aut}(P)$. Let A be an abelian subgroup of P such that $d(A) = m(P)$. Then $\sigma(A)$ is also an abelian subgroup of P. Moreover, it is clear that $d(\sigma(A)) = d(A) = m(P)$. Therefore, $\sigma(J(P)) = J(P)$, so that $J(P)$ is characteristic in P.

(b)
- Q_8: From the lattice, we see that every abelian subgroup is cyclic so that $m(Q_8) = 1$. The abelian subgroups A with $d(A) = 1$ are $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$.
- D_8: From the lattice, we see that the abelian subgroups with maximum number of generators are those isomorphic to V_4, hence $m(D_8) = 2$. The abelian subgroups A with $d(A) = 2$ are $\langle r^2, s \rangle$ and $\langle r^2, rs \rangle$.
- D_{16}: From the lattice, we see that the abelian subgroups with maximum number of generators are those isomorphic to V_4, hence $m(D_{16}) = 2$. The abelian subgroups A with $d(A) = 2$ are $\langle r^4, s \rangle$, $\langle r^4, r^5 s \rangle$, $\langle r^4, r^2 s \rangle$, and $\langle r^4, r^3 s \rangle$.
- QD_{16}: From the lattice, we see that the abelian subgroups with maximum number of generators are those isomorphic to V_4, hence $m(QD_{16}) = 2$. The abelian subgroups A with $d(A) = 2$ are $\langle \tau\sigma^2, \sigma^4 \rangle$ and $\langle \tau, \sigma^4 \rangle$.

(c)
- Any pair of the abelian subgroups in (b) generate Q_8, so that $J(Q_8) = Q_8$.
- Note that $r, s \in \langle r^2, s\rangle \cup \langle r^2, rs\rangle$, so that $J(D_8) = D_8$.
- Note that $r^3 = r^3 s \cdot s$ and $r = r^4 \cdot r^{-3}$ so that the join of all abelian subgroups in (b) generates D_{16}. Therefore, $J(D_{16}) = D_{16}$.
- Observe that
$$\langle \tau\sigma^2, \sigma^4\rangle = \{1, \sigma^4, \tau\sigma^2, \tau\sigma^6\} \quad \text{and} \quad \langle \tau, \sigma^4\rangle = \{1, \sigma^4, \tau, \tau\sigma^4\}.$$
The join of these two subgroups is the subgroup $\langle \sigma^2, \tau\rangle$, which has order 8. Since $\tau^2 = (\sigma^2)^4 = 1$, and $\sigma^2\tau = \tau\sigma^6$, the mapping $\varphi\colon D_8 \to \langle \sigma^2, \tau\rangle$ defined by $\varphi(r) = \sigma^2$ and $\varphi(s) = \tau$ is an isomorphism. Therefore, $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16}.

(d) Note that any abelian subgroup of Q is also an abelian subgroup of P. Therefore, $m(Q) \leq m(P)$. Since $J(P) \leq Q$, every abelian subgroup A of P with $d(A) = m(P)$ is also an abelian subgroup of Q. Therefore, $m(P) \leq m(Q)$. Hence, $m(P) = m(Q)$. Moreover, any abelian subgroup B of Q with $d(B) = m(Q) = m(P)$ is also an abelian subgroup of P. Therefore, $J(P) = J(Q)$.

Using that $J(P) = J(Q)$, then part (a) implies that $J(P)$ char Q. Since $Q \trianglelefteq G$, $J(P) \trianglelefteq G$. ■

4.5 Sylow's Theorem

Let G be a finite group and let p be a prime.

Exercise 4.5.1

Prove that if $P \in \mathrm{Syl}_p(G)$ and H is a subgroup of G containing P then $P \in \mathrm{Syl}_p(H)$. Give an example to show that in general, a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G.

Solution. Let $|G| = p^n m$ where $p \nmid m$. Since $P \leq H \leq G$, $|H| = p^k t$ for some $k \leq n$ and $p \nmid t$. Since $P \in \mathrm{Syl}_p(G)$, $|P| = p^n$. However, since $P \leq H$, $|P| = p^n \leq |H| = p^k t$. Therefore, we must have $k = n$, so that $|H| = p^n t$. Hence, $P \in \mathrm{Syl}_p(H)$.

Consider $G = S_4$ and its subgroup $H = A_4$. Then $|G| = 24$ and $|H| = 12$. A Sylow 2-subgroup of H is isomorphic to V_4, which has order 4. However, a Sylow 2-subgroup of G has order 8, so that the Sylow 2-subgroup of H is not a Sylow 2-subgroup of G. ■

Exercise 4.5.2

Prove that if H is a subgroup of G and $Q \in \mathrm{Syl}_p(H)$ then $gQg^{-1} \in \mathrm{Syl}_p(gHg^{-1})$ for all $g \in G$.

Solution. Let $|H| = p^n m$ where $p \nmid m$. Then $|Q| = p^n$. Note that $|gHg^{-1}| = |H| = p^n m$ since conjugation is an isomorphism. Moreover, $|gQg^{-1}| = |Q| = p^n$. Therefore, $gQg^{-1} \in \mathrm{Syl}_p(gHg^{-1})$. ■

Exercise 4.5.3

Use Sylow's Theorem to prove Cauchy's Theorem. (Note that we only used Cauchy's Theorem for abelian groups–Proposition 3.21–in the proof of Sylow's Theorem, so this line of reasoning is not circular.)

Solution. Let $|G| = p^n m$ where $p \nmid m$. By Sylow's Theorem, there exists some $P \in \mathrm{Syl}_p(G)$ such that $|P| = p^n$. Since $n \geq 1$, P is nontrivial. By Theorem 4.8, we know that the center $Z(P)$ is nontrivial. Since $Z(P)$ is abelian, by Proposition 3.21, there exists some element $x \in Z(P)$ such that $|x| = p$. Therefore, $x \in G$ has order p. ■

Exercise 4.5.4

Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.

Solution. For D_{12}, we have $|D_{12}| = 12 = 2^2 \cdot 3$. Therefore, the Sylow 2-subgroups have order 4 and the Sylow 3-subgroups have order 3. The Sylow 2-subgroups are

$$\langle r^3, s\rangle, \quad \langle r^3, rs\rangle, \quad \langle r^3, r^2 s\rangle.$$

The Sylow 3-subgroups is

$$\langle r^2\rangle,$$

where this is the only Sylow 3-subgroup, since if $n_3 = 4$, there would be 8 elements of order 3, which is impossible.

We first show that the Sylow p-subgroups of a direct product are the direct products of the Sylow p-subgroups of each factor. Let G and H be finite groups, and let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_p(H)$. Then $|P| = p^n$ and $|Q| = p^m$ for some $n, m \geq 0$. Therefore, $|P \times Q| = p^{n+m}$. Moreover, since $|G \times H| = |G||H|$, the highest power of p dividing $|G \times H|$ is also p^{n+m}. Hence, $P \times Q \in \mathrm{Syl}_p(G \times H)$. For the converse, let $R \in \mathrm{Syl}_p(G \times H)$. Then $|R| = p^k$ for some $k \geq 0$. Consider the projections $\pi_G \colon G \times H \to G$ and $\pi_H \colon G \times H \to H$. Then $\pi_G(R)$ is a p-subgroup of G and $\pi_H(R)$ is a p-subgroup of H. Therefore, there exist Sylow p-subgroups P of G and Q of H such that $\pi_G(R) \leq P$ and $\pi_H(R) \leq Q$. Hence, $R \leq P \times Q$. Since $|R| = p^k$ is the highest power of p dividing $|G \times H|$, we must have $|P \times Q| = p^k$. Therefore, $R = P \times Q$. This shows that the Sylow p-subgroups of a direct product are the direct products of the Sylow p-subgroups of each factor.

We now proceed with $S_3 \times S_3$. Note that $|S_3 \times S_3| = 36 = 2^2 \cdot 3^2$. Therefore, the Sylow 2-subgroups have order 4 and the Sylow 3-subgroups have order 9. Moreover, note that $\mathrm{Syl}_2(S_3)$ is the set of subgroups generated by transpositions, and $\mathrm{Syl}_3(S_3)$ is the unique subgroup generated by a 3-cycle. Therefore, we have

$$\mathrm{Syl}_2(S_3 \times S_3) = \{\langle \alpha\rangle \times \langle \beta\rangle \mid \alpha, \beta \in \{(1\,2), (1\,3), (2\,3)\}\}$$

and $\mathrm{Syl}_3(S_3 \times S_3)$ consists of $A_3 \times A_3$. ■

Exercise 4.5.5

Show that a Sylow p-subgroup of D_{2n} is cyclic and normal for every odd prime p.

Solution. Let $|D_{2n}| = 2n = 2p^k m$ where $p \nmid m$ and $k \geq 1$. Then the Sylow p-subgroups have order p^k. Note that r^m has order p^k, so that $\langle r^m \rangle$ is a Sylow p-subgroup and is cyclic. Moreover, conjugacy of Sylow p-subgroups imply that any Sylow p-subgroup is also cyclic.

To see that the Sylow p-subgroup is normal, note that $n_p \equiv 1 \pmod{p}$ and $n_p \mid 2m$. Since p is odd and $p \nmid m$, $(2m, p) = 1$. Therefore, $n_p = 1$, so that the Sylow p-subgroup is unique and hence normal. ■

Exercise 4.5.6

Exhibit all Sylow 3-subgroups of A_4 and all Sylow 3-subgroups of S_4.

Solution. The Sylow 3-subgroups of both A_4 and S_4 have order 3. The Sylow 3-subgroups of S_4 are

$$\langle (1\,2\,3) \rangle, \quad \langle (1\,2\,4) \rangle, \quad \langle (1\,3\,4) \rangle, \quad \langle (2\,3\,4) \rangle.$$

Note that these are also the Sylow 3-subgroups of A_4 since they are all contained in A_4. ■

Exercise 4.5.7

Exhibit all Sylow 2-subgroups of S_4 and find elements of S_4 which conjugate one of these into each of the others.

Solution. The Sylow 2-subgroups of S_4 have order 8. Note that we have calculated 2 of these subgroups in Exercise 4.2.5, namely parts (a) and (b). Since $n_2 \equiv 1 \pmod{2}$ and $n_2 \mid 3$, $n_2 = 1$ or 3. However, there are more than one Sylow 2-subgroup, so that $n_2 = 3$. One of the Sylow 2-subgroups is

$$\langle (1\,2\,3\,4), (2\,4) \rangle = \{1, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (2\,4), (1\,2)(3\,4), (1\,3), (1\,4)(2\,3)\}.$$

The other two can be reached by conjugation. For example, conjugating by $(2\,3)$ gives

$$\langle (1\,3\,2\,4), (3\,4) \rangle = \{1, (1\,3\,2\,4), (1\,2)(3\,4), (1\,4\,2\,3), (3\,4), (1\,3)(2\,4), (1\,2), (1\,4)(2\,3)\},$$

and conjugating by $(3\,4)$ gives

$$\langle (1\,2\,4\,3), (2\,3) \rangle = \{1, (1\,2\,4\,3), (1\,4)(2\,3), (1\,3\,4\,2), (2\,3), (1\,2)(3\,4), (1\,4), (1\,3)(2\,4)\}.$$

Note that these are all distinct but have nontrivial intersections. ■

Exercise 4.5.8

Exhibit two distinct Sylow 2-subgroups of S_5 and an element of S_5 that conjugates one into the other.

Solution. Use any of the Sylow 2-subgroups of S_4 from Exercise 4.5.7 and consider them as subgroups of S_5. ■

Exercise 4.5.9

Exhibit all Sylow 3-subgroups of $\mathrm{SL}_2(\mathbb{F}_3)$ (cf. Exercise 2.1.9).

Solution. Recall that $|\mathrm{SL}_2(\mathbb{F}_3)| = 24 = 3 \cdot 2^3$. Therefore, the Sylow 3-subgroups have order 3. Moreover, recall that $\mathrm{SL}_2(\mathbb{F}_3)$ is generated by the two matrices as listed in Exercise 2.4.9. Since $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 8$, $n_3 = 4$ since we were able to exhibit more than one Sylow 3-subgroup. Conjugating A by B, we obtain another matrix C of order 3. Conjugating B by C gives another matrix D of order 3. Therefore, the other two Sylow 3-subgroups are

$$\langle C \rangle = \left\{ I_2, \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}, \begin{matrix} 2 & 2 \\ 1 & 0 \end{matrix} \right\}, \quad \langle D \rangle = \left\{ I_2, \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \right\}.$$

■

Exercise 4.5.10

Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is the unique Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ (cf. Exercise 2.4.10).

Solution. Let P be the subgroup generated by the two matrices. Note that $P \cong Q_8$ by Exercise 2.4.10 so that $|P| = 8$, and $P \in \mathrm{Syl}_2(\mathrm{SL}_2(\mathbb{F}_3))$. To show uniqueness, let $Q \in \mathrm{Syl}_2(\mathrm{SL}_2(\mathbb{F}_3))$. Since Q is conjugate to P, $Q \cong Q_8$ as well. We now consider $|P \cap Q|$, and let $Z = \langle I \rangle$ be the subgroup of P associated with $Z(Q_8)$. For any $g \in \mathrm{SL}_2(\mathbb{F}_3)$, then $gPg^{-1} \cong Q_8$. However, $gZg^{-1} \leq gPg^{-1}$ is a subgroup of order 2, and $Z \leq gPg^{-1}$ as well, since $Z \leq Z(\mathrm{SL}_2(\mathbb{F}_3))$. It follows that $gZg^{-1} = Z$, hence $Z \trianglelefteq \mathrm{SL}_2(\mathbb{F}_3)$ and every Sylow 2-subgroup must contain Z.

Clearly, the intersection cannot be trivial since both P and Q are isomorphic to Q_8, hence they must both contain Z. If $|P \cap Q| = 2$, then $P \cap Q = Z$. Note that in P, there are 6 elements of order 4. However, taking the case of $n_3 = 3$, then there would be $1 + 1 + 6 \cdot 3 = 20$ elements accounted for, where the first 1 is from the identity, the second 1 is from the unique element of order 2, and $6 \cdot 3$ is from the elements of order 4 in each Sylow 2-subgroup. However, from Exercise 4.5.9, there are at least 8 elements of order 3, giving a total of at least 28 elements, which is impossible. Therefore, $|P \cap Q| \neq 2$.

If $|P \cap Q| = 4$, first let $P = \{I, -I, A, A^3, B, B^3, AB, A^3B^3\}$ where A and B generate P. Since $P \cap Q \leq P \cong Q_8$ and has order 4, it must be one of the cyclic subgroups. Without loss of generality, let $P \cap Q = \langle A \rangle$. Since we are assuming distinct Sylow 2-subgroups, we may let $Q = \{I, -I, A, A^3, C, C^3, AC, A^3C^3\}$ for some $C \notin P$. Let R be the third Sylow 2-subgroup. Then $|P \cap R|$ must also be 4 by the preceding reasons of ruling out 1 and 2, while 8 would imply $P = R$. Therefore, $P \cap R$ is also a cyclic subgroup of order 4. Again, without loss of generality, let $P \cap R = \langle B \rangle$. Then we may let $R = \{I, -I, B, B^3, D, D^3, BD, B^3D^3\}$ for some $D \notin P$. Now consider $Q \cap R$, which must also have order 4. However, by construction, Q and R only share the elements $I, -I$, so that $|Q \cap R| = 2$, a contradiction. Therefore, $|P \cap Q| \neq 4$.

Hence, we must have $|P \cap Q| = 8$, so that $P = Q$. Therefore, P is the unique Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$. ■

Exercise 4.5.11

Show that the center of $\mathrm{SL}_2(\mathbb{F}_3)$ is the group of order 2 consisting of $\pm I$, where I is the identity matrix. Prove that $\mathrm{SL}_2(\mathbb{F}_3)/Z(\mathrm{SL}_2(\mathbb{F}_3)) \cong A_4$. [Use facts about groups of order 12.]

Solution. Consider the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $\mathrm{SL}_2(\mathbb{F}_3)$, where $Z \in Z(\mathrm{SL}_2(\mathbb{F}_3))$. Then

$$AZ = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = ZA$$

from which we can determine $c = 0$ and $a = d$. Then

$$BZ = \begin{pmatrix} a & b \\ a & a+b \end{pmatrix} = \begin{pmatrix} a+b & b \\ a & a \end{pmatrix} = ZB$$

from which we can determine that $a \in \mathbb{F}_3$ and $b = 0$. Then $Z = aI_2$. To prove the second part, we show that $\mathrm{SL}_2(\mathbb{F}_3)/Z(\mathrm{SL}_2(\mathbb{F}_3))$ does not have a normal Sylow 3-subgroup. To that end, let $P \in \mathrm{Syl}_3(\mathrm{SL}_2(\mathbb{F}_3))$, and consider $P \cap Z$. Under the projection homomorphism π restricted to P, it is clear that $\ker(\pi|_P) = P \cap Z$, since $\ker(\pi|_P)$ are elements $p \in P$ such that $\pi(p) = Z$. By the First Isomorphism Theorem, then $P/\ker(\pi|_P) \cong \pi(P)$, or $P/P \cap Z \cong \pi(P)$. Since $(|P|, |Z|) = 1$ and $P \cap Z$ is a subgroup of both, the intersection is trivial so that $P \cong \pi(P)$. Then $|\pi(P)| = 3$ so that $\pi(P) \in \mathrm{Syl}_3(\mathrm{SL}_2(\mathbb{F}_3)/Z(\mathrm{SL}_2(\mathbb{F}_3)))$. This shows that any Sylow 3-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ is also a Sylow 3-subgroup of the quotient.

Since Exercise 4.5.9 showed that $\mathrm{SL}_2(\mathbb{F}_3)$ has 4 Sylow 3-subgroups, then there are also 4 Sylow 3-subgroups in the quotient. Hence, $n_3(\mathrm{SL}_2(\mathbb{F}_3)/Z(\mathrm{SL}_2(\mathbb{F}_3))) = 4 \neq 1$. By the text's classification of groups of order 12, it must be that the quotient group is isomorphic to A_4. ■

Exercise 4.5.12

Let $2n = 2^a k$ where k is odd. Prove that the number of Sylow 2-subgroups of D_{2n} is k. [Prove that if $P \in \mathrm{Syl}_2(D_{2n})$ then $N_{D_{2n}}(P) = P$.]

Solution. We construct a Sylow 2-subgroup. Note that $n = 2^{a-1}k = |r|$ so that $|r^k| = 2^{a-1}$. Since s has order 2, $P = \langle r^k, s\rangle$ has order 2^a and is a Sylow 2-subgroup of D_{2n}. To show that $N_{D_{2n}}(P) = P$, let $g \in N_{D_{2n}}(P)$. We then have two cases:

- If $g = r^i$ for some i, then it normalizes s. In particular, $r^i s r^{-i} = r^{2i}s \in P$. Then $r^{2i}s = r^{km}s$ for some m. It follows that $k \mid 2i$. However, k is odd so that $k \mid i$, hence $r^i \in \langle r^k\rangle \leq P$.
- If $g = sr^i$, it also normalizes s. Then $sr^i s(sr^i)^{-1} = sr^i s r^{-i} = r^{-2i}s \in P$. Then $r^{-2i}s = r^{km}s$ for some m. It follows that $k \mid -2i$. However, k is odd so that $k \mid i$, hence $sr^i \in \langle r^k, s\rangle = P$.

In both cases, we have $g \in P$, so that $N_{D_{2n}}(P) = P$.

Now we show that the number of Sylow 2-subgroups of D_{2n} is k. Note that the number of Sylow 2-subgroups is given by the index of the normalizer of any Sylow 2-subgroup. Since we have shown that the normalizer is just the subgroup itself, the number of Sylow 2-subgroups is given by the index of any Sylow 2-subgroup, which is $|D_{2n}|/|P| = 2^a k/2^a = k$. ∎

Exercise 4.5.13

Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution. Note that $56 = 2^3 \cdot 7$. Recall that $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 8$, so that $n_7 = 1$ or 8. Moreover, $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 7$, so that $n_2 = 1$ or 7. Assume, by way of contradiction, that both $n_7 = 8$ and $n_2 = 7$. Then there are at least $8 \cdot 6 = 48$ elements of order 7. For the Sylow 2-subgroups, their pairwise intersection can have at most 4 elements, so that there are at least $7 \cdot 4 = 28$ elements of order 2-power order. This gives a total of at least 77 elements, which is impossible. Therefore, either $n_7 = 1$ or $n_2 = 1$, so that there is a normal Sylow p-subgroup for some prime p dividing the order of the group. ∎

Exercise 4.5.14

Prove that a group of order 312 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution. Note that $312 = 2^3 \cdot 3 \cdot 13$. Recall that $n_{13} \equiv 1 \pmod 1 3$ and $n_{13} \mid 24$, so that $n_{13} = 1$ or 24. Moreover, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 104$, so that $n_3 = 1, 13, 52$, or 104. Lastly, $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 39$, so that $n_2 = 1, 3, 13$, or 39. Assume, by way of contradiction, that $n_{13} = 24$, $n_3 > 1$, and $n_2 > 1$. In particular, then $n_3 \geq 13$ and $n_2 \geq 3$. The Sylow-3 and Sylow-13 subgroups intersect trivially, while the Sylow 2-subgroups can have at most 4 elements in common. Then there are at least $24 \cdot 12 = 288$ elements of order 13, at least $13 \cdot 2 = 26$ elements of order 3, and at least $3 \cdot 4 = 12$ elements of order 2-power order, giving a total of at least 326 elements, which is impossible. Therefore, either $n_{13} = 1$, or $n_3 = 1$, or $n_2 = 1$, so that there is a normal Sylow p-subgroup for some prime p dividing the order of the group. ∎

Exercise 4.5.15

Prove that a group of order 351 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution. Note that $351 = 3^3 \cdot 13$. Recall that $n_{13} \equiv 1 \pmod 1 3$ and $n_{13} \mid 27$, so that $n_{13} = 1$ or 27. Moreover, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 13$, so that $n_3 = 1$ or 13. Assume, by way of contradiction, that both $n_{13} = 27$ and $n_3 = 13$. The Sylow-13 subgroups intersect trivially, while the Sylow-3 subgroups can have at most 9 elements in common. Then there are at least $27 \cdot 12 = 324$ elements of order 13 and at least $13 \cdot 8 = 104$ elements of order 3, giving a total of at least 428 elements, which is impossible. Therefore, either $n_{13} = 1$ or $n_3 = 1$, so that there is a normal Sylow p-subgroup for some prime p dividing the order of the group. ∎

Exercise 4.5.16

Let $|G| = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

Solution. Assume, by way of contradiction, that G does not contain a normal Sylow subgroup. In particular, $n_r \neq 1$ so that $n_r = pq$. Then G contains $pq(r-1)$ elements of order r. Moreover, $n_q = 1$ or pr. If $n_q = pr$, then there are $pr(q-1)$ elements of order q. Then there are

$$pq(r-1) + pr(q-1) = pqr - pq + prq - pr = 2pqr - p(q+r)$$

elements of order q or r. Observe that $(q-1)(r-1) - 1 > 0$ since $q \geq 3$ and $r \geq 5$. Then

$$(q-1)(r-1) - 1 = qr - q - r = qr - (q+r) > 0$$

so that $qr > q + r$. Then $pqr > p(q + r)$, so that $2pqr - p(q + r) > pqr$. This gives a contradiction since there are at most pqr elements in G. Therefore, $n_q = 1$, so that there is a normal Sylow subgroup in G. ■

Exercise 4.5.17

Prove that if $|G| = 105$ then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Solution. Note that $105 = 3 \cdot 5 \cdot 7$. Recall that $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 15$, so that $n_7 = 1$ or 15. Moreover, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 21$, so that $n_5 = 1$ or 21. Assume, by way of contradiction, that both $n_7 = 15$ and $n_5 = 21$. Then there are at least $15 \cdot 6 = 90$ elements of order 7 and at least $21 \cdot 4 = 84$ elements of order 5, giving a total of at least 174 elements, which is impossible. Therefore, either $n_7 = 1$ or $n_5 = 1$, so that there is a normal Sylow subgroup for either prime.

Without loss of generality, let $P \in \mathrm{Syl}_5(G)$ be normal. Then G/P has order 21, and G/P contains a normal Sylow 7-subgroup Q/P. Taking the preimage of Q/P under the projection homomorphism π, then $\pi^{-1}(Q/P)$ contains a normal Sylow 7-subgroup Q of G. From Corollary 4.20, we know that Q is characteristic in $\pi^{-1}(Q/P)$, and $\pi^{-1}(Q/P)$ is normal in G, so that Q is normal in G as well. Therefore, there is a normal Sylow 5-subgroup and a normal Sylow 7-subgroup in G. ■

Exercise 4.5.18

Prove that a group of order 200 has a normal Sylow 5-subgroup.

Solution. We have $n_5 \equiv 1 \pmod 5$, and $n_5 \mid 8$. The only choice is $n_5 = 1$, so that there is a normal Sylow 5-subgroup in the group. ■

Exercise 4.5.19

Prove that if $|G| = 6545$ then G is not simple.

Solution. Note that $6545 = 5 \cdot 7 \cdot 11 \cdot 17$. Moreover, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 7 \cdot 11 \cdot 17 = 1309$. Since n_5 is not modulo 5 when it is 7, 77, or 1309, $n_5 = 1$. Therefore, there is a normal Sylow 5-subgroup in G, so that G is not simple. ■

Exercise 4.5.20

Prove that if $|G| = 1365$ then G is not simple.

Solution. Note that $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Suppose that none of the $n_i \equiv 1 \pmod i$ for $i = 3, 5, 7, 13$ is equal to 1. Then $n_{13} = 1$ or 105, $n_7 = 1$ or 15, $n_5 = 1, 21$, or 91, and $n_3 = 1, 13$, or 91. Then the number of elements of order 13 is at least $105 \cdot 12 = 1260$, the number of elements of order 7 is at least $15 \cdot 6 = 90$, the number of elements of order 5 is at least $21 \cdot 4 = 84$, and the number of elements of order 3 is at least $13 \cdot 2 = 26$. This gives a total of at least $1260 + 90 + 84 + 26 = 1460$ elements, which is impossible. Therefore, there must be a normal Sylow subgroup in G, so that G is not simple. ■

Exercise 4.5.21

Prove that if $|G| = 2907$ then G is not simple.

Solution. Note that $2907 = 3^2 \cdot 17 \cdot 19$. Suppose that none of the $n_i \equiv 1 \pmod i$ for $i = 3, 17, 19$ is equal to 1. Then $n_{19} = 1$ or 153, $n_{17} = 1$ or 171, and $n_3 = 1$ or 19. Assuming that the Sylow 3-subgroups intersect nontrivially, then there are at least $19 \cdot 6 = 114$ elements of 3-power order, at least $153 \cdot 18 = 2754$ elements of order 19, and at least $171 \cdot 16 = 2736$ elements of order 17, giving a total of at least $114 + 2754 + 2736 = 5604$ elements, which is impossible. Therefore, there must be a normal Sylow subgroup in G, so that G is not simple. ■

Exercise 4.5.22

Prove that if $|G| = 132$ then G is not simple.

Solution. Note that $132 = 2^2 \cdot 3 \cdot 11$. Suppose that none of the $n_i \equiv 1 \pmod{i}$ for $i = 2, 3, 11$ is equal to 1. Then $n_{11} = 1$ or 12, $n_3 = 1$ or 22, and $n_2 = 1, 11$ or 33. Assuming that the Sylow 2-subgroups intersect nontrivially, then there are at least $11 \cdot 3 = 33$ elements of order 2-power order, at least $22 \cdot 2 = 44$ elements of order 3, and at least $12 \cdot 10 = 120$ elements of order 11, giving a total of at least $33 + 44 + 120 = 197$ elements, which is impossible. Therefore, there must be a normal Sylow subgroup in G, so that G is not simple. ■

Exercise 4.5.23

Prove that if $|G| = 462$ then G is not simple.

Solution. Note that $462 = 2 \cdot 3 \cdot 7 \cdot 11$. Since $n_{11} \equiv 1 \pmod{1}1$, and no divisor of $462/11 = 42$ is congruent to 1 modulo 11, $n_{11} = 1$. Therefore, there is a normal Sylow 11-subgroup in G, so that G is not simple. ■

Exercise 4.5.24

Prove that if G is a group of order 231 then $Z(G)$ contains a Sylow 11-subgroup of G and a Sylow 7-subgroup is normal in G.

Solution. Note that $231 = 3 \cdot 7 \cdot 11$. Since $n_{11} \equiv 1 \pmod{1}1$, and no divisor of $231/11 = 21$ is congruent to 1 modulo 11, $n_{11} = 1$. Therefore, there is a normal Sylow 11-subgroup in G. Let P be the Sylow 11-subgroup so that $P \trianglelefteq G$. We proceed similarly to the text regarding groups of order pq. Since P is normal, $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(P)$. Since $P \cong Z_{11}$, $|\text{Aut}(P)| = 10$. Moreover, the image of the action of G on P by conjugation has order dividing 10 but also divides 231, so that the image is trivial. Therefore, $G/C_G(P)$ is trivial, so that $C_G(P) = G$. This means that $P \leq Z(G)$, so that $Z(G)$ contains a Sylow 11-subgroup of G.

Next, we show that a Sylow 7-subgroup is normal in G. Since $n_7 \equiv 1 \pmod{7}$ and no divisor of 33 is congruent to 1 modulo 7, $n_7 = 1$. Therefore, there is a normal Sylow 7-subgroup in G. ■

Exercise 4.5.25

Prove that if G is a group of order 385 then $Z(G)$ contains a Sylow-7 subgroup of G and a Sylow 11-subgroup is normal in G.

Solution. Note that $385 = 5 \cdot 7 \cdot 11$. Since $n_7 \equiv 1 \pmod{7}$, and no divisor of $385/7 = 55$ is congruent to 1 modulo 7, $n_7 = 1$. Therefore, there is a normal Sylow 7-subgroup in G. Let P be the Sylow 7-subgroup so that $P \trianglelefteq G$. Similarly to the previous problem, it's trivial to see that $|\text{Aut}(P)| = 6$, and the image of the action of G on P by conjugation has order dividing 6 but also divides 385, so that the image is trivial. Therefore, $G/C_G(P)$ is trivial, so that $C_G(P) = G$. This means that $P \leq Z(G)$, so that $Z(G)$ contains a Sylow 7-subgroup of G.

Next, we show that a Sylow 11-subgroup is normal in G. Since $n_{11} \equiv 1 \pmod{1}1$ and no divisor of 35 is congruent to 1 modulo 11, $n_{11} = 1$. Therefore, there is a normal Sylow 11-subgroup in G. ■

Exercise 4.5.26

Let G be a group of order 105. Prove that if a Sylow 3-subgroup of G is normal then G is abelian.

Solution. Let P be the Sylow 3-subgroup of G. Since P is normal, $|G/P| = 35$. Then $|\text{Aut}(P)| = 2$, so that the image of the action of G on P by conjugation has order dividing 2 but also divides 35, so that the image is trivial. Therefore, $G/C_G(P)$ is trivial, so that $C_G(P) = G$. This means that $P \leq Z(G)$, so that $Z(G)$ contains a Sylow 3-subgroup of G. In particular, $|G/Z(G)| \leq |G/P| = 35$. Since groups of order 35 are cyclic and $|G/Z(G)|$ divides 35, $G/Z(G)$ is cyclic. By Exercise 3.1.36, then G is abelian. ■

Exercise 4.5.27

Let G be a group of order 315 which has a normal Sylow 3-subgroup. Prove that $Z(G)$ contains a Sylow 3-subgroup of G, and deduce that G is abelian.

Solution. Let P be the Sylow 3-subgroup of G. Note that $|P| = 9$, and $|G/P| = 35$. Then either $P \cong Z_9$ or $P \cong Z_3 \times Z_3$. In the first case, $|\text{Aut}(P)| = 6$, and in the second case, $|\text{Aut}(P)| = 48$. In both cases, $|\text{Aut}(P)|$ divides $|G/P| = 35$, so that the image of the action of G on P by conjugation is trivial. Therefore, $G/C_G(P)$ is trivial, so that $C_G(P) = G$. This means that $P \leq Z(G)$, so that $Z(G)$ contains a Sylow 3-subgroup of G. In particular, $|G/Z(G)| \leq |G/P| = 35$. Since groups of order 35 are cyclic and $|G/Z(G)|$ divides 35, $G/Z(G)$ is cyclic. By Exercise 3.1.36, then G is abelian. ■

Exercise 4.5.28

Let G be a group of order 1575. Prove that if a Sylow 3-subgroup of G is normal, then a Sylow 5-subgroup and a Sylow 7-subgroup are normal. In this situation prove that G is abelian.

Solution. Note that $|G| = 3^2 \cdot 5^2 \cdot 7$. Let P be the normal Sylow-3 subgroup of G. Let Q be a Sylow 5-subgroup and R be a Sylow 7-subgroup of G. Since $P \trianglelefteq G$, $PQ \leq G$ and $PR \leq G$ with orders $3^2 \cdot 5^2$ and $3^2 \cdot 7$ respectively.

Consider a Sylow 5-subgroup of PQ. Note that $n_5(PQ) \equiv 1 \pmod 5$ and $n_5(PQ) \mid 9$, so that $n_5(PQ) = 1$. Therefore, there is a normal Sylow 5-subgroup in PQ, which must be Q since Q is a Sylow 5-subgroup of PQ. It also follows that $P \leq N_{PQ}(Q) \leq N_G(Q)$. Since $|G : N_G(Q)|$ divides $|G : PQ| = 7$ so that $n_5(G) = 1$. We may use similar reasoning to show that $n_7(G) = 1$ as well. Therefore, there is a normal Sylow 5-subgroup and a normal Sylow 7-subgroup in G. Moreover, it is easy to see that the subgroups P, Q, and R are all abelian since p^2-order groups are abelian, and R has prime order hence it is cyclic.

Observe that the pairwise intersections of P, Q, and R are trivial since their orders are pairwise relatively prime. Then $PQR \leq G$ and $|PQR| = 3^2 \cdot 5^2 \cdot 7 = |G|$, so that $G = PQR$. Since P, Q, and R are all abelian, G is abelian as well. ■

Exercise 4.5.29

If G is a non-abelian simple group of order < 100, prove that $G \cong A_5$. (Eliminate all orders but 60.)

Solution. Let p, q, r be distinct primes. From the text, orders of 12, 30, pq, and p^2q where $p < q$ are eliminated. Moreover, orders of p are eliminated as they are cyclic, p^n are eliminated as they have nontrivial centers by Theorem 4.8, and pqr are eliminated by Exercise 4.5.16. The only remaining orders are 24, 36, 40, 48, 54, 56, 72, 80, 84, 90, and 96. We examine each in detail:

- $|G| = 24$: If $n_3 = 4$, then we may have G acting on the set of Sylow 3-subgroups by conjugation. Simplicity of G implies that $\ker \varphi$ is either trivial or all of G. If $\ker \varphi = \{1\}$, then $G \cong S_4$, which is not simple. If $\ker \varphi = G$, then every Sylow 3-subgroup is normal, which is also a contradiction.
- $|G| = 36$: If $n_3 = 4$, let P_1 and P_2 be two distinct Sylow 3-subgroups. Observe that $P_1 \cap P_2 \geq 3$ since P_1P_2 would have 81 elements otherwise. Then $N_G(P_1 \cap P_2)$ contains both P_1 and P_2. Moreover, $P_1 \subseteq N_G(P_1 \cap P_2)$ and $P_2 \subseteq N_G(P_1 \cap P_2)$. Then $|N_G(P_1 \cap P_2)|$ is a multiple of 9 but cannot be 9, since P and Q are both contained such that $P \neq Q$ as $n_3 = 4$. Then $|N_G(P_1 \cap P_2)|$ is either 18 or 36. If it is the former, then it has index 2 which means $N_G(P_1 \cap P_2)$ is normal in G, which is a contradiction. If it is the latter, then $P_1 \cap P_2$ is normal in G, which is also a contradiction.
- $|G| = 40$: Note that $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8$, so that $n_5 = 1$. Therefore, there is a normal Sylow 5-subgroup in G, which is a contradiction.
- $|G| = 48$: By simplicity, we see that $n_2 = 3$. Let P and Q be distinct Sylow-2 subgroups. Note that $|P \cap Q|$ cannot be 1 or 16 as P and Q are distinct. Moreover, they cannot be 2 or 4 since $|PQ|$ would be 128 or 16. Then $|P \cap Q| = 8$. Consider its normalizer $N_G(P \cap Q)$. Observe that $|N_G(P \cap Q)| > 16$ since P and Q are distinct, and the normalizer also divides 48. It follows that $|N_G(P \cap Q)| = 48$ so that $P \cap Q \trianglelefteq G$, which is a contradiction.
- $|G| = 54$: Note that $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 2$, so that $n_3 = 1$. Therefore, there is a normal Sylow 3-subgroup in G, which is a contradiction.
- $|G| = 56$: If $n_7 = 8$, then there are at least $8 \cdot 6 = 48$ elements of order 7, leaving 8 elements left. Since $|P| = 8$ for some $P \in \text{Syl}_2(G)$, we only have room for one Sylow 2-subgroup, so that $n_2 = 1$. Therefore, there is a normal Sylow 2-subgroup in G, which is a contradiction.
- $|G| = 72$: Suppose $n_3 = 4$. Then the induced homomorphism $\varphi : G \to S_4$ cannot have a nontrivial kernel. Then G has a nontrivial normal subgroup, which is a contradiction.
- $|G| = 80$: If $n_6 = 16$, then there are at least $16 \cdot 4 = 64$ elements of order 5, leaving only 16 elements left. Since $|P| = 16$ for some $P \in \text{Syl}_2(G)$, we only have room for one Sylow 2-subgroup, so that $n_2 = 1$. Therefore, there is a normal Sylow 2-subgroup in G, which is a contradiction.
- $|G| = 84$: Since $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 12$, $n_7 = 1$. Therefore, there is a normal Sylow 7-subgroup in G, which is a contradiction.

- $|G| = 90$: If $n_5 = 6$, then there are at least 24 elements of order 5. Moreover, $n_3 = 10$ such that all the Sylow-3 subgroups intersect trivially, then there are at least $10 \cdot 8 = 80$ elements of order 3, which is impossible. Then the Sylow-3 subgroups must intersect nontrivially. If $P, Q \in \mathrm{Syl}_3(G)$ such that $|P \cap Q| = 3$, we may use a similar argument as in $|G| = 36$ to determine that $N_G(P \cap Q)$ has order 45 or 90.
- $|G| = 96$: We have that either $n_3 = 4$ or $n_3 = 16$, since $n_3 \mid 32$. Consider $N_G(P)$ for some $P \in \mathrm{Syl}_3(G)$. Then $|G : N_G(P)| = 4$ if $n_3 = 4$ so that an induced homomorphism from G to S_4 has a nontrivial kernel, which is a contradiction. If $n_3 = 16$, we may use the same arguments as $|G| = 36$ or 90 to show a contradiction as well.

By Theorem 4.23, we know that simple groups of order 60 are isomorphic to A_5. Therefore, if G is a non-abelian simple group of order less than 100, then $G \cong A_5$. ■

Exercise 4.5.30

How many elements of order 7 must there be in a simple group of order 168?

Solution. Note that $168 = 2^3 \cdot 3 \cdot 7$. Since $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 24$, $n_7 = 1$ or 8. If $n_7 = 1$, then there is a normal Sylow 7-subgroup in the group, which is a contradiction. Therefore, $n_7 = 8$. Since each Sylow-7 subgroup has 6 elements of order 7, and the Sylow-7 subgroups intersect trivially, there are $8 \cdot 6 = 48$ elements of order 7 in a simple group of order 168. ■

Exercise 4.5.31

For $p = 2, 3$ and 5, find $n_p(A_5)$ and $n_p(S_5)$. (Note that $A_4 \leq A_5$.)

Solution. Recall that A_5 is simple. Then for A_5:

- $n_2(A_5)$: Since $A_4 \leq A_5$ and A_4 contains 3 Sylow-2 subgroups, $n_2(A_5) \geq 3$. Note that the elements of any $P \in \mathrm{Syl}_2(A_5)$ are of the form $(a\ b)(c\ d)$. Then there are 15 elements of order 2 in A_5, and each Sylow-2 subgroup has 3 elements of order 2, so that there are $15/3 = 5$ Sylow-2 subgroups in A_5.
- $n_3(A_5)$: Since A_5 contains 20 elements of order 3, and each Sylow-3 subgroup has 2 elements of order 3, there are $20/2 = 10$ Sylow-3 subgroups in A_5.
- $n_5(A_5)$: Since $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 12$, $n_5(A_5) = 6$.

For S_5:

- $n_2(S_5)$: Consider subgroups of the form $\langle (a\ b\ c\ d), (a\ c) \rangle$ where a is minimal out of the 4 integers. Subgroups of this form can be checked to see that they are indeed order 8 and are thus Sylow-2 subgroups (in fact, these are isomorphic to D_8). We may construct 15 such subgroups so that $n_2(S_5) \geq 15$. Since $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 15$, $n_2(S_5) = 15$.
- $n_3(S_5)$: We may use a similar counting argument as $n_2(A_5)$ to show that there are 10 Sylow-3 subgroups in S_5 as well.
- $n_5(S_5)$: Since we have more than two Sylow-5 subgroups in S_5, $n_5(S_5) = 6$.

■

Exercise 4.5.32

Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K. Deduce that if $P \in \mathrm{Syl}_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$ (in words: normalizers of Sylow p-subgroups are self-normalizing).

Solution. Let $k \in K$. Note that $kPk^{-1} \leq kHk^{-1} = H$ since $H \trianglelefteq K$. Moreover, kPk^{-1} is a Sylow p-subgroup of H since P is a Sylow p-subgroup of H. However, $P \trianglelefteq H$ implies that P is the unique Sylow p-subgroup of H. Therefore, $kPk^{-1} = P$, so that $P \trianglelefteq K$.

By assumption, $P \trianglelefteq H$ and $H \trianglelefteq N_G(H)$ by definition. The previous part shows that $P \trianglelefteq N_G(H)$. Since P is a Sylow p-subgroup of H, P is a Sylow p-subgroup of $N_G(H)$ as well. Then by the previous part, $P \trianglelefteq N_G(H)$ implies that $N_G(H) \trianglelefteq N_G(H)$, so that $N_G(H) = H$. ■

Exercise 4.5.33

Let P be a normal Sylow p-subgroup of G and let H be any subgroup of G. Prove that $P \cap H$ is the unique Sylow p-subgroup of H.

Solution. Assume that $P \cap H$ is not the unique Sylow p-subgroup of H. Then there is some $Q \in \mathrm{Syl}_p(H)$ such that $P \cap H$ is not contained in Q. Since $P \trianglelefteq G$ and Q is a p-subgroup of G, $Q \leq P$ since P is the unique Sylow p-subgroup of G. Moreover, $Q \leq H$, so that $Q \leq P \cap H$, which is a contradiction. Therefore, $P \cap H \trianglelefteq H$. ■

Exercise 4.5.34

Let $P \in \mathrm{Syl}_p(G)$ and assume $N \trianglelefteq G$. Use the conjugacy part of Sylow's Theorem to prove that $P \cap N$ is a Sylow p-subgroup of N. Deduce that PN/N is a Sylow p-subgroup of G/N (note that this may also be done by the Second Isomorphism Theorem—cf. Exercise 3.3.9).

Solution. We first note that it is clear that for any $g \in G$, then $g(P \cap N)g^{-1} = (gPg^{-1}) \cap (gNg^{-1}) = (gPg^{-1}) \cap N$ since $N \trianglelefteq G$. Since $P \cap N$ is a p-group, $P \cap N \leq Q$ for some $Q \in \mathrm{Syl}_p(N)$. Moreover, Q being a p-group implies that $Q \leq gPg^{-1}$ for some $g \in G$. By definition, $Q \leq N$ so that we have

$$Q \leq (gPg^{-1}) \cap N = g(P \cap N)g^{-1} \leq gQg^{-1}$$

From this, we have that $P \cap N \leq Q \leq g(P \cap N)g^{-1}$. By finiteness and the fact that $|P \cap N| = |g(P \cap N)g^{-1}|$, then $P \cap N = Q$. Therefore, $P \cap N$ is a Sylow p-subgroup of N.

Next, we show that PN/N is a Sylow p-subgroup of G/N. By the Second Isomorphism Theorem, we have that $PN/N \cong P/(P \cap N)$. Let $|G| = p^\alpha m$ where $p \nmid m$ and $|N| = p^\beta n$ where $p \nmid n$. Observe that $|G/N : PN/N| = |G : PN|$ divides $|G : P| = m$. It follows that $|G/N : PN/N|$ is relatively prime to p. Since $P \cap N \leq P$, $\beta \leq \alpha$ so that $|PN/N| = |P/(P \cap N)| = p^{\alpha-\beta}$. Therefore, PN/N is a Sylow p-subgroup of G/N. ■

Exercise 4.5.35

Let $P \in \mathrm{Syl}_p(G)$ and let $H \leq G$. Prove that $gPg^{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$. Give an explicit example that $hPh^{-1} \cap H$ is not necessarily a Sylow p-subgroup of H for any $h \in H$ (in particular, we cannot always take $g = 1$ in the first part of this theorem, as we could when H was normal in G).

Solution. By the First Sylow Theorem, there exists $Q \in \mathrm{Syl}_p(H)$. The conjugacy part of Sylow's Theorem guarantees that there exists some $g \in G$ such that $Q \leq gPg^{-1}$. Moreover, $Q \leq H$ so that $Q \leq gPg^{-1} \cap H$. Observe that $gPg^{-1} \cap H$ is a p-group since it is a subgroup of gPg^{-1}. Therefore, $gPg^{-1} \cap H \leq Q$ for some $Q \in \mathrm{Syl}_p(H)$. From this, we have that $Q = gPg^{-1} \cap H$, so that $gPg^{-1} \cap H$ is a Sylow p-subgroup of H.

Let $G = S_3$, $P = \langle (1\,2) \rangle$ and $H = \langle (1\,3) \rangle$ with $p = 2$. Then P is a Sylow-2 subgroup of G. However, $hPh^{-1} \cap H$ is trivial for any $h \in H$, so that $hPh^{-1} \cap H$ is not a Sylow-2 subgroup of H for any $h \in H$. ■

Exercise 4.5.36

Prove that if N is a normal subgroup of G then $n_p(G/N) \leq n_p(G)$.

Solution. We first show that the map $\varphi \colon \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/N)$ defined by $\varphi(P) = PN/N$ is well defined. Let $P \in \mathrm{Syl}_p(G)$. By Exercise 4.5.34, we have that PN/N is a Sylow p-subgroup of G/N, so that $\varphi(P) \in \mathrm{Syl}_p(G/N)$.

We now show that φ is surjective. Let $\overline{Q} \in \mathrm{Syl}_p(G/N)$. By the conjugacy part of Sylow's Theorem, there exists some $\overline{g} \in G/N$ such that

$$\overline{Q} = \overline{g}\,\overline{P}\,\overline{g}^{-1} = \pi(gPg^{-1})$$

where $\pi \colon G \to G/N$ is the natural projection homomorphism. Since $P \in \mathrm{Syl}_p(G)$, $gPg^{-1} \in \mathrm{Syl}_p(G)$ as well. Hence, $\pi(gPg^{-1}) = \overline{Q}$ so that $\varphi(gPg^{-1}) = \overline{Q}$. Therefore, φ is surjective, so that $n_p(G/N) \leq n_p(G)$. ■

Exercise 4.5.37

Let R be a normal p-subgroup of G (not necessarily a Sylow subgroup).

(a) Prove that R is contained in every Sylow p-subgroup of G.
(b) If S is another normal p-subgroup of G, prove that RS is also a normal p-subgroup of G.
(c) The subgroup $O_p(G)$ is defined to be the group generated by all normal p-subgroups of G. Prove that $O_p(G)$ is the unique largest p-subgroup of G and $O_p(G)$ equals the intersection of all Sylow p-subgroups of G.
(d) Let $\overline{G} = G/O_p(G)$. Prove that $O_p(\overline{G}) = \overline{1}$ (i.e., $\overline{G}$ has no nontrivial normal p-subgroup).

Solution.

(a) Let $P \in \mathrm{Syl}_p(G)$. Observe that RP is a p-subgroup of G since R and P are both p-groups. Moreover, $P \leq RP$ and P is a Sylow p-subgroup of G, so that $P = RP$. It follows that $R \leq P$, so that R is contained in every Sylow p-subgroup of G.

(b) Let $g \in G$. Since $R \trianglelefteq G$ and $S \trianglelefteq G$, $gRg^{-1} = R$ and $gSg^{-1} = S$. Then $g(RS)g^{-1} = (gRg^{-1})(gSg^{-1}) = RS$, so that $RS \trianglelefteq G$. Moreover, RS is a p-group because $R \cap S$ is a p-group, hence $|RS|$ is a power of p.

(c) By induction, we have that the product of any finite number of normal p-subgroups of G is a normal p-subgroup of G. Since the set of normal p-subgroups of G is nonempty (it contains the trivial subgroup), $O_p(G)$ is a normal p-subgroup of G. Moreover, if R is a normal p-subgroup of G, then $R \leq O_p(G)$ by definition. Uniqueness follows from that fact that $O_p(G)$ contains every normal p-subgroup of G and is itself a normal p-subgroup of G.

Next, we show that $O_p(G)$ equals the intersection of all Sylow p-subgroups of G. Let $\mathcal{P}$ be the set of all Sylow p-subgroups of G. Since every normal p-subgroup of G is contained in every Sylow p-subgroup of G, $O_p(G)$ is contained in every Sylow p-subgroup of G, so that $O_p(G) \leq \bigcap_{P \in \mathcal{P}} P$. Conversely, let $\bigcap_{P \in \mathcal{P}} P = R$. Since every Sylow p-subgroup contains every normal p-subgroup, every Sylow p-subgroup contains R, so that R is a normal subgroup of G. Moreover, since the intersection of any number of subgroups is a subgroup, R is a subgroup. Finally, since each Sylow p-subgroup is a p-group, their intersection is also a p-group. Therefore, $\bigcap_{P \in \mathcal{P}} P = R \leq O_p(G)$.

(d) Let $\overline{R}$ be a normal p-subgroup of $\overline{G}$. Let $\pi\colon G \to \overline{G}$ be the natural projection homomorphism. Then $\pi^{-1}(\overline{R})$ is a normal subgroup of G since $\overline{R}$ is normal in $\overline{G}$. Moreover, $\pi^{-1}(\overline{R})$ is a p-group as follows: using the First Isomorphism Theorem, we have that $\pi^{-1}(\overline{R})/O_p(G) \cong \overline{R}$. It follows that

$$|\pi^{-1}(\overline{R})| = |O_p(G)||\overline{R}| = p^\alpha p^\beta = p^{\alpha+\beta}$$

hence $\pi^{-1}(\overline{R})$ is a p-group. Since $\pi^{-1}(\overline{R})$ is a normal p-subgroup of G, $\pi^{-1}(\overline{R}) \leq O_p(G)$. It follows that $\overline{R} = \pi(\pi^{-1}(\overline{R})) \leq \pi(O_p(G)) = \overline{1}$, so that $\overline{R}$ is trivial. Therefore, $O_p(\overline{G}) = \overline{1}$. ∎

Exercise 4.5.38

Use the method of proof in Sylow's Theorem to show that if n_p is not congruent to 1 (mod p)^2 then there are distinct Sylow p-subgroups P and Q of G such that $|P : P \cap Q| = |Q : P \cap Q| = p$.

Solution. Let G act on $\mathrm{Syl}_p(G) = \{P_1, P_2, \ldots P_{n_p}\}$ by conjugation. Note that $P = P_1$ also acts on $\mathrm{Syl}_p(G)$ by conjugation, which we can then decompose into the orbits

$$\mathrm{Syl}_p(G) = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_k, \quad n_p = \sum_{i=1}^{k} |\mathcal{O}_i|$$

By definition, $|\mathcal{O}_i| = |P : N_P(P_i)|$. Using Lemma 4.19, we see that $N_P(P_i) = P \cap N_G(P_i) = P \cap P_i$, hence $|\mathcal{O}_i| = |P : P \cap P_i|$. We also note that $|\mathcal{O}_1| = 1$ since $P \in \mathrm{Syl}_p(G)$ is fixed by the action of P on $\mathrm{Syl}_p(G)$ by conjugation, and $|\mathcal{O}_i| > 1$ for $i > 1$ since P_i is not fixed by the action of P on $\mathrm{Syl}_p(G)$ by conjugation.

By definition, each P_i is a p-group, hence their intersections are also p-groups. It follows that each $|\mathcal{O}_i|$ is a power of p. If the orders of each $\mathcal{O}_i$ are all at least p^2, hence

$$n_p = |\mathcal{O}_1| + \sum_{i=2}^{k} |\mathcal{O}_i| \equiv 1 \pmod{p}^2$$

Then n_p is congruent to 1 (mod p)^2, which is a contradiction. Therefore, there exists some $i > 1$ such that $|\mathcal{O}_i| = p$. Let $Q = P_i$. Then $|P : P \cap Q| = p$ as desired. By symmetry, we also have that $|Q : P \cap Q| = p$. ∎

Exercise 4.5.39

Show that the subgroup of strictly upper triangular matrices in $\mathrm{GL}_n(\mathbb{F}_p)$ (cf. Exercise 2.1.17) is a Sylow p-subgroup of this finite group. (Use the order formula in Section 1.4 to find the order of a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.)

Solution. According to the definition of $\mathrm{GL}_n(\mathbb{F}_p)$, we have that

$$|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1} (p^n - p^i) = p^{n(n-1)/2} \prod_{i=1}^{n} (p^i - 1)$$

Then the order of a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ is $p^{n(n-1)/2}$. Let P be the subgroup of strictly upper triangular matrices in $\mathrm{GL}_n(\mathbb{F}_p)$. We know by Exercise 2.1.17 that P is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. If the main diagonal of a matrix in P are all 1's, then there are $n(n-1)/2$ entries above the main diagonal, and each entry can be any element of $\mathbb{F}_p$. It follows that $|P| = p^{n(n-1)/2}$, so that P is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. ■

Exercise 4.5.40

Prove that the number of Sylow p-subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ is $p+1$. (Exhibit two distinct Sylow p-subgroups.)

Solution. Since $n_p = |G : N_P(G)|$ for any $P \in \mathrm{Syl}_p(G)$, we can find n_p by finding the normalizer of a Sylow p-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let P be the subgroup of strictly upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. We have that

$$P = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}_p \right\} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

Let A be the generator of P. Let $X \in G$ be an arbitrary element of $\mathrm{GL}_2(\mathbb{F}_p)$. For X to be in $N_G(P)$, then we must have that $XAX^{-1} \in P$, or $XAX^{-1} = A^k$ for some $k \in \mathbb{F}_p$. Let

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad X^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Then we have that

$$XAX^{-1} = \frac{1}{ad-bc} \begin{pmatrix} ad - ac - bc & a^2 \\ -c^2 & -bc + ac + ad \end{pmatrix}$$

For XAX^{-1} to be in P, we must have that $c = 0$. It follows that

$$XAX^{-1} = \frac{1}{ad} \begin{pmatrix} ad & a^2 \\ 0 & ad \end{pmatrix}, \quad N_G(P) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, d \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

where $a, d \in \mathbb{F}_p^\times$ since X must be invertible. We have that $|N_G(P)| = p(p-1)^2$, so that

$$n_p = |G : N_G(P)| = \frac{|\mathrm{GL}_2(\mathbb{F}_p)|}{|N_G(P)|} = \frac{p(p-1)^2(p+1)}{p(p-1)^2} = p+1$$ ■

Exercise 4.5.41

Prove that $\mathrm{SL}_2(\mathbb{F}_4) \cong A_5$ (cf. Exercise 2.1.9 for the definition of $\mathrm{SL}_2(\mathbb{F}_4)$).

Solution. It is clear that $|\mathrm{SL}_2(\mathbb{F}_4)| = 60$. Moreover, $n_5 \equiv 1 \pmod 5$, so we only need to exhibit 2 distinct Sylow-5 subgroups of $\mathrm{SL}_2(\mathbb{F}_4)$ to show that $\mathrm{SL}_2(\mathbb{F}_4)$ is simple.

Let α and β be the two remaining elements of $\mathbb{F}_4$ that aren't 0 or 1. Since $\mathbb{F}_4^\times$ is cyclic, α and β are generators of $\mathbb{F}_4^\times$, are inverses of each other, and satisfy $\alpha^2 = \beta$ and $\beta^2 = \alpha$, hence $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. We also claim that $\mathbb{F}_4 \cong V_4$ as additive groups. If $\mathbb{F}_4 \cong \mathbb{Z}/4\mathbb{Z}$ instead, then we may suppose that $1 + 1 = \alpha$. Then $(1+1)(1+1) = \alpha^2 \neq 1$. But by distribution, we have that $(1+1)(1+1) = 1+1+1+1 = 0$, which is a contradiction. Therefore, $\mathbb{F}_4 \cong V_4$, and every element has additive order 2.

To find two distinct Sylow-5 groups of $\mathrm{SL}_2(\mathbb{F}_4)$, we first find an element of order 5 in $\mathrm{SL}_2(\mathbb{F}_4)$. Noting that $\alpha + 1 = \alpha^2$, consider the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$$

Then we have that

$$A^2 = \begin{pmatrix} 1 & \alpha \\ \alpha & \alpha^2 + 1 \end{pmatrix}$$

where $\alpha^2 + 1 = 1 + \alpha + 1 = \alpha$. We also have

$$A^3 = \begin{pmatrix} \alpha & \alpha \\ \alpha & 1 \end{pmatrix}$$

In computing $A^3 \cdot A^2$, we obtain $\alpha^2 + \alpha = \alpha(\alpha + 1) = 1$ so that $|A| = 5$. Considering B with α^2 in place of α in A, it can be similarly concluded that $|B| = 5$ with $\langle B \rangle \neq \langle A \rangle$. Since we have produced 2 distinct Sylow-5 subgroups of $\mathrm{SL}_2(\mathbb{F}_4)$, $\mathrm{SL}_2(\mathbb{F}_4)$ is simple. By Theorem 4.23, we have that $\mathrm{SL}_2(\mathbb{F}_4) \cong A_5$. ■

Exercise 4.5.42

Prove that the group of rigid motions in $\mathbb{R}^3$ of an icosahedron is isomorphic to A_5. (Recall that the order of this group is 60: Exercise 1.2.13.)

Solution. Since an icosahedron has 12 vertices, we obtain 6 pairs of opposite vertices. For each pair, we admit rotations of $2\pi/5$ about the axis through the pair since 5 faces meet at each vertex. This subgroup is clearly $\mathbb{Z}/5\mathbb{Z}$, hence we have 6 Sylow-5 subgroups. Since $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 12$, $n_5 = 6$. Therefore, the group of rigid motions in $\mathbb{R}^3$ of an icosahedron is simple. By Theorem 4.23, we have that the group of rigid motions in $\mathbb{R}^3$ of an icosahedron is isomorphic to A_5. ■

Exercise 4.5.43

Prove that the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron is isomorphic to A_5. (As with the cube and tetrahedron, the icosahedron and dodecahedron are dual solids.) [Recall that the order of this group is 60: Exercise 1.2.12.]

Solution. By duality of the icosahedron and dodecahedron, we may associate pairs of vertices in Exercise 4.5.42 with pairs of faces instead. The proof is very similar, hence we omit the details. We conclude that the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron is isomorphic to A_5. ■

Exercise 4.5.44

Let p be the smallest prime dividing the order of the finite group G. If $P \in \mathrm{Syl}_p(G)$ and P is cyclic, prove that $N_G(P) = C_G(P)$.

Solution. Observe that $C_G(P) \leq N_G(P)$ by definition. Note that $|P| = p^k$ for some $k \in \mathbb{Z}^+$ and is cyclic. Noting that $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ and $|\mathrm{Aut}(P)| = p^{k-1}(p-1)$, then $|N_G(P)/C_G(P)|$ divides $p^{k-1}(p-1)$. It follows that every prime q that divides $|N_G(P)/C_G(P)|$ must satisfy $q \mid p^{k-1}(p-1)$. Since p is the smallest prime dividing the order of G, but P is also a Sylow p-subgroup of G, $|N_G(P)/C_G(P)|$ cannot be divisible by p, hence it divides $p-1$. Since $p - 1 < p$, $|N_G(P)/C_G(P)|$ cannot be divisible by any prime, so that $|N_G(P)/C_G(P)| = 1$. Therefore, $N_G(P) = C_G(P)$. ■

Exercise 4.5.45

Find generators for a Sylow p-subgroup of S_{2p}, where p is an odd prime. Show that this is an abelian group of order p^2.

Solution. Utilizing the formula obtained from Exercise 1.2.8, the highest power of p dividing $|S_{2p}|$ is p^2. We can find a Sylow p-subgroup of S_{2p} by considering the subgroup generated by the two disjoint p-cycles $(1\ 2\ cdots\ p)$ and $(p\ +\ 1\ p\ +\ 2\ cdots\ 2p)$. Since these two cycles are disjoint, they commute with each other, so that the subgroup generated by these two cycles is an abelian group. Moreover, since each cycle has order p, the subgroup generated by these two cycles has order p^2. ■

Exercise 4.5.46

Find generators for a Sylow p-subgroup of S_{p^2}, where p is a prime. Show that this is a non-abelian group of order p^{p+1}.

Solution. Again, we may use Exercise 1.2.8 to see that the highest power of p dividing $|S_{p^2}|$ is p^{p+1}. To build the Sylow p-subgroup P, we note that $|P| = p^p p$, which suggest that we will need to construct two subgroups A and B of P such that $|A| = p^p$, $|B| = p$, and $P = AB$. Let $\alpha_i = (ip\ +\ 1\ ip\ +\ 2\ cdots\ ip\ +\ p)$ for $i = 0, 1, \ldots p-1$. It is clear that the α_i are pairwise disjoint p-cycles, hence $A = \langle \alpha_0, \alpha_1, \ldots \alpha_{p-1} \rangle$ is an abelian group of order p^p.

Consider the p-cycle

$$\beta = (1\ p+1\ 2p+1\ \cdots (p-1)p+1)(2\ p+2\ 2p+2\ \cdots (p-1)p+2)\cdots(p\ 2p\ 3p\ cdots\ p^2)$$

It is clear that β has order p. Moreover, β acts on A by conjugation as follows:

$$\beta\alpha_i\beta^{-1} = \alpha_{i+1}$$

where the indices are taken modulo p. Equipped with $B = \langle\beta\rangle$, we see that B normalizes A since β permutes the generators of A. Moreover, $A \cap B = \{1\}$ since A is an abelian group of order p^p and B is a cyclic group of order p. It follows that $P = AB$ is a subgroup of S_{p^2} of order p^{p+1}, so that P is a Sylow p-subgroup of S_{p^2}. Finally, we show that P is non-abelian. Note that $\beta\alpha_0\beta^{-1} = \alpha_1 \neq \alpha_0$, so that β does not commute with α_0. Therefore, P is non-abelian. ■

Exercise 4.5.47

Write and execute a computer program which
(i) gives each number $n < 10,000$ that is not a power of a prime and that has some prime divisor p such that n_p is not forced to be 1 for all groups of order n by the congruence condition in Sylow's Theorem, and
(ii) gives for each n in (i) the factorization of n into prime powers and gives the list of all permissible values of n_p for all primes p dividing n (i.e., those values not ruled out by Part 3 of Sylow's Theorem).

Solution. See `sylow-odd.txt` for the solution. ■

Exercise 4.5.48

Carry out the same process as in the preceding exercise for all even numbers less than 1,000. Explain the relative lengths of the lists versus the number of integers tested.

Solution. See `sylow-even.txt` for the solution.

In Exercise 4.5.47, we only counted 1,714 integers. In this exercise, we counted 491 integers which include the integers of the form $2^\alpha m$, hence n_2 will not be forced to be 1 for all groups of order n by the congruence condition in Sylow's Theorem. Therefore, we have a much longer relative list of integers in this exercise than in the previous exercise. ■

Exercise 4.5.49

Prove that if $|G| = 2^n m$ where m is odd and G has a cyclic Sylow-2 subgroup, then G has a normal subgroup of order m. (Use induction, Exercise 4.2.11 and Exercise 4.2.12.)

Solution. From Exercise 4.2.11 and Exercise 4.2.12, we may deduce the following: if G is finite with $x \in G$ such that $|x|$ is even and $|G|/|x|$ is odd, then G has a normal subgroup of index 2.

Fix an odd m. Inducting on n, we observe that $n = 1$ is trivially true as the subgroup would have order m and index 2, hence it would be normal. Supposing the hypothesis is true up to $n-1$, consider $|G| = 2^n m$. Let $x \in G$ be a generator for the cyclic Sylow-2 subgroup of G. Then $|x|$ is even and $|G|/|x|$ is odd, so that G has a normal subgroup N of index 2. In particular, $|N| = 2^{n-1}m$ so that by the inductive hypothesis, N (which is cyclic because the Sylow-2 subgroup is cyclic) has a normal cyclic subgroup K of order m.

We now show that $K \trianglelefteq G$. We claim that K is the unique subgroup of N of order m. If $L \leq N$ is another subgroup with order m, then $K \trianglelefteq N$ implies that $KL \leq N$, hence

$$|KL| = \frac{|K||L|}{|K \cap L|} = \frac{m^2}{|K \cap L|}.$$

Since $|KL|$ divides $|N|$, $m/|K \cap L|$ divides 2^{n-1}, so that $|K \cap L| = m$. It follows that $K = L$, so that K is the unique subgroup of N of order m. Since K is the unique subgroup of N of order m, $gKg^{-1} = K$ for any $g \in G$, so that $K \trianglelefteq G$. Therefore, G has a normal subgroup of order m. ■

Exercise 4.5.50

Prove that if U and W are normal subsets of a Sylow p-subgroup P of G then U is conjugate to W if and only if U is conjugate to W in $N_G(P)$. Deduce that two elements in the center of P are conjugate in G if and only if they are conjugate in $N_G(P)$. (A subset U of P is normal in P if $N_P(U) = P$.)

Solution.
$\boxed{\Rightarrow}$ Suppose U is conjugate to W in G. Then there exists $g \in G$ such that $gUg^{-1} = W$, or $g^{-1}Wg = U$. Taking some $p \in P$ and some $gpg^{-1} \in gPg^{-1}$, then

$$gpg^{-1}Wgp^{-1}g^{-1} = gpUp^{-1}g^{-1} = gUg^{-1} = W$$

where $pUp^{-1} = U$ since $U \trianglelefteq P$.

Since gPg^{-1} is a p-group, and $W \trianglelefteq P$, $P \leq N_G(W)$. Hence, $P \in \mathrm{Syl}_p(N_G(W))$. By the conjugacy part of Sylow's Theorem, there exists some $n \in N_G(W)$ such that $nPn^{-1} = gPg^{-1}$. Then $n^{-1}g \in N_G(P)$ since $n^{-1}gPg^{-1}gn^{-1} = P$, so that $n^{-1}gUg^{-1}n = n^{-1}Wn = W$. Therefore, U is conjugate to W in $N_G(P)$.
$\boxed{\Leftarrow}$ If U is conjugate to W in $N_G(P)$, then there exists some $n \in N_G(P)$ such that $nUn^{-1} = W$. Since $N_G(P) \leq G$, U is conjugate to W in G as well because $n \in G$. ■

Exercise 4.5.51

Let P be a Sylow p-subgroup of G and let M be any subgroup of G which contains $N_G(P)$. Prove that $|G : M| \equiv 1 \pmod{p}$.

Solution. Since $P \in \mathrm{Syl}_p(G)$, $P \in \mathrm{Syl}_p(M)$ as well since $N_G(P) \leq M$. Moreover, let $m \in N_M(P)$. Then $mPm^{-1} = P$, so that $m \in N_G(P)$ since P is a Sylow p-subgroup of G. Then we have $N_M(P) \subseteq N_G(P)$. Conversely, $N_G(P) \subseteq N_M(P)$ since $N_G(P) \leq M$. It follows that $N_M(P) = N_G(P)$, so that $|G : N_G(P)| = |M : N_M(P)| \equiv 1 \pmod{p}$. Then

$$|G : N_G(P)| = |G : M||M : N_G(P)| = |G : M||M : N_M(P)| \equiv 1 \pmod{p}$$

so that $|G : M| \equiv 1 \pmod{p}$. ■

Exercise 4.5.52

Suppose G is a finite simple group in which every proper subgroup is abelian. If M and N are distinct, maximal subgroups of G, prove that $M \cap N = 1$. (See Exercise 4.3.23.)

Solution. Let $X = M \cap N$. Because M and N are abelian, then X is abelian. Moreover, $N_G(X)$ contains both M and N so that $N_G(X) = G$ and $X \trianglelefteq G$. Simplicity of G forces $X = 1$. Therefore, $M \cap N = 1$. ■

Exercise 4.5.53

Use the preceding exercise to prove that if G is any non-abelian group in which every proper subgroup is abelian then G is not simple. (Let G be a counterexample to this assertion and use Exercise 4.3.24 to show that G has more than one conjugacy class of maximal subgroups. Use the method of Exercise 4.3.23 to count the elements which lie in all conjugates of M and N, where M and N are nonconjugate maximal subgroups of G; show that this gives more than $|G|$ elements.)

Solution. Assume for the sake of contradiction that G is simple. We first note that G is the union of its maximal subgroups, since every proper subgroup of G is contained in a maximal subgroup. Moreover, conjugates of maximal subgroups are also maximal: if M is a maximal subgroup of G with $g \in G$ such that $gMg^{-1} \leq H$ for some $H \leq G$, then $M \leq g^{-1}Hg$ so that $g^{-1}Hg = G$ or M. It follows that $gMg^{-1} = G$ or M, hence $gMg^{-1} = M$ since M is a proper subgroup of G. Therefore, gMg^{-1} is a maximal subgroup of G. Lastly, simplicity of G forces M to be a nonnormal subgroup, hence $N_G(M) = M$ by maximality of M.

We now show that there are at least two distinct conjugacy classes of maximal subgroups of G. Assume by way of contradiction that there is only one conjugacy class of maximal subgroups of G. Let M be a maximal subgroup of G such that for any maximal subgroup N of G, there exists some $g \in G$ such that $gMg^{-1} = N$. Moreover, recall that the number of conjugates of M is $|G : N_G(M)| = |G : M|$. Since conjugates intersect trivially by Exercise 4.5.52, then the number of elements in the union of all conjugates of M is $|G : M|(|M| - 1) + 1$, or $|G| - |G : M| + 1$. However, $M \neq G$, hence $|G : M| > 1$, so that $|G| - |G : M| + 1 < |G|$. This is a contradiction since G is the union of its maximal subgroups. Therefore, there are at least two distinct conjugacy classes of maximal subgroups of G.

Lastly, observe that $|M| \geq 2$ and $|N| \geq 2$ since M and N are non-abelian. It follows that

$$|G| - |G : M| - |G : N| = |G|\left(1 - \frac{1}{|M|} - \frac{1}{|N|}\right) \geq 0.$$

From this, we see that

$$|G| + (|G| - |G : M| - |G : N|) + 1 > |G|$$

so that G has more than $|G|$ elements, which is a contradiction. Therefore, G is not simple. ■

Exercise 4.5.54

Prove the following classification: if G is a finite group of order $p_1 p_2 \cdots p_r$ where the p_i's are distinct primes such that p_i does not divide $p_j - 1$ for all i and j, then G is cyclic. (By induction, every proper subgroup of G is cyclic, so G is not simple by the preceding exercise. If N is a nontrivial proper normal subgroup, N is cyclic and G/N acts as automorphisms of N. Use Proposition 16 to show that $N \leq Z(G)$ and use induction to show $G/Z(G)$ is cyclic, hence G is abelian by Exercise 3.1.36.)

Solution. We proceed by induction on r. For $r = 1$, then $|G| = p_1$ which implies that G is cyclic.

Assume by way of contradiction that G is not abelian. By Exercise 4.5.53, G is not simple. Let N be a nontrivial normal subgroup of G with $|N| = q_1 q_2 \cdots q_s$ are primes from $p_1, p_2, \ldots, p_r$. Moreover, N is cyclic by the inductive hypothesis.

By $N \trianglelefteq G$, then G acts on N which induces the homomorphism $\psi \colon G \to \mathrm{Aut}(N)$. Moreover, cyclicity of N implies that

$$|\mathrm{Aut}(N)| = \varphi(|N|) = \prod_{i=1}^{s} (q_i - 1).$$

By definition, we have that no p_i divides any of $q_i - 1$, hence $\ker \psi = G$. It follows that G acts trivially on N, so that $N \leq Z(G)$. We then see that $G/Z(G)$ is cyclic by the inductive hypothesis since $|G/Z(G)|$ divides $|G|$. By Exercise 3.1.36, G is abelian, which is a contradiction. Therefore, G is abelian.

Finally, we show that G is cyclic. Let g_i be a generator of the Sylow p_i-subgroup of G for each i. Since the Sylow p_i-subgroups of G are all cyclic, $\langle g_i \rangle \cap \langle g_j \rangle = 1$ for all $i \neq j$. It follows that $g_1 g_2 \cdots g_r$ has order $p_1 p_2 \cdots p_r$, so that $G = \langle g_1 g_2 \cdots g_r \rangle$ is cyclic. ■

Exercise 4.5.55

Prove the converse to the preceding exercise: if $n \geq 2$ is an integer such that every group of order n is cyclic, then $n = p_1 p_2 \cdots p_r$ is a product of distinct primes and p_i does not divide $p_j - 1$ for all i, j. (If n is not of this form, construct noncyclic groups of order n using direct products of noncyclic groups of order p^2 and pq, where $p \mid q - 1$.)

Solution. We proceed by contrapositive, i.e., if n is not a product of distinct primes, or if n is a product of distinct primes, but there exist some i and j such that $p_i \mid p_j - 1$, then there exists some noncyclic group of order n.

- Suppose n is not a product of distinct primes, i.e., $n = p^2 m$ for some prime p and some integer $m \geq 1$. Consider the group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Note that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is a noncyclic group of order p^2, since every nonidentity element of $\mathbb{Z}/p\mathbb{Z}$ has order p. If G were cyclic, then the isomorphic copy of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in G, namely $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \{0\}$, would also be cyclic, which is a contradiction. Therefore, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is a noncyclic group of order n.
- By the text, if $p \mid q - 1$, then there exists a non-abelian group of order pq. Let H be such a group, and let m be an integer such that $n = pqm$, and $(pq, m) = 1$. Consider the group $H \times \mathbb{Z}/m\mathbb{Z}$. Using similar reasoning as in the previous case, $(H \times \{0\}) \cong H$ is a noncyclic subgroup of $H \times \mathbb{Z}/m\mathbb{Z}$, so that $H \times \mathbb{Z}/m\mathbb{Z}$ is a noncyclic group of order n. ■

Exercise 4.5.56

If G is a finite group in which every proper subgroup is abelian, show that G is solvable.

Solution. We proceed by induction on $|G|$. If G is abelian, then G is solvable. Assume that the hypothesis holds for all groups of order less than $|G|$. If G is not simple, then there exists some nontrivial normal subgroup N of G. Since N and G/N are both groups in which every proper subgroup is abelian (specifically, G/N has every proper subgroup abelian because each $H/N \leq G/N$ has some $H \leq G$ that is abelian, by hypothesis), by the inductive hypothesis, N and G/N are solvable. It follows that G is solvable as well. If G is simple, then by Exercise 4.5.53, G is abelian, hence solvable. Therefore, in either case, G is solvable. ■

4.6 The Simplicity of A_n

Let G be a group and let Ω be an infinite set.

Exercise 4.6.1

Prove that A_n does not have a proper subgroup of index $< n$ for all $n \geq 5$.

Solution. Suppose $H \leq A_n$ is a proper subgroup of index $k < n$. Then A_n acts on the left cosets of H by left multiplication, inducing a homomorphism $\varphi\colon A_n \to S_k$. Observe that $n/2 > 0$ for all $n \geq 5$. This lets us conclude that $\ker\varphi$ must be nontrivial, for otherwise φ would be injective and $|A_n| \leq |S_k|$. However, $k < n$ implies $k \leq n-1$, or $k! \leq (n-1)! < n!/2 = |A_n|$, which is a contradiction. Since $\ker\varphi$ is a nontrivial normal subgroup of A_n, $\ker\varphi = A_n$ since A_n is simple for all $n \geq 5$. It follows that φ is the trivial homomorphism, so that $H = A_n$, which is a contradiction. Therefore, A_n does not have a proper subgroup of index $< n$ for all $n \geq 5$. ∎

Exercise 4.6.2

Find all normal subgroups of S_n for all $n \geq 5$.

Solution. Observe some normal subgroups of S_n are 1, A_n, and S_n for all $n \geq 5$. To see that these are the only normal subgroups of S_n, let $N \trianglelefteq S_n$ be a normal subgroup, and consider $N \cap A_n$. We claim that $N \cap A_n \trianglelefteq A_n$.

Let $\sigma \in N \cap A_n$. Then for any $\tau \in A_n$, we have that $\tau\sigma\tau^{-1} \in A_n$ since A_n is a subgroup of S_n. Moreover, $\tau\sigma\tau^{-1} \in N$ since $N \trianglelefteq S_n$. It follows that $\tau\sigma\tau^{-1} \in N \cap A_n$, so that $N \cap A_n \trianglelefteq A_n$. Since A_n is simple for all $n \geq 5$, $N \cap A_n$ is either 1 or A_n.

(1) If $N \cap A_n = A_n$, then $A_n \subseteq N$. By maximality of A_n in S_n, then $N = A_n$ or $N = S_n$.
(2) If $N \cap A_n = 1$, consider $NA_n \leq S_n$ because $N \trianglelefteq S_n$ and $A_n \trianglelefteq S_n$. It follows that $|NA_n| = |N||A_n|$. Because $NA_n \leq S_n$, then $|NA_n| = |N||A_n| \leq |S_n|$, so that $|N| \leq 2$. If $|N| = 2$, then $N = \langle\rho\rangle$ for some order 2 element ρ. However, $N \trianglelefteq S_n$ implies that $\tau\rho\tau^{-1} = \rho$ for all $\tau \in S_n$, or that $\rho \in Z(S_n)$, which is a contradiction since $Z(S_n) = 1$ for all $n \geq 3$. Therefore, $|N| = 1$, so that $N = 1$. ∎

Exercise 4.6.3

Prove that A_n is the only proper subgroup of index $< n$ in S_n for all $n \geq 5$.

Solution. Let $H \leq S_n$ be a proper subgroup where $|S_n : H| = k < n$. Then S_n acts on the left cosets of H by left multiplication, inducing a homomorphism $\varphi\colon S_n \to S_k$. Observe that $n/2 > 0$ for all $n \geq 5$. This lets us conclude that $\ker\varphi$ must be nontrivial, for otherwise φ would be injective and $|S_n| \leq |S_k|$. However, $k < n$ implies $k \leq n-1$, or $k! \leq (n-1)! < n! = |S_n|$, which is a contradiction. Since $\ker\varphi$ is a nontrivial normal subgroup of S_n, $\ker\varphi = A_n$ or $\ker\varphi = S_n$ since these are the only normal subgroups of S_n for all $n \geq 5$. If $\ker\varphi = S_n$, then φ is the trivial homomorphism, so that $H = S_n$, which is a contradiction. Therefore, $\ker\varphi = A_n$, so that $A_n \subseteq H$. By maximality of A_n in S_n, then $H = A_n$. Therefore, A_n is the only proper subgroup of index $< n$ in S_n for all $n \geq 5$. ∎

Exercise 4.6.4

Prove that A_n is generated by the set of all 3-cycles for each $n \geq 3$.

Solution. Let S be the set of all 3-cycles in A_n. Observe that $\langle S\rangle \leq A_n$ since $S \subseteq A_n$. To show the other direction, let $\sigma \in A_n$. We show that two transpositions in σ can be replaced by 3-cycles. There are two cases to discuss: Let $(a\ b)$, $(c\ d)$ be two transpositions in σ.

- If $\{a,b\} \cap \{c,d\} = \varnothing$, then we can replace $(a\ b)(c\ d)$ by the product of 3-cycles $(a\ c\ d)(a\ d\ c)$.
- If $\{a,b\} \cap \{c,d\} = \{x\}$ for some x, then we can replace $(a\ b)(c\ d)$ by the 3-cycle $(a\ c\ d)$ if $x = a$ or $x = c$, and by the 3-cycle $(b\ c\ d)$ if $x = b$ or $x = d$.

∎

Exercise 4.6.5

Prove that if there exists a chain of subgroups $G_1 \leq G_2 \leq \cdots \leq G$ such that

$$G = \bigcup_{i=1}^{\infty} G_i$$

and each G_i is simple, then G is simple.

Solution. Let $N \trianglelefteq G$. We first note that $N \cap G_i \trianglelefteq G_i$ for every i as follows: for some $x \in N \cap G_i$ and $g \in G_i$, then $gxg^{-1} \in G_i$ since G_i is a subgroup of G. Moreover, $gxg^{-1} \in N$ since $N \trianglelefteq G$. It follows that $gxg^{-1} \in N \cap G_i$, so that $N \cap G_i \trianglelefteq G_i$.

By simplicity of each G_i, then $N \cap G_i$ is either 1 or G_i. If $N \cap G_i = G_i$ for some i, then $G_i \subseteq N$. In particular, we have for some G_j with $j > i$ that $G_i \subseteq G_j \subseteq N$, so that $N = G$. If $N \cap G_i = 1$ for all i, then N is the union of the trivial subgroup, so that $N = 1$. Therefore, in either case, N is either 1 or G, so that G is simple. ■

Exercise 4.6.6

Let D be the subgroup of S_Ω consisting of permutations which move only a finite number of elements of Ω (described in Exercise 4.3.17), and let A be the set of all elements $\sigma \in D$ such that σ acts as an even permutation on the (finite) set of points it moves. Prove that A is an infinite simple group. (Show that every pair of elements of D lie in a finite simple subgroup of D.)

Solution. Note that for $\sigma, \tau \in A$, then $\sigma\tau^{-1}$ is an even permutation on the set of points moved by σ and τ, so that A is a subgroup of D. Moreover, A is normal in D since for any $\sigma \in A$ and any $\tau \in D$, $\tau\sigma\tau^{-1}$ is an even permutation on the set of points moved by σ and τ, so that $\tau\sigma\tau^{-1} \in A$. Therefore, $A \trianglelefteq D$. Moreover, A is infinite since Ω is infinite, so that there are infinitely many even permutations on Ω that move only a finite number of elements of Ω.

Since Ω is infinite, for each $n \geq 5$, we can consider the subset Ω_n such that $|\Omega_n| = n$, and $\Omega_n \subseteq \Omega_{n+1}$ for all n. Define

$$B_n = \{\sigma \in A \mid M(\sigma) \subseteq \Omega_n\}$$

Consider the bijection $\varphi \colon B_n \to A_n$ defined by $\varphi(\sigma) = \sigma|_{\Omega_n}$, where $\sigma|_{\Omega_n}$ is the restriction of σ to Ω_n. It is clear that this is a homomorphism, hence $B_n \cong A_n$. Moreover, B_n is simple since A_n is simple for all $n \geq 5$. Considering the chain of subgroups $B_5 \leq B_6 \leq \cdots$, we see that

$$A = \bigcup_{n=5}^{\infty} B_n.$$

By Exercise 4.6.5, A is simple. ■

Exercise 4.6.7

Under the notation of the preceding exercise, prove that if $H \trianglelefteq S_\Omega$ and $H \neq 1$, then $A \leq H$, i.e., A is the unique (nontrivial) minimal normal subgroup of S_Ω.

Solution. Let $\sigma \in H$. Since σ moves only a finite number of elements of Ω, there exists some $\Gamma \subseteq \Omega$ with $|\Gamma| \geq 5$ such that $\sigma(\omega) = \omega$ for all $\omega \in \Omega - \Gamma$. If σ is an odd permutation, let $x, y \in \Omega - \Gamma$ be distinct (which exist since Ω is infinite) and replace σ with $\sigma(x\ y) \in H$ and Γ with $\Gamma \cup \{x, y\}$. Thus, we may assume without loss of generality that σ is an even permutation fixing every point outside Γ.

Let B be the set of elements of A which fix every point outside Γ. Since $B \cong A_{|\Gamma|}$ and $|\Gamma| \geq 5$, B is simple. Since $H \cap B \trianglelefteq B$ is nontrivial (it contains σ), simplicity of B gives $B \leq H$. In particular, H contains a 3-cycle $(alpha\ beta\ gamma)$. Now let $(a\ b\ c)$ be any 3-cycle in S_Ω. Since there exists $\tau \in S_\Omega$ with $\tau(\alpha) = a$, $\tau(\beta) = b$, $\tau(\gamma) = c$, and $H \trianglelefteq S_\Omega$, we have $\tau(alpha\ beta\ gamma)\tau^{-1} = (a\ b\ c) \in H$. Since every element of A is a product of 3-cycles and H is a subgroup, we conclude $A \leq H$. ■

Exercise 4.6.8

Under the notation of the preceding two exercises, prove that $|D| = |A| = |\Omega|$. Deduce that

$$\text{if } S_\Omega \cong S_\Delta, \text{ then } |\Omega| = |\Delta|.$$

(Use the fact that D is generated by transpositions. You may assume that countable unions and finite direct products of sets of cardinality $|\Omega|$ also have cardinality $|\Omega|$.)

Solution. We first show that $|D| = |\Omega|$. Since D is generated by transpositions, every element of D is a finite product of transpositions. For each $n \geq 1$, the set of products of exactly n transpositions has cardinality at most $|\Omega|^n = |\Omega|$, since each transposition is determined by a pair of elements of Ω. Since

$$D = \bigcup_{n=1}^{\infty} D_n$$

where D_n is the set of products of at most n transpositions, and a countable union of sets of cardinality $|\Omega|$ has cardinality $|\Omega|$, we get $|D| \leq |\Omega|$. Since the map $\omega \mapsto (omega\ alpha)$ for a fixed $\alpha \in \Omega$ is an injection $\Omega \to D$, we conclude $|D| = |\Omega|$.

We now show that $|A| = |\Omega|$. Since $A \leq D$, we have $|A| \leq |D| = |\Omega|$. Conversely, fix distinct $x, y \in \Omega$. Then the map $\omega \mapsto (omega\ x\ y)$ for $\omega \in \Omega - \{x, y\}$ is an injection $\Omega - \{x, y\} \to A$, so $|\Omega| \leq |A|$. Therefore, $|A| = |\Omega|$.

Finally, suppose $S_\Omega \cong S_\Delta$ via some isomorphism φ. By the preceding exercise, A is the unique minimal normal subgroup of S_Ω, and similarly A' is the unique minimal normal subgroup of S_Δ. Since φ maps normal subgroups to normal subgroups, $\varphi(A) = A'$, so $|A| = |A'|$, and therefore $|\Omega| = |\Delta|$. ∎

5 Direct and Semidirect Products and abelian Groups

5.1 Direct Products

Exercise 5.1.1

Show that the center of a direct product is the direct product of the centers:

$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$$

Deduce that the direct product of two groups is abelian if and only if each of the factors is abelian.

Solution. Let $G = G_1 \times G_2 \times \cdots \times G_n$. Let $z = (z_1, z_2, \ldots, z_n) \in Z(G)$. Then for any $g = (g_1, g_2, \ldots, g_n) \in G$, we have $zg = gz$, or equivalently,

$$(z_1 g_1, z_2 g_2, \ldots, z_n g_n) = (g_1 z_1, g_2 z_2, \ldots, g_n z_n)$$

This implies that $z_i g_i = g_i z_i$ for all i, so $z_i \in Z(G_i)$ for all i. Thus, $z \in Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$, and we have shown that $Z(G) \subseteq Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$.

Conversely, let $z = (z_1, z_2, \ldots, z_n) \in Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$. Then for any $g = (g_1, g_2, \ldots, g_n) \in G$, we have

$$zg = (z_1 g_1, z_2 g_2, \ldots, z_n g_n) = (g_1 z_1, g_2 z_2, \ldots, g_n z_n) = gz$$

Thus, $z \in Z(G)$, and we have shown that $Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n) \subseteq Z(G)$.

In particular, if two groups G_1 and G_2 are abelian, then $Z(G_1) = G_1$ and $Z(G_2) = G_2$, so $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2) = G_1 \times G_2$, which is abelian. Conversely, if $G_1 \times G_2$ is abelian, then $Z(G_1 \times G_2) = G_1 \times G_2$, so $Z(G_1) \times Z(G_2) = G_1 \times G_2$, which implies that $Z(G_1) = G_1$ and $Z(G_2) = G_2$, so both G_1 and G_2 are abelian. ∎

Exercise 5.1.2

Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 \times \cdots \times G_n$. Let I be a proper, nonempty subset of $\{1, \ldots, n\}$ and let $J = \{1, \ldots, n\} - I$. Define G_I to be the set of elements of G that have the identity G_j in position j for all $j \in J$.

(a) Prove that G_I is isomorphic to the direct product of the G_i for $i \in I$.
(b) Prove that G_I is a normal subgroup of G and that $G/G_I \cong G_J$.
(c) Prove that $G \cong G_I \times G_J$.

Solution.

(a) Define the map

$$\varphi : G_I \to \prod_{i \in I} G_i, \quad \varphi((g_1, g_2, \ldots, g_n)) = (g_i)_{i \in I}.$$

Since G_I and $\prod_{i \in I} G_i$ are both groups under componentwise multiplication and φ preserves multiplication componentwise, φ is a homomorphism. To see that φ is injective, suppose $\varphi((g_1, \ldots, g_n)) = (1)_{i \in I}$, the identity in $\prod_{i \in I} G_i$. Then $g_i = 1$ for all $i \in I$, and since $g_j = 1$ for all $j \in J$ by definition of G_I, we have $(g_1, \ldots, g_n) = (1, \ldots, 1)$, the identity in G_I.

To see that φ is surjective, let $(h_i)_{i \in I} \in \prod_{i \in I} G_i$. Then $(g_1, \ldots, g_n) \in G_I$ defined by $g_i = h_i$ for $i \in I$ and $g_j = 1$ for $j \in J$ satisfies $\varphi((g_1, \ldots, g_n)) = (h_i)_{i \in I}$. Hence, φ is surjective, and we conclude that φ is an isomorphism.

(b) As shown in part (a), we may identify G_J with the direct product of the G_j for $j \in J$. Define the map

$$\pi_J : G \to G_J, \quad \pi_J((g_1, g_2, \ldots, g_n)) = (g_j)_{j \in J}.$$

As in the previous part, π_J is seen to be a surjective homomorphism. The kernel of π_J consists of all elements $(g_1, \ldots, g_n) \in G$ such that $g_j = 1$ for all $j \in J$, which is precisely the definition of G_I, so $\ker \pi_J = G_I$. By the First Isomorphism Theorem, we have $G/G_I \cong \pi_J(G) = G_J$.

(c) Using part (a) to identify G_I and G_J with their respective direct products, define the map

$$\psi : G \to G_I \times G_J, \quad \psi((g_1, g_2, \ldots, g_n)) = ((g_i)_{i \in I}, (g_j)_{j \in J}).$$

It is clear that ψ is a homomorphism, and it is injective since if $\psi((g_1, \ldots, g_n)) = ((1)_{i \in I}, (1)_{j \in J})$, then $g_i = 1$ for all $i \in I$ and $g_j = 1$ for all $j \in J$, so $(g_1, \ldots, g_n) = (1, \ldots, 1)$.

It is surjective since for any $((h_i)_{i \in I}, (k_j)_{j \in J}) \in G_I \times G_J$, we have $(g_1, \ldots, g_n) \in G$ defined by $g_i = h_i$ for $i \in I$ and $g_j = k_j$ for $j \in J$ satisfies $\psi((g_1, \ldots, g_n)) = ((h_i)_{i \in I}, (k_j)_{j \in J})$. Hence, ψ is an isomorphism, and we conclude that $G \cong G_I \times G_J$. ∎

Exercise 5.1.3

Under the notation of the preceding exercise, let I and K be any disjoint nonempty subsets of $\{1, 2, \ldots, n\}$, and let G_I and G_K be the subgroups of G defined above. Prove that $xy = yx$ for all $x \in G_I$ and $y \in G_K$.

Solution. Let $x \in G_I$ and $y \in G_K$. Then x has the identity in all coordinates corresponding to $J = \{1, 2, \ldots, n\} - I$, and y has the identity in all coordinates corresponding to $L = \{1, 2, \ldots, n\} - K$. Since I and K are disjoint, we have $J \cup L = \{1, 2, \ldots, n\}$, so every coordinate of x and y is the identity in at least one of them. Thus, when we compute the product xy, we have

$$xy = (x_1y_1, x_2y_2, \ldots, x_ny_n) = (y_1x_1, y_2x_2, \ldots, y_nx_n) = yx$$

as desired. ■

Exercise 5.1.4

Let A and B be finite groups, and let p be a prime. Prove that any Sylow p-subgroup of $A \times B$ is of the form $P \times Q$, where $P \in \mathrm{Syl}_p(A)$ and $Q \in \mathrm{Syl}_p(B)$. Prove that $n_p(A \times B) = n_p(A)n_p(B)$. Generalize both of these results to a direct product of any finite number of finite groups (so that the number of Sylow p-subgroups of a direct product is the product of the numbers of Sylow p-subgroups of the factors).

Solution. Let $|A| = p^\alpha m$ and $|B| = p^\beta n$, where $p \nmid m$ and $p \nmid n$. Then $|A \times B| = |A||B| = p^{\alpha+\beta}mn$. Let $R \in \mathrm{Syl}_p(A \times B)$. Then $|R| = p^{\alpha+\beta}$, so R is a Sylow p-subgroup of $A \times B$. Let $\pi_A \colon A \times B \to A$ and $\pi_B \colon A \times B \to B$ be the projection maps. Then $\pi_A(R)$ is a p-subgroup of A, so $\pi_A(R) \subseteq P$ for some $P \in \mathrm{Syl}_p(A)$. Similarly, $\pi_B(R) \subseteq Q$ for some $Q \in \mathrm{Syl}_p(B)$. Thus, $R \subseteq P \times Q$. Since $|P \times Q| = |P||Q| = p^{\alpha+\beta}$, we must have $R = P \times Q$.

To show $n_p(A \times B) = n_p(A)n_p(B)$, we note that the Sylow p-subgroups of $A \times B$ are precisely the subgroups of the form $P \times Q$, where $P \in \mathrm{Syl}_p(A)$ and $Q \in \mathrm{Syl}_p(B)$. Since there are $n_p(A)$ choices for P and $n_p(B)$ choices for Q, we have $n_p(A \times B) = n_p(A)n_p(B)$.

Generalization to a direct product of any finite number of finite groups follows by induction on the number of factors. ■

Exercise 5.1.5

Exhibit a nonnormal subgroup of $Q_8 \times Z_4$ (note that every subgroup of each factor is normal).

Solution. Note that Q_8 is non-abelian, so we may use the idea of a diagonal subgroup from Exercise 3.1.38. In particular, let $H = \langle (i, 1) \rangle = \{(1, 0), (i, 1), (-1, 2), (-i, 3)\}$. Then H is a subgroup of $Q_8 \times Z_4$ that is isomorphic to $\langle i \rangle$. However,

$$(j, 0)(i, 1)(j, 0)^{-1} = (ji(-j), 0 + 1 + 0) = (-i, 1)$$

is not in H, so H is not normal in $Q_8 \times Z_4$. ■

Exercise 5.1.6

Show that all subgroups of $Q_8 \times E_{2^n}$ are normal.

Solution. Let $H \leq Q_8 \times E_{2^n}$. Suppose $(a, b) \in H$ and $(x, y) \in Q_8 \times E_{2^n}$. Note that $(a^{-1}, b) \in H$, since every $b \in E_{2^n}$ is its own inverse. Then

$$(x, y)(a, b)(x, y)^{-1} = (xax^{-1}, yby^{-1}) = (xax^{-1}, b),$$

where we used the fact that E_{2^n} is abelian. Since every subgroup of Q_8 is normal, we have $xax^{-1} \in \langle a \rangle$. Note that $xax^{-1} \neq a^2$, since a^2 is the unique element of order 2 in Q_8, and xax^{-1} has the same order as a. Then either $xax^{-1} = a$ or $xax^{-1} = a^{-1}$. Both (a, b) and (a^{-1}, b) are in H, so $(xax^{-1}, b) \in H$. Hence, $H \trianglelefteq Q_8 \times E_{2^n}$. ■

Exercise 5.1.7

Let $G_1, G_2, \ldots, G_n$ be groups and π be a fixed element of S_n. Prove that the map

$$\varphi_\pi \colon G_1 \times G_2 \times \cdots \times G_n \to G_{\pi^{-1}(1)} \times G_{\pi^{-1}(2)} \times \cdots \times G_{\pi^{-1}(n)}$$

defined by

$$\varphi_\pi(g_1, g_2, \ldots, g_n) = (g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \ldots, g_{\pi^{-1}(n)})$$

is an isomorphism (so that changing the order of the factors in a direct product does not change the isomorphism type).

Solution. Let $\pi \in S_n$ and let φ_π be the map defined in the problem statement. Let $g = (g_1, g_2, \ldots, g_n)$ and $h = (h_1, h_2, \ldots, h_n)$ be elements of $G_1 \times G_2 \times \cdots \times G_n$. Then

$$\begin{aligned}
\varphi_\pi(gh) &= \varphi_\pi(g_1h_1, g_2h_2, \ldots, g_nh_n) \\
&= (g_{\pi^{-1}(1)}h_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}h_{\pi^{-1}(2)}, \ldots, g_{\pi^{-1}(n)}h_{\pi^{-1}(n)}) \\
&= (g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \ldots, g_{\pi^{-1}(n)})(h_{\pi^{-1}(1)}, h_{\pi^{-1}(2)}, \ldots, h_{\pi^{-1}(n)}) \\
&= \varphi_\pi(g)\varphi_\pi(h)
\end{aligned}$$

Noting that $\pi \in S_n$ is a bijection, consider the map $\varphi_{\pi^{-1}} \colon G_{\pi^{-1}(1)} \times G_{\pi^{-1}(2)} \times \cdots \times G_{\pi^{-1}(n)} \to G_1 \times G_2 \times \cdots \times G_n$ defined by

$$\varphi_{\pi^{-1}}(k_1, k_2, \ldots, k_n) = (k_{\pi(1)}, k_{\pi(2)}, \ldots, k_{\pi(n)})$$

Then $\varphi_{\pi^{-1}}$ is a homomorphism by the same argument as above. Moreover, $\varphi_{\pi^{-1}}$ is the inverse of φ_π, since

$$\varphi_\pi(\varphi_{\pi^{-1}}(k_1, k_2, \ldots, k_n)) = \varphi_\pi(k_{\pi(1)}, k_{\pi(2)}, \ldots, k_{\pi(n)}) = (k_1, k_2, \ldots, k_n)$$

and

$$\varphi_{\pi^{-1}}(\varphi_\pi(g_1, g_2, \ldots, g_n)) = \varphi_{\pi^{-1}}(g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \ldots, g_{\pi^{-1}(n)}) = (g_1, g_2, \ldots, g_n).$$

Therefore, φ_π is an isomorphism. ∎

Exercise 5.1.8

Let $G_1 = G_2 = \cdots = G_n$ and let $G = G_1 \times \cdots \times G_n$. Under the notation of the preceding exercise show that $\varphi_\pi \in \mathrm{Aut}(G)$. Show also that the map $\pi \mapsto \varphi_\pi$ is an injective homomorphism of S_n into $\mathrm{Aut}(G)$. (In particular, $\varphi_{\pi_1} \circ \varphi_{\pi_2} = \varphi_{\pi_1\pi_2}$. It is at this point that the π^{-1}'s in the definition of φ_π are needed. The underlying reason for this is that if e_i is the n-tuple with 1 in position i and zeros elsewhere, $1 \le i \le n$, then S_n acts on $\{e_1, \ldots, e_n\}$ by $\pi \cdot e_i = e_{\pi(i)}$; this is a left group action. If the n-tuple $(g_1, \ldots, g_n)$ is represented by $g_1e_1 + \cdots + g_ne_n$, then this left group action on $\{e_1, \ldots, e_n\}$ extends to a left group action on sums by

$$\pi \cdot (g_1e_1 + g_2e_2 + \cdots + g_ne_n) = g_1e_{\pi(1)} + g_2e_{\pi(2)} + \cdots + g_ne_{\pi(n)}.$$

The coefficient of $e_{\pi(i)}$ on the right-hand side is g_i, so the coefficient of e_i is $g_{\pi^{-1}(i)}$. Thus, the right-hand side may be rewritten as $g_{\pi^{-1}(1)}e_1 + g_{\pi^{-1}(2)}e_2 + \cdots + g_{\pi^{-1}(n)}e_n$, which is precisely the sum attached to the n-tuple $(g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \ldots, g_{\pi^{-1}(n)})$. In other words, any permutation of the "position vectors" $e_1, \ldots, e_n$ (which fixes their coefficients) is the same as the inverse permutation on the coefficients (fixing the e_i's). If one uses π's in place of π^{-1}'s in the definition of φ_π then the map $\pi \mapsto \varphi_\pi$ is not necessarily a homomorphism–it corresponds to a *right* group action.)

Solution. Note that $\varphi_\pi \in \mathrm{Aut}(G)$ since φ_π is an isomorphism from G to itself. Let $\pi_1, \pi_2 \in S_n$. Then

$$\begin{aligned}
\varphi_{\pi_1}(\varphi_{\pi_2}(g_1, g_2, \ldots, g_n)) &= \varphi_{\pi_1}(g_{\pi_2^{-1}(1)}, g_{\pi_2^{-1}(2)}, \ldots, g_{\pi_2^{-1}(n)}) \\
&= (g_{\pi_2^{-1}(\pi_1^{-1}(1))}, g_{\pi_2^{-1}(\pi_1^{-1}(2))}, \ldots, g_{\pi_2^{-1}(\pi_1^{-1}(n))}) \\
&= (g_{(\pi_1\pi_2)^{-1}(1)}, g_{(\pi_1\pi_2)^{-1}(2)}, \ldots, g_{(\pi_1\pi_2)^{-1}(n)}) \\
&= \varphi_{\pi_1\pi_2}(g_1, g_2, \ldots, g_n)
\end{aligned}$$

Therefore, the map $\pi \mapsto \varphi_\pi$ is a homomorphism. To see that it is injective, note that if φ_π is the identity automorphism, then for all i, $g_{\pi^{-1}(i)} = g_i$ for all $g_i \in G_i$, which implies π is the identity permutation. Hence, the map is injective. ∎

Exercise 5.1.9

Let G_i be a field F for all i and use the preceding exercise to show that the set of $n \times n$ matrices with one 1 in each row and each column is a subgroup of $\mathrm{GL}_n(F)$ isomorphic to S_n (these matrices are the *permutation matrices* since they simply permute the standard basis $e_1, \ldots, e_n$ (as above) of the n-dimensional vector space $F \times F \times \cdots \times F$).

Solution. Let $G = F \times F \times \cdots \times F$ (n times) and let $\pi \in S_n$. Then φ_π is an automorphism of G that permutes the standard basis vectors $e_1, e_2, \ldots, e_n$. In particular, $\varphi_\pi(e_i) = e_{\pi(i)}$ for all i. Thus, the matrix representation of φ_π with respect to the standard basis is a permutation matrix. Since the map $\pi \mapsto \varphi_\pi$ is an injective homomorphism from S_n to $\mathrm{Aut}(G)$, the set of permutation matrices forms a subgroup of $\mathrm{GL}_n(F)$ that is isomorphic to S_n. ■

Exercise 5.1.10

Let p be a prime. Let A and B be two cyclic groups of order p with generators x and y respectively. Set $E = A \times B$ so that E is the elementary abelian group of order p^2: E_{p^2} Prove that the distinct subgroups of E of order p are

$$\langle x \rangle, \quad \langle xy \rangle, \quad \langle xy^2 \rangle, \quad \ldots, \quad \langle xy^{p-1} \rangle, \quad \langle y \rangle$$

(note that there are $p + 1$ of them).

Solution. Note that any proper, nontrivial subgroup of E must have order p, and every element of E has order p. The text shows that there are $p + 1$ subgroups of E of order p, so it suffices to show that the subgroups listed in the problem statement are distinct. Note that $\langle x \rangle$ and $\langle y \rangle$ are distinct since they have different generators. Moreover, $\langle xy^i \rangle$ is distinct from $\langle x \rangle$ and $\langle y \rangle$ for all i, since xy^i is not a power of x or y (as can be seen because $\langle x \rangle \cap \langle y \rangle$ is trivial). Finally, $\langle xy^i \rangle$ is distinct from $\langle xy^j \rangle$ for $i \neq j$, since if $\langle xy^i \rangle = \langle xy^j \rangle$, xy^i is a power of xy^j, which implies y^{i-j} is a power of x, which is impossible since $\langle x \rangle \cap \langle y \rangle$ is trivial. Thus, all the subgroups listed in the problem statement are distinct. ■

Exercise 5.1.11

Let p be a prime, and let $n \in \mathbb{Z}^+$. Find a formula for the number of subgroups of order p in the elementary abelian group E_{p^n}.

Solution. Every element of E_{p^n} has order p, so every subgroup of order p is generated by a single nonidentity element. Since there are $p^n - 1$ nonidentity elements in E_{p^n}, and each subgroup of order p has $p - 1$ generators (the nonidentity elements of the subgroup), the number of subgroups of order p in E_{p^n} is

$$\frac{p^n - 1}{p - 1} = 1 + p + p^2 + \cdots + p^{n-1}$$

as desired. ■

Exercise 5.1.12

Let A and B be groups. Assume $Z(A)$ contains a subgroup Z_1 and $Z(B)$ contains a subgroup Z_2 with $Z_1 \cong Z_2$. Let this isomorphism be given by the map $x_i \mapsto y_i$ for all $x_i \in Z_1$. A ***central product*** of A and B is a quotient

$$(A \times B)/Z \quad \text{where} \quad Z = \{(x_i, y_i^{-1}) \mid x_i \in Z_1\}$$

and is denoted by $A * B$–it is not unique since it depends on Z_1, Z_2 and the isomorphism between them. (Think of $A * B$ as the direct product of A and B "collapsed" by identifying each element $x_i \in Z_1$ with its corresponding element $y_i \in Z_2$.)

(a) Prove that the images of A and B in the quotient group $A * B$ are isomorphic to A and B, respectively, and that these images intersect in a central subgroup isomorphic to Z_1. Find $|A * B|$.

(b) Let $Z_4 = \langle x \rangle$. Let $D_8 = \langle r, s \rangle$ and $Q_8 = \langle i, j \rangle$ be given by their usual generators and relations. Let $Z_4 * D_8$ be the central product of Z_4 and D_8 which identifies x^2 and r^2 (i.e., $Z_1 = \langle x^2 \rangle$, $Z_2 = \langle r^2 \rangle$ and the isomorphism is $x^2 \mapsto r^2$) and let $Z_4 * Q_8$ be the central product of Z_4 and Q_8 which identifies x^2 and -1. Prove that $Z_4 * D_8 \cong Z_4 * Q_8$.

Solution.

(a) Consider the maps $\pi_A : A \to A * B$ and $\pi_B : B \to A * B$ defined by $\pi_A(a) = (a, 1)Z$ and $\pi_B(b) = (1, b)Z$. It is clear that π_A and π_B are homomorphisms. Moreover, $\ker \pi_A$ consists of the elements $a \in A$ such that $(a, 1) \in Z$. Then $y_i = 1$, and since $x_i \mapsto y_i$ is an isomorphism, we have $x_i = 1$, so $a = 1$. Thus, $\ker \pi_A$ is trivial, and π_A is injective. Similarly, $\ker \pi_B$ is trivial, and π_B is injective. Therefore, the images of A and B in $A * B$ are isomorphic to A and B, respectively. Moreover, the images of A and B in $A * B$ intersect in the subgroup $\{(x_i, 1)Z \mid x_i \in Z_1\}$, which is isomorphic to Z_1. Finally, since Z has $|Z_1|$ elements, we have

$$|A * B| = \frac{|A||B|}{|Z_1|}.$$

(b) Denote Z_D and Z_Q as the subgroups of $Z_4 \times D_8$ and $Z_4 \times Q_8$ that are identified in the central products. Put x and y as the generators of the Z_4 factors in $Z_4 * D_8$ and $Z_4 * Q_8$, respectively. Put r and s as the generators of D_8 and i and j as the generators of Q_8. Let $\mathbf{x} = (x, 1)Z_D$ be the coset of Z_D in $Z_4 * D_8$, and denote all other elements of $Z_4 * D_8$ and $Z_4 * Q_8$ similarly.

A preliminary observation is that we need an element in $Z_4 * Q_8$ that corresponds to $\mathbf{s} \in Z_4 * D_8$. We claim that the element $\mathbf{z} = \mathbf{j}\mathbf{y}^{-1}$ has order 2 and conjugates $\mathbf{i}$ to $\mathbf{i}^{-1}$. Note that $|\mathbf{z}| \neq 1$, for otherwise $\mathbf{j} = \mathbf{y}$. This would imply $\mathbf{j} \in \pi_{Z_4}(y) = \langle \mathbf{y} \rangle$, but $\mathbf{j}$ does not commute with $\mathbf{i}$, so $\mathbf{j} \notin \langle \mathbf{y} \rangle$. Then

$$\mathbf{z}^2 = \mathbf{j}\mathbf{y}^{-1}\mathbf{j}\mathbf{y}^{-1} = \mathbf{j}^2\mathbf{y}^{-2} = \mathbf{1},$$

so $\mathbf{z}$ has order 2. Moreover, we have

$$\mathbf{z}\mathbf{i}\mathbf{z}^{-1} = \mathbf{j}\mathbf{y}^{-1}\mathbf{i}\mathbf{y}\mathbf{j}^{-1} = \mathbf{j}\mathbf{i}\mathbf{j}^{-1} = \mathbf{i}^{-1}.$$

Then $\mathbf{z}$ has the same properties as $\mathbf{s}$, so we may define a map $\varphi : Z_4 * D_8 \to Z_4 * Q_8$ by

$$\varphi(\mathbf{x}^\alpha \mathbf{r}^\beta \mathbf{s}^\gamma) = \mathbf{y}^\alpha \mathbf{i}^\beta \mathbf{z}^\gamma.$$

We claim that φ is well defined. To see this, note that the relations in $Z_4 * D_8$ are satisfied in $Z_4 * Q_8$ under the map φ. In particular, we have in $Z_4 * D_8$ that $\mathbf{r}^4 = \mathbf{s}^2 = \mathbf{1}$, $\mathbf{x}^2 = \mathbf{r}^2$, and $\mathbf{srs} = \mathbf{r}^{-1}$. Then in $Z_4 * Q_8$, we have

$$\varphi(\mathbf{r}^4) = \mathbf{i}^4 = \mathbf{1}, \quad \varphi(\mathbf{s}^2) = \mathbf{z}^2 = \mathbf{1}, \quad \varphi(\mathbf{x}^2) = \mathbf{y}^2 = \mathbf{i}^2 = \varphi(\mathbf{r}^2), \quad \text{and} \quad \varphi(\mathbf{srs}) = \mathbf{ziz} = \mathbf{i}^{-1}.$$

Additionally, $\mathbf{y}$ is central in $Z_4 * Q_8$, which follows from the fact that Z_4 is central in $Z_4 * D_8$ and φ preserves the relations. Thus, φ is a homomorphism.

To see that φ is surjective, note that any element of $Z_4 * Q_8$ can be written as $\mathbf{y}^\alpha \mathbf{i}^\beta \mathbf{z}^\gamma$, which is the image of $\mathbf{x}^\alpha \mathbf{r}^\beta \mathbf{s}^\gamma$ under φ. Since Z_4 and Q_8 are generated by $\mathbf{y}$ and $\mathbf{i}, \mathbf{j}$ respectively, putting $\mathbf{j} = \mathbf{zy}$ shows that $\mathbf{y}, \mathbf{i}, \mathbf{z}$ generate $Z_4 * Q_8$. From part (a), we know that $|Z_4 * D_8| = |Z_4||D_8|/|Z_1| = 16$ and $|Z_4 * Q_8| = |Z_4||Q_8|/|Z_1| = 16$, so φ is a surjective homomorphism between two groups of the same order, and hence it is an isomorphism. ■

Exercise 5.1.13

Give presentations for the groups $Z_4 * D_8$ and $Z_4 * Q_8$ constructed in the preceding exercise.

Solution. To construct the presentations, we note that $\mathbf{x}$ should satisfy the relations of Z_4, $\mathbf{r}$ and $\mathbf{s}$ should satisfy the relations of D_8, and $\mathbf{i}$ and $\mathbf{z}$ should satisfy the relations of Q_8. Moreover, we have the relations $\mathbf{x}^2 = \mathbf{r}^2$ in $Z_4 * D_8$, since $\mathbf{x}^2\mathbf{r}^{-2} = \mathbf{1}$. Lastly, $\mathbf{x}$ is central in that $\mathbf{xr} = \mathbf{rx}$ and $\mathbf{xs} = \mathbf{sx}$ in $Z_4 * D_8$. Then a presentation for $Z_4 * D_8$ is

$$\langle \mathbf{x}, \mathbf{r}, \mathbf{s} \mid \mathbf{r}^4 = \mathbf{s}^2 = \mathbf{1}, \mathbf{x}^2 = \mathbf{r}^2, \mathbf{srs} = \mathbf{r}^{-1}, \mathbf{xr} = \mathbf{rx}, \mathbf{xs} = \mathbf{sx} \rangle.$$

To find a presentation for $Z_4 * Q_8$, we may use the isomorphism φ from the preceding exercise to rewrite the presentation for $Z_4 * D_8$ in terms of $\mathbf{y}, \mathbf{i}, \mathbf{z}$. In particular, we have $\mathbf{y}^2 = \mathbf{i}^2\mathbf{z}^2$, $\mathbf{z}^2 = \mathbf{1}$, and $\mathbf{yi} = \mathbf{iyz}$. Thus, a presentation for $Z_4 * Q_8$ is

$$\langle \mathbf{y}, \mathbf{i}, \mathbf{z} \mid \mathbf{i}^4 = \mathbf{z}^2 = \mathbf{1}, \mathbf{y}^2 = \mathbf{i}^2, \mathbf{ziz} = \mathbf{i}^{-1}, \mathbf{yi} = \mathbf{iy}, \mathbf{yz} = \mathbf{zy} \rangle.$$ ■

Exercise 5.1.14

Let $G = A_1 \times A_2 \times \cdots \times A_n$, and for each i, let B_i be a normal subgroup of A_i. Prove that $B_1 \times B_2 \times \cdots \times B_n \trianglelefteq G$, and that

$$(A_1 \times A_2 \times \cdots \times A_n)/(B_1 \times B_2 \times \cdots \times B_n) \cong (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n).$$

Solution. Let $G = A_1 \times A_2 \times \cdots \times A_n$ and let $B_i \trianglelefteq A_i$ for all i. Let $H = B_1 \times B_2 \times \cdots \times B_n$. It is clear that H is a subgroup of G. Moreover, since each B_i is normal in A_i, we have that for any $g = (a_1, a_2, \ldots, a_n) \in G$ and any $h = (b_1, b_2, \ldots, b_n) \in H$, we have

$$ghg^{-1} = (a_1 b_1 a_1^{-1}, a_2 b_2 a_2^{-1}, \ldots, a_n b_n a_n^{-1}) \in H$$

since $a_i b_i a_i^{-1} \in B_i$ for all i. Thus, H is normal in G.

Consider the map $\varphi : G \to (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n)$ defined by

$$\varphi((a_1, a_2, \ldots, a_n)) = (a_1 B_1, a_2 B_2, \ldots, a_n B_n).$$

It is clear that φ is a homomorphism. Moreover, φ is surjective since for any $(a_1 B_1, a_2 B_2, \ldots, a_n B_n)$, we have $\varphi((a_1, a_2, \ldots, a_n)) = (a_1 B_1, a_2 B_2, \ldots, a_n B_n)$. Finally, the kernel of φ is the set of all $(a_1, a_2, \ldots, a_n)$ such that $a_i \in B_i$ for all i, which is exactly H. Thus, by the First Isomorphism Theorem, we have

$$G/H \cong (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n)$$

as desired. ■

Exercise 5.1.15

Let I be any nonempty index set and let $(G_i, \star_i)$ be a group for each $i \in I$. The *direct product* of the groups G_i, $i \in I$ is the set $G = \prod_{i \in I} G_i$ (the Cartesian product of the G_i's) with a binary operation defined as follows: if $\prod a_i$ and $\prod b_i$ are elements of G, then their product in G is given by

$$\left(\prod_{i \in I} a_i\right)\left(\prod_{i \in I} b_i\right) = \prod_{i \in I} (a_i \star_i b_i)$$

(i.e., the group operation in the direct product is defined componentwise).

(a) Show that this binary operation is well defined and associative.

(b) Show that the element $\prod 1_i$ satisfies the axiom for the identity of G, where 1_i is the identity of G_i for all i.

(c) Show that the element $\prod a_i^{-1}$ is the inverse of $\prod a_i$, where the inverse of each component element a_i is taken in the group G_i.

Conclude that the direct product is a group. (Note that if $I = \{1, 2, \ldots, n\}$, this definition of the direct product is the same as the n-tuple definition in the text.)

Solution.

(a) To show that the operation is well defined, let $\prod \alpha_i = \prod a_i$ and $\prod \beta_i = \prod b_i$. Then $\alpha_i = a_i$ and $\beta_i = b_i$ for all i, so

$$\left(\prod_{i \in I} \alpha_i\right)\left(\prod_{i \in I} \beta_i\right) = \prod_{i \in I} (\alpha_i \star_i \beta_i) = \prod_{i \in I} (a_i \star_i b_i)$$

as desired. To show associativity, let $\prod a_i$, $\prod b_i$, and $\prod c_i$ be elements of G. Then

$$\begin{aligned}
\left(\prod_{i \in I} a_i\right)\left(\left(\prod_{i \in I} b_i\right)\left(\prod_{i \in I} c_i\right)\right) &= \left(\prod_{i \in I} a_i\right)\left(\prod_{i \in I} (b_i \star_i c_i)\right) \\
&= \prod_{i \in I} (a_i \star_i (b_i \star_i c_i)) \\
&= \prod_{i \in I} ((a_i \star_i b_i) \star_i c_i) \\
&= \left(\prod_{i \in I} (a_i \star_i b_i)\right)\left(\prod_{i \in I} c_i\right) \\
&= \left(\left(\prod_{i \in I} a_i\right)\left(\prod_{i \in I} b_i\right)\right)\left(\prod_{i \in I} c_i\right)
\end{aligned}$$

as desired.

(b) Let $\prod a_i$ be an element of G. Then

$$\left(\prod_{i\in I} 1_i\right)\left(\prod_{i\in I} a_i\right) = \prod_{i\in I}(1_i \star_i a_i) = \prod_{i\in I} a_i$$

and

$$\left(\prod_{i\in I} a_i\right)\left(\prod_{i\in I} 1_i\right) = \prod_{i\in I}(a_i \star_i 1_i) = \prod_{i\in I} a_i.$$

Thus, $\prod 1_i$ is the identity element of G.

(c) Let $\prod a_i$ be an element of G. Then

$$\left(\prod_{i\in I} a_i\right)\left(\prod_{i\in I} a_i^{-1}\right) = \prod_{i\in I}(a_i \star_i a_i^{-1}) = \prod_{i\in I} 1_i$$

and

$$\left(\prod_{i\in I} a_i^{-1}\right)\left(\prod_{i\in I} a_i\right) = \prod_{i\in I}(a_i^{-1} \star_i a_i) = \prod_{i\in I} 1_i.$$

Thus, $\prod a_i^{-1}$ is the inverse of $\prod a_i$. We conclude that G is a group with inverse and identity as described above. ■

Exercise 5.1.16

State and prove the generalization of Proposition 2 to arbitrary direct products.

Solution. Proposition 2 stated for direct arbitrary groups is as follows: if $G = \prod_{i\in I} G_i$ is a direct product of groups, then

(1) Fix each i with j-th coordinate where $j \neq i$ is the identity element of G_j for $1 \leq j \leq n$. Then

$$\widehat{G}_i = \{(1, 1, \ldots, 1, g_i, 1, \ldots) \mid g_i \in G_i\}$$

is a normal subgroup of G that is isomorphic to G_i, or that

$$G/\widehat{G}_i \cong \prod_{j\neq i} G_j.$$

(2) For fixed i, define $\pi_i \colon G \to G_i$ by $\pi_i((g_j)_{j\in I}) = g_i$. Then π_i is a surjective homomorphism with kernel $\widehat{G}_i$, so $G/\widehat{G}_i \cong G_i$.

(3) If $x \in G_i$ and $y \in G_j$ for $i \neq j$, then x and y commute in G.

The proof is similar to the proof of Proposition 2 in the text.

(1) It is clear that $\widehat{G}_i$ is a subgroup of G. Moreover, for any $\prod_{j\in I} g_j \in G$ and any $h = \prod_{j\neq i} 1_j h_i \in \widehat{G}_i$, we have

$$\left(\prod_{j\in I} g_j\right) h \left(\prod_{j\in I} g_j\right)^{-1} = \prod_{j\neq i} 1_j (g_i h_i g_i^{-1}) \in \widehat{G}_i$$

since $g_i h_i g_i^{-1} \in G_i$. Thus, $\widehat{G}_i$ is normal in G. Consider the map $\varphi \colon G_i \to \widehat{G}_i$ defined by $\varphi(g_i) = \prod_{j\neq i} 1_j g_i$. It is clear that φ is a homomorphism. Moreover, if $\varphi(g_i) = \prod_{j\neq i} 1_j g_i = \prod_{j\neq i} 1_j$, then g_i is the identity element of G_i, so φ is injective. Finally, for any $\prod_{j\neq i} 1_j h_i \in \widehat{G}_i$, we have $\varphi(h_i) = \prod_{j\neq i} 1_j h_i$, so φ is surjective. Thus, $\widehat{G}_i$ is isomorphic to G_i.

Consider the map

$$\psi \colon G \to \prod_{j\neq i} G_j \text{ defined by } \psi\left(\prod_{j\in I} g_j\right) = \prod_{j\neq i} g_j.$$

It is clear that ψ is a homomorphism. Moreover, the kernel of ψ is $\widehat{G}_i$, so by the First Isomorphism Theorem, we have

$$G/\widehat{G}_i \cong \prod_{j\neq i} G_j.$$

(2) For fixed i, it is clear that π_i is a homomorphism. Moreover, π_i is surjective since for any $g_i \in G_i$, we have $\pi_i(\prod_{j\in I} 1_j g_i) = g_i$. Finally, the kernel of π_i is $\widehat{G_i}$, so by the First Isomorphism Theorem, we have

$$G/\widehat{G_i} \cong G_i.$$

(3) Let $x = \prod_{j\neq i} 1_j x_i$ and $y = \prod_{j\neq k} 1_j y_k$ for some $i \neq k$. Then

$$xy = \prod_{j\neq i,k} 1_j x_i y_k = \prod_{j\neq i,k} 1_j y_k x_i = yx$$

as desired.

■

Exercise 5.1.17

Let I be any nonempty index set and let G_i be a group for each $i \in I$. The *restricted direct product* or *direct sum* of the groups G_i is the set of elements of the direct product which are the identity in all but finitely many components, that is, the set of all elements $\prod a_i \in \prod_{i\in I} G_i$ such that $a_i = 1_i$ for all but a finite number of $i \in I$.

(a) Prove that the restricted direct product is a subgroup of the direct product.
(b) Prove that the restricted direct product is normal in the direct product.
(c) Let $I = \mathbb{Z}^+$ and let p_i be the ith integer prime. Show that if $G_i = \mathbb{Z}/p_i\mathbb{Z}$ for all $i \in \mathbb{Z}^+$, then every element of the restricted direct product of the G_i's has finite order but $\prod_{i\in\mathbb{Z}^+} G_i$ has elements of infinite order. Show that in this example the restricted direct product is the torsion subgroup of the direct product (cf. Exercise 2.1.16).

Solution.

(a) Let $G = \prod_{i\in I} G_i$ and let H be the restricted direct product of the G_i's. It is clear that H is a subset of G. Moreover, if $\prod a_i$ and $\prod b_i$ are elements of H, then there are only finitely many i such that $a_i \neq 1_i$ and only finitely many i such that $b_i \neq 1_i$. Thus, there are only finitely many i such that $a_i b_i \neq 1_i$, so $\prod a_i \prod b_i = \prod(a_i b_i)$ is an element of H. Finally, if $\prod a_i$ is an element of H, then there are only finitely many i such that $a_i \neq 1_i$, so there are only finitely many i such that $a_i^{-1} \neq 1_i$, so $\prod a_i^{-1}$ is an element of H. Thus, $H \leq G$.

(b) Let $G = \prod_{i\in I} G_i$ and let H be the restricted direct product of the G_i's. Let $\prod a_i$ be an element of G and let $\prod b_i$ be an element of H. Then there are only finitely many i such that $b_i \neq 1_i$, so there are only finitely many i such that $a_i b_i a_i^{-1} \neq 1_i$, so $\prod a_i \prod b_i \prod a_i^{-1}$ is an element of H. Thus, $H \trianglelefteq G$.

(c) Let $G = \prod_{i\in\mathbb{Z}^+} G_i$ where $G_i = \mathbb{Z}/p_i\mathbb{Z}$ for all i. Let H be the restricted direct product of the G_i's. If $\prod a_i$ is an element of H, then there are only finitely many i such that $a_i \neq 1_i$, so there are only finitely many i such that a_i has order greater than 1, so $\prod a_i$ has finite order. On the other hand, if $\prod a_i$ is an element of G such that a_i is a generator of G_i for all i, then $\prod a_i$ has infinite order since for any positive integer n, we have $(\prod a_i)^n = \prod a_i^n$, and there are infinitely many i such that $a_i^n \neq 1_i$.

To show $H = \mathrm{Tor}(G)$, we note that $H \subseteq \mathrm{Tor}(G)$ since every element of H has finite order. Conversely, if $\prod a_i$ is an element of $\mathrm{Tor}(G)$, then there is some positive integer n such that $(\prod a_i)^n = \prod a_i^n = \prod 1_i$, so $a_i^n = 1_i$ for all i. Since G_i is cyclic of prime order, this implies that a_i is either the identity or a generator of G_i. If there are infinitely many i such that a_i is a generator of G_i, then $\prod a_i$ has infinite order, which is a contradiction. Thus, there are only finitely many i such that a_i is a generator of G_i, so there are only finitely many i such that $a_i \neq 1_i$, so $\prod a_i$ is an element of H. Therefore, $\mathrm{Tor}(G) \subseteq H$, and we conclude that $\mathrm{Tor}(G) = H$. ■

Exercise 5.1.18

In each of (a) to (e) give an example of a group with the specified properties:

(a) an infinite group in which every element has order 1 or 2
(b) an infinite group in which every element has finite order but for each positive integer n there is an element of order n
(c) a group with an element of infinite order and an element of order 2
(d) a group G such that every finite group is isomorphic to some subgroup of G
(e) a nontrivial group G such that $G \cong G \times G$.

Solution.

(a) Consider the infinite direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$. Every element of this group is a tuple of 0's and 1's, and the order of each element is either 1 (if the tuple is the identity) or 2 (if the tuple has at least one 1).

(b) Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \cdots$. Every element of G has finite order since it is a tuple of elements from finite cyclic groups. Moreover, for each positive integer n, the element that is the identity in all components except the n-th component, which is a generator of $\mathbb{Z}/n\mathbb{Z}$, has order n.

(c) Consider the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. The element $(1, 0)$ has order 2, and the element $(0, 1)$ has infinite order.

(d) By Cayley's Theorem, every finite group is isomorphic to a subgroup of some symmetric group S_n. We may then consider the group $G = S_1 \times S_2 \times S_3 \times \cdots$. For any finite group H, there is some n such that H is isomorphic to a subgroup of S_n, so H is isomorphic to a subgroup of G.

(e) Let $G = \mathbb{Z} \times \mathbb{Z} \times \cdots$. Consider the map $\varphi \colon G \to G \times G$ defined by

$$\varphi((a_1, a_2, a_3, \ldots)) = ((a_1, a_3, a_5, \ldots), (a_2, a_4, a_6, \ldots)).$$

It is clear that φ is a homomorphism. Moreover, if $\varphi((a_1, a_2, a_3, \ldots)) = ((0, 0, 0, \ldots), (0, 0, 0, \ldots))$, then $a_i = 0$ for all i, so φ is injective. Finally, let $((b_1, b_2, b_3, \ldots), (c_1, c_2, c_3, \ldots))$ be an element of $G \times G$. Then

$$\varphi((b_1, c_1, b_2, c_2, b_3, c_3, \ldots)) = ((b_1, b_2, b_3, \ldots), (c_1, c_2, c_3, \ldots)),$$

so φ is surjective. Thus, φ is an isomorphism and $G \cong G \times G$. ■

5.2 The Fundamental Theorem of Finitely Generated abelian Groups

Exercise 5.2.1

In each parts (a) to (e), give the number of nonisomorphic abelian groups of the specified order–do not list the groups:
(a) order 100, (b) order 576, (c) order 1155, (d) order 42875, (e) order 2704.

Solution.

(a) $100 = 2^2 \cdot 5^2$; 2 partitions of 2, hence $2 \cdot 2 = 4$ nonisomorphic abelian groups of order 100.
(b) $576 = 2^6 \cdot 3^2$; 11 partitions of 6, hence $11 \cdot 2 = 22$ nonisomorphic abelian groups of order 576.
(c) $1155 = 3 \cdot 5 \cdot 7 \cdot 11$. Only one abelian group of order 1155.
(d) $42875 = 5^3 \cdot 7^3$; 3 partitions of 3, hence $3 \cdot 3 = 9$ nonisomorphic abelian groups of order 42875.
(e) $2704 = 2^4 \cdot 13^2$; 5 partitions of 4, hence $5 \cdot 2 = 10$ nonisomorphic abelian groups of order 2704. ■

Exercise 5.2.2

In each of parts (a) to (e), give the lists of invariant factors for all abelian groups of the specified order:
(a) group 270, (b) order 9801, (c) order 320, (d) order 105, (e) order 44100.

Solution.

(a) $270 = 2 \cdot 3^3 \cdot 5$. The invariant factors are $\{270\}, \{90, 3\}, \{30, 3, 3\}$.
(b) $9801 = 3^4 \cdot 11^2$. The invariant factors are $\{9801\}, \{891, 11\}, \{3267, 3\}, \{297, 33\}, \{1089, 9\}, \{99, 99\}, \{1089, 3, 3\}, \{99, 33, 3\}, \{363, 3, 3, 3\}, \{33, 33, 3, 3\}$.
(c) $320 = 2^6 \cdot 5$. The invariant factors are $\{320\}, \{160, 2\}, \{80, 4\}, \{80, 2, 2\}, \{40, 8\}, \{40, 4, 2\}, \{40, 2, 2, 2\}, \{20, 4, 4\}, \{20, 4, 2, 2\}, \{20, 2, 2, 2, 2\}, \{10, 2, 2, 2, 2, 2\}$.
(d) $105 = 3 \cdot 5 \cdot 7$. The invariant factors are $\{105\}$.
(e) $44100 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2$. The invariant factors are $\{44100\}, \{22050, 2\}, \{14700, 3\}, \{8820, 5\}, \{6300, 7\}, \{4410, 10\}, \{3150, 14\}, \{2205, 15\}, \{1800, 21\}, \{1260, 35\}, \{1470, 30\}, \{1050, 42\}, \{630, 70\}, \{420, 105\}, \{210, 210\}$. ■

Exercise 5.2.3

In each of the parts (a) to (e), give the lists of elementary divisors for all abelian groups of the specified order, and then match each list with the corresponding list of invariant factors found in the preceding exercise:
(a) group 270, (b) order 9801, (c) order 320, (d) order 105, (e) order 44100.

Solution.

(a) $\{2, 27, 5\}, \{2, 9, 5, 3\}, \{2, 3, 5, 3, 3\}$.
(b) $\{81, 121\}, \{81, 11, 11\}, \{27, 121, 3\}, \{27, 11, 3, 11\}, \{9, 121, 9\}, \{9, 11, 9, 11\}, \{9, 121, 3, 3\}, \{9, 11, 3, 11, 3\}, \{3, 121, 3, 3, 3\}, \{3, 11, 3, 11, 3, 3\}$.
(c) $\{64, 5\}, \{32, 5, 2\}, \{16, 5, 4\}, \{16, 5, 2, 2\}, \{8, 5, 8\}, \{8, 5, 4, 2\}, \{8, 5, 2, 2, 2\}, \{4, 5, 4, 4\}, \{4, 5, 4, 2, 2\}, \{4, 5, 2, 2, 2, 2\}, \{2, 5, 2, 2, 2, 2, 2\}$.
(d) $\{3, 5, 7\}$.
(e) $\{4, 9, 25, 49\}, \{2, 9, 25, 49, 2\}, \{4, 3, 25, 49, 3\}, \{4, 9, 5, 49, 5\}, \{4, 9, 25, 7, 7\}, \{2, 3, 25, 49, 2, 3\}, \{2, 9, 5, 49, 2, 5\}, \{2, 9, 25, 7, 2, 7\}, \{4, 3, 5, 49, 3, 5\}, \{2, 3, 25, 49, 2, 3\}, \{2, 9, 5, 49, 2, 7\}, \{4, 3, 25, 7, 3, 7\}, \{2, 3, 5, 49, 2, 3, 5\}, \{2, 3, 25, 7, 2, 3, 7\}, \{4, 3, 5, 7, 3, 5, 7\}, \{2, 3, 5, 7, 2, 3, 5, 7\}$. ■

Exercise 5.2.4

In each of parts (a) to (d), determine which pairs of abelian groups listed are isomorphic (here the expression $\{a_1, a_2, \ldots, a_k\}$ denotes the abelian group $Z_{a_1} \times Z_{a_2} \times \cdots \times Z_{a_k}$).
(a) $\{4, 9\}$, $\{6, 6\}$, $\{8, 3\}$, $\{9, 4\}$, $\{6, 4\}$, $\{64\}$.
(b) $\{2^2, 2 \cdot 3^2\}$, $\{2^2 \cdot 3, 2 \cdot 3\}$, $\{2^3 \cdot 3^2\}$, $\{2^2 \cdot 3^2, 2\}$.
(c) $\{5^2 \cdot 7^2, 3^2 \cdot 5 \cdot 7\}$, $\{3^2 \cdot 5^2 \cdot 7, 5 \cdot 7^2\}$, $\{3 \cdot 5^2, 7^2, 3 \cdot 5 \cdot 7\}$, $\{5^2 \cdot 7, 3^2 \cdot 5, 7^2\}$.
(d) $\{2^2 \cdot 5 \cdot 7, 2^3 \cdot 5^3, 2 \cdot 5^2\}$, $\{2^3 \cdot 5^3 \cdot 7, 2^3 \cdot 5^3\}$, $\{2^2, 2 \cdot 7, 2^3, 5^3, 5^3\}$, $\{2 \cdot 5^3, 2^2 \cdot 5^3, 2^3, 7\}$.

Solution.

(a) $\{4, 9\}$ and $\{9, 4\}$ have the same elementary divisors, so they are isomorphic. In order, the other four groups have elementary divisors $\{3, 2, 3, 2\}$, $\{8, 3\}$, $\{3, 2, 4\}$, and $\{64\}$, so they are not isomorphic to each other or to $\{4, 9\}$.
(b) $\{2^2, 2 \cdot 3^2\}$ and $\{2^2 \cdot 3^2, 2\}$ have the same elementary divisors, so they are isomorphic. In order, the other two groups have elementary divisors $\{2^2 \cdot 3, 2 \cdot 3\}$ and $\{2^3 \cdot 3^2\}$, so they are not isomorphic to each other or to $\{2^2, 2 \cdot 3^2\}$.
(c) The first, second, and fourth groups have the same elementary divisors $\{5^2, 7^2, 3^2, 5, 7\}$, so they are isomorphic. The third group has elementary divisors $\{3, 5^2, 7^2, 3, 5, 7\}$, so it is not isomorphic to the other three groups.
(d) The third and fourth groups have the elementary divisors $\{2, 125, 4, 125, 8, 7\}$, so they are isomorphic. ■

Exercise 5.2.5

Let G be a finite abelian group of type $(n_1, n_2, \ldots, n_t)$. Prove that G contains an element of order m if and only if $m \mid n_1$. Deduce that G is of exponent n_1.

Solution.
$\boxed{\Rightarrow}$ Let $g = (g_1, g_2, \ldots, g_t) \in G$ have order m. Then $m = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_t|)$, so $|g_i| \mid m$ for all i. Since G is of type $(n_1, n_2, \ldots, n_t)$, we have $|g_i| \mid n_i$ for all i, so m divides $\operatorname{lcm}(n_1, n_2, \ldots, n_t) = n_1$.
$\boxed{\Leftarrow}$ If $m \mid n_1$, then there exists an element of order m in the cyclic subgroup of order n_1.

Since G contains an element of order n_1, the exponent of G is at least n_1. On the other hand, if $g \in G$, then $|g| \mid n_1$, so the exponent of G divides n_1. Thus, the exponent of G is exactly n_1. ■

Exercise 5.2.6

Prove that any finite group has a finite exponent. Give an example of an infinite group with finite exponent. Does a finite group of exponent m always contain an element of order m?

Solution. Let G be a finite group. Then there are only finitely many elements of G, so there are only finitely many orders of elements in G. Let m be the least common multiple of the orders of all elements of G. Then for any $g \in G$, we have $g^m = e$, so G has exponent dividing m.

An example of an infinite group with finite exponent is the infinite direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$. Every element of this group has order 1 or 2, so the exponent of this group is 2.

A finite group of exponent m does not always contain an element of order m: consider S_3, which has exponent 6 but does not contain an element of order 6. ■

Exercise 5.2.7

Let p be a prime and let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$ be an abelian p-group, where $|x_i| = p^{\alpha_i} > 1$ for all i. Define the pth*-power map*

$$\varphi \colon A \to A \quad \text{by} \quad \varphi \colon x \mapsto x^p.$$

(a) Prove that φ is a homomorphism.
(b) Describe the image and kernel of φ in terms of the given generators.
(c) Prove both $\ker \varphi$ and $A/\operatorname{im} \varphi$ have rank n (i.e., have the same rank as A) and prove these groups are both isomorphic to the elementary abelian group, E_{p^n}, of order p^n.

Solution.
(a) Let $x = (x_1^{s_1}, x_2^{s_2}, \ldots, x_n^{s_n})$ and $y = (x_1^{t_1}, x_2^{t_2}, \ldots, x_n^{t_n})$ be elements of A. Then

$$\begin{aligned}
\varphi(xy) &= \varphi((x_1^{s_1+t_1}, x_2^{s_2+t_2}, \ldots, x_n^{s_n+t_n})) \\
&= (x_1^{p(s_1+t_1)}, x_2^{p(s_2+t_2)}, \ldots, x_n^{p(s_n+t_n)}) \\
&= (x_1^{ps_1} x_1^{pt_1}, x_2^{ps_2} x_2^{pt_2}, \ldots, x_n^{ps_n} x_n^{pt_n}) \\
&= (x_1^{ps_1}, x_2^{ps_2}, \ldots, x_n^{ps_n})(x_1^{pt_1}, x_2^{pt_2}, \ldots, x_n^{pt_n}) \\
&= \varphi(x)\varphi(y)
\end{aligned}$$

as desired.

(b) φ collects all the p-powers, so $\operatorname{im}\varphi = \langle x_1^p\rangle \times \langle x_2^p\rangle \times \cdots \times \langle x_n^p\rangle$. Moreover, $\ker\varphi$ consists of all elements $(x_1^{s_1}, x_2^{s_2}, \ldots, x_n^{s_n})$ such that $x_1^{ps_1} = x_2^{ps_2} = \cdots = x_n^{ps_n} = e$, which implies that ps_i is a multiple of p^{α_i} for all i, so s_i is a multiple of $p^{\alpha_i - 1}$ for all i. Thus,

$$\ker\varphi = \langle x_1^{p^{\alpha_1 - 1}}\rangle \times \langle x_2^{p^{\alpha_2 - 1}}\rangle \times \cdots \times \langle x_n^{p^{\alpha_n - 1}}\rangle.$$

(c) Note that $x_i^{p^{\alpha_i - 1}}$ has order p for all i, so $\ker\varphi$ is an elementary abelian group of order p^n. Moreover, note that each $\langle x_i\rangle$ is cyclic, hence every group is normal. Examining $\langle x_i\rangle/\langle x_i^p\rangle$, we see that $\langle x_i\rangle/\langle x_i^p\rangle$ is an elementary abelian group of order p. Since $A/\operatorname{im}\varphi$ is the direct product of the $\langle x_i\rangle/\langle x_i^p\rangle$, we conclude that $A/\operatorname{im}\varphi$ is an elementary abelian group of order p^n, by Exercise 5.1.14. ■

Exercise 5.2.8

Let A be a finite abelian group (written multiplicatively) and let p be a prime. Let

$$A^p = \{a^p \mid a \in A\} \qquad \text{and} \qquad A_p = \{x \mid x^p = 1\}$$

(so A^p and A_p are the image and kernel of the pth-power map, respectively).

(a) Prove that $A/A^p \cong A_p$. [Show that they are both elementary abelian and they have the same order.]

(b) Prove that the number of subgroups of A of order p equals the number of subgroups of A of index p. [Reduce to the case where A is an elementary abelian p-group.]

Solution.

(a) By Theorem 5.5, we may write A as a direct product:

$$A \cong A_{p_1} \times A_{p_2} \times \cdots \times A_{p_k},$$

where each A_{p_i} is a p_i-group for distinct primes $p_1, p_2, \ldots, p_k$. There are two cases:

- If $p \neq p_i$ for all i, then then $(p, p_i) = 1$ for all i, so the p-th power map is an automorphism of each A_{p_i}, so $A^p = A$ and $A_p = \{1\}$, so $A/A^p \cong A_p$.
- If $p = p_i$ for some i, then it is an automorphism for all A_j for $j \neq i$, while the case for A_{p_i} is handled by Exercise 5.2.7. Thus,

$$A^p = A_{p_1} \times \cdots \times A_{p_{i-1}} \times A_{p_i}^p \times A_{p_{i+1}} \times \cdots \times A_{p_k}$$

and

$$A_p = \{1\} \times \cdots \times \{1\} \times (A_{p_i})_p \times \{1\} \times \cdots \times \{1\}.$$

We may again use Exercise 5.1.14 along with the fact that $A_{p_i}/A_{p_i}^p \cong A_{p_i}^p$ to conclude that $A/A^p \cong A_p$.

(b) Let $H \leq A$ such that $|A : H| = p$. Let $a \in A$. Then $aH \in A/H$. Since $|A : H| = p$, $|aH| = 1$ or p. If $|aH| = 1$, then $a \in H$. If $|aH| = p$, then $a^p H = H$, or $a^p \in H$. In either case, we have $a^p \in H$, so $A^p \subseteq H$. By the Lattice Isomorphism Theorem, then subgroups of A containing A^p are in bijection with subgroups of A/A^p. By the previous part, $A/A^p \cong A_p$, so the number of index p subgroups of A equals the number of index p subgroups of A_p.

Now let $K \leq A$ where $|K| = p$. For any $k \in K$, we know $k^p = 1$, so $K \subseteq A_p$. Then subgroups of order p in A are exactly the subgroups of order p in A_p, since $A_p \leq A$. Thus, the number of subgroups of order p in A equals the number of subgroups of order p in A_p.

Note that A_p is an elementary abelian p-group, so it is isomorphic to E_{p^n} for some n. By Exercise 5.1.11, the number of subgroups of order p in E_{p^n} is $\frac{p^n-1}{p-1}$. To see that the number of subgroups of index p in E_{p^n} is also $\frac{p^n-1}{p-1}$, we note that there are $p^n - 1$ surjective homomorphisms from E_{p^n} to E_p, and each subgroup of index p is the kernel of exactly $p - 1$ such homomorphisms, so there are $\frac{p^n-1}{p-1}$ subgroups of index p in E_{p^n}. ■

Exercise 5.2.9

Let $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$. Find the number of elements of order 2 and the number of subgroups of index 2 in A.

Solution. Note that

- $Z_{60} \cong Z_4 \times Z_3 \times Z_5$,
- $Z_{45} \cong Z_9 \times Z_5$,
- $Z_{12} \cong Z_4 \times Z_3$, and

- $Z_{36} \cong Z_4 \times Z_9$.

Thus, the 2-power part of A is $Z_4 \times Z_4 \times Z_4$. Elements of order 2 in A consist of elements of order 2 in the 2-power part of A and elements of order 1 in the other parts of A. The 2-power map sends $(a, b, c) \in A$ to $(2a, 2b, 2c)$, so the kernel of the 2-power map is $\{0, 2\} \times \{0, 2\} \times \{0, 2\}$, which has order $2^3 = 8$. The kernel contains 7 nonidentity elements, so there are 7 elements of order 2 in A.

To see the number of subgroups of index 2 in A, note that index 2 subgroups of A are kernels of surjective homomorphisms from A to Z_2. Since A is abelian, any homomorphism from A to Z_2 is determined by the images of the generators of A. Note that there are exactly 2 homomorphisms from Z_4 to Z_2, which is $x \mapsto 1$ and $x \mapsto y$ for $Z_2 = \langle y \rangle$ and $Z_4 = \langle x \rangle$. Thus, there are $2^3 = 8$ homomorphisms from the 2-power part of A to Z_2. Since one of these homomorphisms is the trivial homomorphism, there are 7 surjective homomorphisms from the 2-power part of A to Z_2, hence there are 7 subgroups of index 2 in A. ■

Exercise 5.2.10

Let n and k be positive integers and let A be the free abelian group of rank n (written additively). Prove that A/kA is isomorphic to the direct product of n copies of $\mathbb{Z}/k\mathbb{Z}$ (here, $kA = \{ka \mid a \in A\}$). [See Exercise 5.1.14.]

Solution. It is easy to see that $kA = k\mathbb{Z} \times \cdots \times k\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $k\mathbb{Z} \trianglelefteq \mathbb{Z}$. By Exercise 5.1.14, we have $A/kA \cong \mathbb{Z}/k\mathbb{Z} \times \cdots \times \mathbb{Z}/k\mathbb{Z}$. ■

Exercise 5.2.11

Let G be a nontrivial, finite abelian group of rank t.
(a) Prove that the rank of G equals the maximum of the ranks of its Sylow subgroups.
(b) Prove that G can be generated by t elements, but no subset with fewer than t elements generates G. (One way of doing this is by using part(a) together with Exercise 5.2.7.)

Solution.

(a) Let G be of type $(n_1, n_2, \ldots, n_t)$, and consider the invariant factor decomposition of G:

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t}.$$

Let p be a prime dividing the smallest factor n_t. Then the Sylow p-subgroup of G is isomorphic to $Z_{p^{\alpha_1}} \times Z_{p^{\alpha_2}} \times \cdots \times Z_{p^{\alpha_t}}$, where α_i is the largest power of p dividing n_i. Since $\alpha_t > 0$, the Sylow p-subgroup has rank t. On the other hand, if q is any prime, then for any $Q \in \mathrm{Syl}_q(G)$, we have

$$Q \cong Z_{q^{\beta_1}} \times Z_{q^{\beta_2}} \times \cdots \times Z_{q^{\beta_t}},$$

where $\beta_i \mid n_i$ for all i with some potentially trivial factors, so the rank of Q is at most t. Thus, the rank of G equals the maximum of the ranks of its Sylow subgroups.

(b) It is clear that G is generated by t elements. Suppose $G = \langle g_1, g_2, \ldots, g_{t-1} \rangle$ and some $P \in \mathrm{Syl}_p(G)$, which has rank t. Projecting G onto P, we see that $P = \langle \pi(g_1), \pi(g_2), \ldots, \pi(g_{t-1}) \rangle$. However, letting φ be the p-power map on P as defined in Exercise 5.2.7, we have that $P/\mathrm{im}\,\varphi \cong E_{p^t}$, so $P/\mathrm{im}\,\varphi$ has rank t. Since $\pi(g_1), \pi(g_2), \ldots, \pi(g_{t-1})$ generate $P/\mathrm{im}\,\varphi$, we have a contradiction. Thus, no subset with fewer than t elements generates G. ■

Exercise 5.2.12

Let n and m be positive integers with $d = (n, m)$. Let $Z_n = \langle x \rangle$ and $Z_m = \langle y \rangle$. Let A be the central product of $\langle x \rangle$ and $\langle y \rangle$ with an element of order d identified, which has presentation

$$\langle x, y \mid x^n = y^m = 1, xy = yx, x^{n/d} = y^{m/d} \rangle.$$

Describe A as a direct product of two cyclic groups.
Note: While the problem specifically calls for two direct products, the proof shows that for any general n, m, A is actually cyclic with order $Z_{nm/d}$, so the second direct product is trivial. I'm not sure if this is a typo, but just know that the problem will have a trivial direct product in the end.

Solution. Since we have an element of order d identified, it is easy to see that $|A| = nm/d$. By Exercise 5.2.5, we know that $\exp(Z_n \times Z_m) = \operatorname{lcm}(n,m) = nm/d$. Note that $|x| = n$ and $|y| = m$ in A still, for otherwise there would be a contradiction to the order of A as we would not be able to account for all the elements of A.

Again, by Exercise 5.2.5, we know that A contains an element of order n iff $n \mid \exp(A)$, and A contains an element of order m iff $m \mid \exp(A)$. Since $\exp(A) \mid |A| = nm/d$, we have that $\exp(A)$ is a common multiple of n and m, so $\exp(A)$ is a multiple of $\operatorname{lcm}(n,m) = nm/d$, hence $\operatorname{lcm}(n,m) \mid \exp(A)$. On the other hand, $\exp(A) \mid |A| = nm/d$ since the order of any element divides the order of the group, so $\exp(A) \mid \operatorname{lcm}(n,m)$. Thus, $\exp(A) = \operatorname{lcm}(n,m)$. We now conclude that A is cyclic, so $A \cong Z_{nm/d} \times Z_1$. ∎

Exercise 5.2.13

Let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_r \rangle$ be a finite abelian group with $|x_i| = n_i$ for $1 \le i \le r$. Find a presentation for A. Prove that if G is any group containing commuting elements $g_1, \ldots, g_r$ such that $g_i^{n_i} = 1$ for $1 \le i \le r$, then there is a unique homomorphism from A to G which sends x_i to g_i for all i.

Solution. A presentation for A is given by

$$\langle x_1, x_2, \ldots, x_r \mid x_i^{n_i} = 1 \text{ for } 1 \le i \le r, x_i x_j = x_j x_i \text{ for } 1 \le i < j \le r \rangle.$$

Now, observe that every element of A is of the form $x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r}$ for some integers $s_1, s_2, \ldots, s_r$. Define $\varphi \colon A \to G$ by $\varphi(x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r}) = g_1^{s_1} g_2^{s_2} \cdots g_r^{s_r}$. Since the g_i commute, φ is well defined. Moreover, φ is a homomorphism since

$$\begin{aligned}
\varphi((x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r})(x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r})) &= \varphi(x_1^{s_1+t_1} x_2^{s_2+t_2} \cdots x_r^{s_r+t_r}) \\
&= g_1^{s_1+t_1} g_2^{s_2+t_2} \cdots g_r^{s_r+t_r} \\
&= (g_1^{s_1} g_2^{s_2} \cdots g_r^{s_r})(g_1^{t_1} g_2^{t_2} \cdots g_r^{t_r}) \\
&= \varphi(x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r}) \varphi(x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r})
\end{aligned}$$

for all integers $s_1, s_2, \ldots, s_r$ and $t_1, t_2, \ldots, t_r$. Finally, $\varphi(x_i) = g_i$ for all i by definition. To see that φ is the unique homomorphism from A to G sending x_i to g_i for all i, let $\psi \colon A \to G$ be any such homomorphism. Then $\psi(x_1^{s_1} x_2^{s_2} \cdots x_r^{s_r}) = \psi(x_1)^{s_1} \psi(x_2)^{s_2} \cdots \psi(x_r)^{s_r} = g_1^{s_1} g_2^{s_2} \cdots g_r^{s_r}$ for all integers $s_1, s_2, \ldots, s_r$, so $\psi = \varphi$. ∎

Exercise 5.2.14

For any group G define the *dual group* of G (denoted $\widehat{G}$) to be the set of all homomorphisms from G into the multiplicative group of roots of unity in $\mathbb{C}$. Define a group operation in $\widehat{G}$ by pointwise multiplication of functions: if χ, ψ are homomorphisms from G into the group of roots of unity then $\chi\psi$ is the homomorphism given by $(\chi\psi)(g) = \chi(g)\psi(g)$ for all $g \in G$, where the latter multiplication takes place in $\mathbb{C}$.

(a) Show that this operation on $\widehat{G}$ makes $\widehat{G}$ into an abelian group. [Show that the identity is the map $g \mapsto 1$ for all $g \in G$ and the inverse of $\chi \in \widehat{G}$ is the map $g \mapsto \chi(g)^{-1}$.]

(b) If G is a finite abelian group, prove that $\widehat{G} \cong G$. [Write G as $\langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ and if $n_i = |x_i|$ define χ_i to be the homomorphism which sends x_i to $e^{2\pi i/n_i}$ and sends x_j to 1, for all $j \ne i$. Prove χ_i has order n_i in $\widehat{G}$ and $\widehat{G} = \langle \chi_1 \rangle \times \cdots \times \langle \chi_r \rangle$.]

Solution.

(a) Multiplication in $\mathbb{C}$ is already associative and commutative, so pointwise multiplication of functions is also associative and commutative. The map $\varepsilon \colon G \to \mathbb{C}$ given by $\varepsilon(g) = 1$ for all $g \in G$ is a homomorphism, since $\varepsilon(gh) = 1 = 1 \cdot 1 = \varepsilon(g)\varepsilon(h)$ for all $g, h \in G$, and 1 is a root of unity. Moreover, for any $\chi \in \widehat{G}$, then $(\chi\varepsilon)(g) = \chi(g)\varepsilon(g) = \chi(g) \cdot 1 = \chi(g)$ for all $g \in G$. Thus, ε is the identity element of $\widehat{G}$. Finally, if $\chi \in \widehat{G}$, then the map $\chi^{-1} \colon G \to \mathbb{C}$ given by $\chi^{-1}(g) = \chi(g)^{-1}$ is a homomorphism, since $\chi^{-1}(gh) = \chi(gh)^{-1} = (\chi(g)\chi(h))^{-1} = \chi(g)^{-1}\chi(h)^{-1} = \chi^{-1}(g)\chi^{-1}(h)$ for all $g, h \in G$, and $\chi(g)^{-1}$ is a root of unity since $\chi(g)$ is a root of unity. Moreover, $\chi\chi^{-1} = \varepsilon$, so χ^{-1} is the inverse of χ in $\widehat{G}$.

(b) To see that χ_i has order n_i in $\widehat{G}$, let $g = x_1^{s_1} \cdots x_r^{s_r} \in G$. Then

$$\chi_i(g) = \chi_i(x_1^{s_1} \cdots x_r^{s_r}) = \chi_i(x_1)^{s_1} \cdots \chi_i(x_r)^{s_r} = e^{2\pi i s_i/n_i},$$

where all terms $\chi_i(x_j)^{s_j}$ for $j \ne i$ are 1. Thus, $\chi_i^k(g) = e^{2\pi i k s_i/n_i}$ for all integers k, so $\chi_i^k = \varepsilon$ if and only if $n_i \mid k$. Thus, χ_i has order n_i in $\widehat{G}$. Now, note by Exercise 5.2.13 that there exists a unique homomorphism $\varphi \colon G \to \widehat{G}$ such that $\varphi(x_i) = \chi_i$ for all i. We now show that φ is an isomorphism.

Let $g = x_1^{s_1} \cdots x_r^{s_r} \in G$ such that $\varphi(g) = \varepsilon$. Then for any x_i, we have that

$$\varphi(g)(x_i) = (\chi_1^{s_1} \cdots \chi_r^{s_r})(x_i) = \chi_i^{s_i}(x_i) = e^{2\pi i s_i/n_i} = 1.$$

Thus, $n_i \mid s_i$ for all i, so $g = x_1^{s_1} \cdots x_r^{s_r} = 1$. Therefore, φ is injective. Similarly, for any $\chi \in \widehat{G}$, and $x_i^{n_i} = 1$ for some i, then $\chi(x_i)^{n_i} = \chi(x_i^{n_i}) = \chi(1) = 1$, so $\chi(x_i)$ is an n_i-th root of unity, so $\chi(x_i) = e^{2\pi i s_i/n_i}$ for some integer s_i. Thus, $\chi = \varphi(x_1^{s_1} \cdots x_r^{s_r})$, so φ is surjective. Therefore, φ is an isomorphism, so $\widehat{G} \cong G$. ∎

Exercise 5.2.15

Let $G = \langle x \rangle \times \langle y \rangle$, where $|x| = 8$ and $|y| = 4$.
(a) Find all pairs a, b in G such that $G = \langle a \rangle \times \langle b \rangle$ (where a and b are expressed in terms of x and y).
(b) Let $H = \langle x^2 y, y^2 \rangle \cong Z_4 \times Z_2$. Prove that there are no elements a, b of G such that $G = \langle a \rangle \times \langle b \rangle$ and $H = \langle a^2 \rangle \times \langle b^2 \rangle$ (i.e., one cannot pick direct product generators for G in such a way that some powers of these are direct product generators for H).

Solution.

(a) From the description of G, we see that G is of type $(8, 4)$, so we have the following conditions for $G = \langle a \rangle \times \langle b \rangle$:
- $|a| = 8$ and $|b| = 4$,
- $\langle a \rangle \cap \langle b \rangle = 1$.

Let $a = x^s y^t$ and $b = x^u y^v$ for some integers s, t, u, v. Then $|a| = \operatorname{lcm}(8/\gcd(8, s), 4/\gcd(4, t))$ and $|b| = \operatorname{lcm}(8/\gcd(8, u), 4/\gcd(4, v))$. For $|a|$ to be 8, we must have $\gcd(8, s) = 1$, implying that s must be odd, while t may range freely. For $|b|$ to be 4, then $8/\gcd(8, u) \mid 4$ and $\max(8/\gcd(8, u), 4/\gcd(4, v)) = 4$, so we have the following cases:
(1) If $\gcd(8, u) = 8$, then $u = 0$ and v must be odd.
(2) If $\gcd(8, u) = 4$, then $u = 4$ and v must be odd.
(3) If $\gcd(8, u) = 2$, then $u = 2, 6$ and v can be free.

To have trivial intersection, we must have that $x^{ks} y^{kt} = x^{\ell u} y^{\ell v} = 1$, or $ks \equiv \ell u \pmod 8$ and $kt \equiv \ell v \pmod 4$ implies that $k \equiv 0 \pmod 8$ and $\ell \equiv 0 \pmod 4$, which is seen from $a^k = 1$ and $b^\ell = 1$ iff $8 \mid k$ and $4 \mid \ell$. Thus, we check the cases for $|b|$:
(1) $u = 0$ and v is odd: We have $ks \equiv 0 \pmod 8$ and $kt \equiv \ell v \pmod 4$. Since s is odd, $k \equiv 0 \pmod 8$. Then $kt \equiv 0 \pmod 4$, hence $\ell v \equiv 0 \pmod 4$. Since v is odd, $\ell \equiv 0 \pmod 4$, so we have trivial intersection.
(2) $u = 4$ and v is odd: We have $ks \equiv 4\ell \pmod 8$ and $kt \equiv \ell v \pmod 4$. Since s is odd, $k \equiv 4\ell s^{-1} \pmod 8$. Note that $k \equiv 0 \pmod 4$, so $kt \equiv 0 \pmod 4$, hence $\ell v \equiv 0 \pmod 4$. Since v is odd, $\ell \equiv 0 \pmod 4$, so we have trivial intersection.
(3) $u = 2$ and v free (the case $u = 6$ and v free is similar): We have $ks \equiv 2\ell \pmod 8$ and $kt \equiv \ell v \pmod 4$. Since s is odd, $k \equiv 2\ell s^{-1} \pmod 8$. We know that intersection will be nontrivial when $k \not\equiv 0 \pmod 8$ and $\ell \not\equiv 0 \pmod 4$. By inspection, we see that $\ell = 2$ gives $k \equiv 4s^{-1} \equiv 4 \pmod 8$ and $4t \equiv 2v \pmod 4$, which has nontrivial solution when v is even. Inspecting odd v, we see that $k \equiv 2\ell s^{-1} \pmod 8$ reduced mod 4 gives $k \equiv 2\ell s^{-1} \pmod 4$. Then $2\ell s^{-1} \equiv \ell v \pmod 4$ implies that $\ell(2s^{-1} - v) \equiv 0 \pmod 4$. Since v is odd, $2s^{-1} - v$ is odd, so $\ell \equiv 0 \pmod 4$, so we have trivial intersection.

Therefore, the pairs a, b such that $G = \langle a \rangle \times \langle b \rangle$ are given by
- $a = x^s y^t$ and $b = y^v$ for some odd integers s, v and any integer t,
- $a = x^s y^t$ and $b = x^4 y^v$ for some odd integers s, v and any integer t,
- $a = x^s y^t$ and $b = x^2 y^v$ for some odd integer s, any integer t, and any odd integer v, or
- $a = x^s y^t$ and $b = x^6 y^v$ for some odd integer s, any integer t, and any odd integer v.

(b) We begin with the elements of H:

$$H = \{1, x^2y, x^4y^2, x^6y^3, y^2, x^2y^3, x^4y, x^6y^2\}$$

Note that $H = \langle x^2 y \rangle \times \langle y^2 \rangle$, so it suffices to check whether or not a^2 generates $\langle x^2 y \rangle$ from the choices of a from part (a). Note that $a^2 = x^{2s} y^{2t}$, which implies that y will always have an even exponent. However, the only element with even exponent on y from $\langle x^2 y \rangle$ is with the term $x^4 y^2$, which would imply that $\langle x^4 y^2 \rangle = \langle x^2 y \rangle$, which is a contradiction since $x^2 y$ has order 4 while $x^4 y^2$ has order 2. Thus, there are no elements a, b of G such that $G = \langle a \rangle \times \langle b \rangle$ and $H = \langle a^2 \rangle \times \langle b^2 \rangle$. ∎

Exercise 5.2.16

Prove that no finitely generated abelian group is divisible (cf. Exercise 2.4.19).

Solution. Let A be a finitely generated abelian group. By Theorem 5.5, we can write A as a direct product of cyclic groups:

$$A \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t},$$

where $n_i > 1$ for all i and $r \geq 0$. For $r > 0$, observe that $\mathbb{Z}$ is not divisible, since there is no $x \in \mathbb{Z}$ such that $2x = 1$. For $r = 0$, observe that A is a finite abelian group. By Exercise 2.4.19, finite abelian groups are not divisible. Thus, no finitely generated abelian group is divisible. ■

5.3 Table of Groups of Small Order

Exercise 5.3.1

Prove that $D_{16}, Z_2 \times D_8, Z_2 \times Q_8, Z_4 * D_8, QD_{16}$, and M are nonisomorphic, non-abelian groups of order 16 (where $Z_4 * D_8$ is described in Exercise 5.1.12 and QD_{16} and M are described in Exercise 2.5.11 and Exercise 2.5.14 respectively).

Solution. We do a "decision tree"-like process to show that these are nonisomorphic:

- D_{16}
  - $Z_2 \times D_8$ has no element of order 8, while D_{16} does.
  - $Z_2 \times Q_8$ has no element of order 8, while D_{16} does.
  - $Z_4 * D_8$ has no elements of order 8, since taking quotients only preserves divisibility of orders from $Z_4 \times D_8$, which has no elements of order 8, while D_{16} does.
  - In QD_{16}, we have $|\sigma^4| = 2$, and $|\sigma^k\tau| = 2$ when
    $$\sigma^k\tau\sigma^k\tau = \sigma^k\sigma^{3k}\tau\tau = \sigma^{4k},$$
    hence $\sigma^{4k} = 1$ when k is even, hence there are only 5 elements of order 2 in QD_{16}, while there are 8 reflections of order 2, plus the central rotation r^4, for a total of 9 elements of order 2 in D_{16}.
  - M has $|u| = 2$, with
    $$uv^kuv^k = uuv^{5k}v^k = v^{6k},$$
    so $v^{6k} = 1$ when $8 \mid 6k$, or $4 \mid 3k$, or $4 \mid k$. Then only $k = 4$ works, giving M a total of 3 elements of order 2.
- $Z_2 \times D_8$
  - $Z_2 \times Q_8$ does not have the same number of elements of order 2 as $Z_2 \times D_8$ does, since D_8 has 5 elements of order 2, while Q_8 has only 1 element of order 2.
  - Note that $\overline{(x^k, q)} \in Z_4 * Q_8 \cong Z_4 * D_8$ has order 2 when $(x^k, q)^2 = (1, 1)$ or $(x^2, -1)$. Since we already identify x^2 with -1 in the quotient, the case of $q^2 = 1$ and $2i \equiv 0 \pmod 4$ gives the same element, hence only 1 element of order 2. The other case of $q^2 = -1$ and $2i \equiv 2 \pmod 4$, or i odd and $q = Q_8 - Z(Q_8)$ gives 6 elements of order 2, for a total of 7 elements of order 2 in $Z_4 * D_8$, while $Z_2 \times D_8$ has 11 elements of order 2.
  - QD_{16} contains elements of order 8, while $Z_2 \times D_8$ does not.
  - M contains elements of order 8, while $Z_2 \times D_8$ does not.
- $Z_2 \times Q_8$
  - Note that $Z_2 \times Q_8$ only has 3 elements of order 2, while $Z_4 * D_8$ has 7 elements of order 2.
  - QD_{16} contains elements of order 8, while $Z_2 \times Q_8$ does not.
  - M contains elements of order 8, while $Z_2 \times Q_8$ does not.
- $Z_4 * D_8$
  - QD_{16} contains elements of order 8, while $Z_4 * D_8$ does not.
  - M contains elements of order 8, while $Z_4 * D_8$ does not.
- QD_{16}
  - M has only 3 elements of order 2, while QD_{16} has 5 elements of order 2. ■

5.4 Recognizing Direct Products

Let G be a group.

Exercise 5.4.1

Prove that if $x, y \in G$, then $[y, x] = [x, y]^{-1}$. Deduce that for any subsets A and B of G, $[A, B] = [B, A]$ (recall that $[A, B]$ is the *subgroup* of G generated by the commutators $[a, b]$).

Solution. Note that

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = yxy^{-1}x^{-1} = [y, x].$$

Hence, $[y, x] = [x, y]^{-1}$. For any subsets A and B of G, the subgroup $[A, B]$ is generated by the commutators $[a, b]$ for $a \in A$ and $b \in B$. Since $[a, b] = [b, a]^{-1}$, it follows that $[A, B] = [B, A]$. ■

Exercise 5.4.2

Prove that a subgroup H of G is normal if and only if $[G, H] \leq H$.

Solution. By Exercise 5.4.1, we know $[H, G] = [G, H]$. Then use Proposition 5.7(2). ■

Exercise 5.4.3

Let $a, b, c \in G$. Prove that
(a) $[a, bc] = [a, c](c^{-1}[a, b]c)$,
(b) $[ab, c] = (b^{-1}[a, c]b)[b, c]$.

Solution.
(a) $[a, bc] = a^{-1}(bc)^{-1}a(bc) = a^{-1}c^{-1}b^{-1}abc = a^{-1}c^{-1}ac(c^{-1}a^{-1}b^{-1}abc) = [a, c](c^{-1}[a, b]c)$.
(b) $[ab, c] = (ab)^{-1}c^{-1}(ab)c = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}ac(c^{-1}a^{-1}b^{-1}abc) = (b^{-1}[a, c]b)[b, c]$. ■

Exercise 5.4.4

Find the commutator subgroups of S_4 and A_4.

Solution. Note that $A_4 \trianglelefteq S_4$ and $S_4/A_4 \cong Z_2$, which is abelian, so $[S_4, S_4] \leq A_4$. On the other hand, A_4 is generated by the 3-cycles, and $[S_4, S_4]$ contains all 3-cycles since for any 3-cycle $(a\ b\ c)$, we have that

$$(a\ b\ c) = (a\ b)^{-1}(a\ c)^{-1}(a\ b)(a\ c) = [(a\ c), (a\ b)],$$

so $A_4 \leq [S_4, S_4]$. Thus, $[S_4, S_4] = A_4$.

By Exercise 3.5.9, we know that $V_4 \trianglelefteq A_4$ and $A_4/V_4 \cong Z_3$, which is abelian, so $[A_4, A_4] \leq V_4$. On the other hand, A_4 is non-abelian, so $[A_4, A_4]$ is nontrivial. Since V_4 is the only nontrivial subgroup of A_4 that is normal, we must have $[A_4, A_4] = V_4$. ■

Exercise 5.4.5

Prove that A_n is the commutator subgroup of S_n for all $n \geq 5$.

Solution. Similar argument as in the previous exercise, where $S_n/A_n \cong Z_2$. ■

Exercise 5.4.6

Exhibit a representative of each cycle type of A_5 as a commutator in S_5.

Solution. The cycle types of A_5 are the identity, 3-cycles, products of two disjoint 2-cycles, and 5-cycles. The identity is the commutator of any element with itself, so we can take $[1,1] = 1$. For a 3-cycle $(a\ b\ c)$, we have that

$$(a\ b\ c) = (a\ b)^{-1}(a\ c)^{-1}(a\ b)(a\ c) = [(a\ c),(a\ b)].$$

For a product of two disjoint 2-cycles $(a\ b)(c\ d)$, we have that

$$(a\ b)(c\ d) = (a\ b\ d)^{-1}(b\ c\ d)^{-1}(a\ b\ d)(b\ c\ d) = [(a\ b\ d),(b\ c\ d)].$$

For a 5-cycle $(a\ b\ c\ d\ e)$, we have that

$$(a\ b\ c\ d\ e) = (a\ e\ d)^{-1}((b\ e)(c\ d))^{-1}(a\ e\ d)((b\ e)(c\ d)) = [(a\ e\ d),(b\ e)(c\ d)].$$ ■

Exercise 5.4.7

Prove that if p is a prime and P is a non-abelian group of order p^3, then $P' = Z(P)$.

Solution. Let P be a non-abelian group of order p^3. By the class equation, we have that $|Z(P)|$ divides p^3 and is greater than 1, so $|Z(P)| = p$ or p^2. If $|Z(P)| = p^2$, then $P/Z(P)$ is cyclic, so P is abelian, which is a contradiction. Thus, $|Z(P)| = p$, so $P/Z(P)$ is of order p^2, hence abelian. Therefore, $P' \leq Z(P)$. On the other hand, if $P' < Z(P)$, then properness of P' implies that $|P'| = 1$, so P is abelian, which is a contradiction. Thus, $P' = Z(P)$. ■

Exercise 5.4.8

Assume $x, y \in G$, and both x and y commute with $[x,y]$. Prove that for all $n \in \mathbb{Z}^+$,

$$(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}.$$

Solution. We first prove that for all $n \in \mathbb{Z}^+$,

$$y^n x = x y^n [y,x]^n.$$

We do this by induction on n. For $n = 1$, we have $yx = (xyy^{-1}x^{-1})(yx) = xy[y,x]$. Now, assume that $y^n x = xy^n[y,x]^n$ for some $n \in \mathbb{Z}^+$. Then

$$y^{n+1}x = y(y^n x) = y(xy^n[y,x]^n) = (yx)y^n[y,x]^n = xy[y,x]y^n[y,x]^n = xy^{n+1}[y,x]^{n+1}.$$

Now, we prove the main statement by induction on n. For $n = 1$, we have $(xy)^n = xy = x^n y^n [y,x]^{\frac{n(n-1)}{2}}$. Now, assume that $(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}$ for some $n \in \mathbb{Z}^+$. Then

$$\begin{aligned}
(xy)^{n+1} &= (xy)^n (xy) \\
&= (x^n y^n [y,x]^{\frac{n(n-1)}{2}})(xy) \\
&= x^n y^n [y,x]^{\frac{n(n-1)}{2}} xy \\
&= x^n y^n xy [y,x]^{\frac{n(n-1)}{2}} \\
&= x^{n+1} y^{n+1} [y,x]^{\frac{(n+1)n}{2}}.
\end{aligned}$$ ■

Exercise 5.4.9

Prove that if p is an odd prime, and P is a group of order p^3, then the p-th power map $x \mapsto x^p$ is a homomorphism of P into $Z(P)$. If P is not cyclic, show that the kernel of the p-th power map has order p^2 or p^3. Is the squaring map a homomorphism in non-abelian groups of order 8? Where is the oddness of p needed in the above proof?

Solution. Note that the abelian case is trivial, so we may assume P is non-abelian. By Exercise 5.4.7, we have $P' = Z(P)$, so $P/Z(P)$ is abelian. Note that $[y,x] \in P' = Z(P)$ for all $x, y \in P$, so x and y both commute with $[y,x]$. Moreover, $|Z(P)| = p$ by Exercise 5.4.7, hence

$$(xy)^p = x^p y^p [y,x]^{\frac{p(p-1)}{2}} = x^p y^p,$$

where the last equality holds since $[y,x]$ has order dividing p and $\frac{p(p-1)}{2}$ is divisible by p when p is odd. Thus, the p-th power map is a homomorphism of P into $Z(P)$. To see that $x^p \in Z(P)$ for all $x \in P$, note that for any $y \in P$, we have

$$yx^p y^{-1} = (yxy^{-1})^p = (x[y,x])^p = x^p [y,x]^p = x^p.$$

Suppose now that P is not cyclic. Since the map is to $Z(P)$, which has order p, the image of the map has order dividing p. If the image is trivial, then the kernel is all of P, so the kernel has order p^3. If the image is nontrivial, then the kernel has order p^2 by the First Isomorphism Theorem.

For the squaring map in non-abelian groups of order 8, we have Q_8 and D_8. In Q_8, observe that $(ij)^2 = (k)^2 = -1$, while $i^2j^2 = 1$. In D_8, we similarly have $(rs)^2 = 1$, while $r^2s^2 = r^2$. Thus, the squaring map is not a homomorphism in non-abelian groups of order 8. Lastly, the oddness of p is needed in the proof to ensure that $\frac{p(p-1)}{2}$ is divisible by p, which allows us to conclude that $[y, x]^{\frac{p(p-1)}{2}} = 1$. ■

Exercise 5.4.10

Prove that a finite abelian group is the direct product of its Sylow subgroups.

Solution. Inducting on the number of prime factors of the group, we first consider $n = 1$, or when $|G| = p_1^n$ for some prime p_1. Then G is its own Sylow p_1-subgroup, so the statement holds. We now assume that any abelian with fewer than n prime factors is the direct product of its Sylow subgroups, and let G be an abelian group with n prime factors. Put

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

Let H be some subgroup of G generated by the Sylow p_i subgroups for $1 \leq i \leq n-1$. By definition, every element of H is generated by some element from a Sylow p_i-subgroup, so its order must divide the LCM $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{n-1}^{\alpha_{n-1}}$, so H is a proper subgroup of G. Moreover, H contains all such Sylow p_i-subgroups for $1 \leq i \leq n-1$, hence $|H| \geq p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{n-1}^{\alpha_{n-1}}$. Since H is a proper subgroup of G, we must have $|H| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{n-1}^{\alpha_{n-1}}$. By the inductive hypothesis, H is the direct product of its Sylow subgroups, so

$$H = P_1 \times P_2 \times \cdots \times P_{n-1},$$

where P_i is the Sylow p_i-subgroup of G for $1 \leq i \leq n-1$. Since G is abelian, we have that P_n is normal in G, so HP_n is a subgroup of G. Moreover, since H and P_n have trivial intersection because $p_n^{\alpha_n}$ and $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{n-1}^{\alpha_{n-1}}$ are relatively prime, we have that $HP_n = H \times P_n$. Since $|HP_n| = |H||P_n| = |G|$, we must have $HP_n = G$, so

$$G = P_1 \times P_2 \times \cdots \times P_n.$$ ■

Exercise 5.4.11

Prove that if $G = HK$ where H and K are characteristic subgroups of G with $H \cap K = 1$, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Deduce that if G is an abelian group of finite order, then $\mathrm{Aut}(G)$ is isomorphic to the direct product of the automorphism groups of its Sylow subgroups.

Solution. Let $\varphi \in \mathrm{Aut}(G)$. Since H and K are characteristic subgroups of G, we have $\varphi(H) = H$ and $\varphi(K) = K$. Thus, we can define $\varphi_H = \varphi|_H$ and $\varphi_K = \varphi|_K$, which are automorphisms of H and K respectively. We can then define a map $\Phi : \mathrm{Aut}(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ by $\Phi(\varphi) = (\varphi_H, \varphi_K)$. To see that Φ is a homomorphism, let $\varphi, \psi \in \mathrm{Aut}(G)$ be given. Then

$$\Phi(\varphi \circ \psi) = ((\varphi \circ \psi)_H, (\varphi \circ \psi)_K) = (\varphi_H \circ \psi_H, \varphi_K \circ \psi_K) = \Phi(\varphi) \circ \Phi(\psi).$$

To see that Φ is injective, let $\varphi \in \mathrm{Aut}(G)$ be given such that $\Phi(\varphi) = (1_H, 1_K)$, where 1_H and 1_K are the identity automorphisms of H and K respectively. Then $\varphi(h) = h$ for all $h \in H$ and $\varphi(k) = k$ for all $k \in K$. Since every element of G can be uniquely expressed as hk for some $h \in H$ and $k \in K$, we have $\varphi(hk) = \varphi(h)\varphi(k) = hk$, so φ is the identity automorphism of G. Thus, Φ is injective.

To show that Φ is surjective, let $(\psi_H, \psi_K) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ be given. We can define a map $\psi : G \to G$ by $\psi(hk) = \psi_H(h)\psi_K(k)$ for all $h \in H$ and $k \in K$. Because $H \cap K = 1$, and $G = HK$, every element of G can be uniquely expressed as hk for some $h \in H$ and $k \in K$. We check that ψ is a homomorphism:

$$\psi(h_1k_1 \cdot h_2k_2) = \psi(h_1h_2k_1k_2) = \psi_H(h_1h_2)\psi_K(k_1k_2) = \psi_H(h_1)\psi_H(h_2)\psi_K(k_1)\psi_K(k_2) = \psi(h_1k_1)\psi(h_2k_2),$$

where k_1 and h_2 commute since H and K are the factors of $G = H \times K$. Since ψ_H and ψ_K are automorphisms, ψ is a bijection, hence an automorphism of G. Moreover, $\Phi(\psi) = (\psi_H, \psi_K)$, so Φ is surjective.

Therefore, we have shown that $\Phi : \mathrm{Aut}(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ is an isomorphism. For the second part of the problem, since a finite abelian group is the direct product of its Sylow subgroups by the previous exercise, and conjugation is trivial in an abelian group, we have that each Sylow subgroup is characteristic, so the automorphism group of the finite abelian group is isomorphic to the direct product of the automorphism groups of its Sylow subgroups. ■

Exercise 5.4.12

Use Theorem 4.17 to describe the automorphism group of a finite cyclic group.

Solution. From Proposition 4.17, we know that $\text{Aut}(Z_p) \cong Z_{p-1}$, and $\text{Aut}(Z_{p^n}) \cong Z_{p^{n-1}(p-1)}$ for any prime p and $n \geq 2$. For $n \geq 3$ and $p = 2$, we have that $\text{Aut}(Z_{2^n}) \cong Z_2 \times Z_{2^{n-2}}$ that is not cyclic. Hence, for any finite cyclic group Z_n with (specific) prime factorization $n = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, we have by Exercise 5.4.10 and the previous exercise that

$$\text{Aut}(Z_n) \cong \text{Aut}(Z_{2^{\alpha_1}}) \times \text{Aut}(Z_{p_2^{\alpha_2}}) \times \cdots \times \text{Aut}(Z_{p_k^{\alpha_k}}).$$

Note that $\text{Aut}(Z_{p_i^{\alpha_i}}) \cong Z_{p_i^{\alpha_i - 1}(p_i - 1)}$ is cyclic for $i \geq 2$, and $\text{Aut}(Z_{2^{\alpha_1}})$ is cyclic if $\alpha_1 \leq 2$ and is not cyclic if $\alpha_1 \geq 3$. Thus, the structure of $\text{Aut}(Z_n)$ depends on the exponent of 2 in the prime factorization of n. We can check the following cases:

- $\alpha_1 = 0$: Then the 2-part of n is trivial, so $\text{Aut}(Z_n) \cong Z_{p_2^{\alpha_2 - 1}(p_2 - 1)} \times \cdots \times Z_{p_k^{\alpha_k - 1}(p_k - 1)}$ is cyclic if and only if $k = 1$, or the $p_i^{\alpha_i - 1}(p_i - 1)$ are pairwise relatively prime.
- $\alpha_1 = 1$: Then the 2-part of n is Z_2 with $\text{Aut}(Z_2)$ trivial, so $\text{Aut}(Z_n) \cong Z_{p_2^{\alpha_2 - 1}(p_2 - 1)} \times \cdots \times Z_{p_k^{\alpha_k - 1}(p_k - 1)}$ is cyclic if and only if the orders $p_i^{\alpha_i - 1}(p_i - 1)$ are pairwise relatively prime and relatively prime to 2, which is equivalent to the condition in the previous case. Hence, the same condition as $\alpha_1 = 0$ applies here.
- $\alpha_1 = 2$: Then the 2-part of n is Z_4, so $\text{Aut}(Z_n) \cong \text{Aut}(Z_4) \times Z_{p_2^{\alpha_2 - 1}(p_2 - 1)} \times \cdots \times Z_{p_k^{\alpha_k - 1}(p_k - 1)}$ is cyclic if and only if $k = 1$, similar to $\alpha_1 = 0$, or the $p_i^{\alpha_i - 1}(p_i - 1)$ are pairwise relatively prime and relatively prime to 2.
- $\alpha_1 \geq 3$: Then the 2-part of n is $Z_2 \times Z_{2^{\alpha_1 - 2}}$, so $\text{Aut}(Z_n) \cong \text{Aut}(Z_{2^{\alpha_1}}) \times Z_{p_2^{\alpha_2 - 1}(p_2 - 1)} \times \cdots \times Z_{p_k^{\alpha_k - 1}(p_k - 1)}$ is not cyclic. ■

Exercise 5.4.13

Prove that D_{8n} is not isomorphic to $D_{4n} \times Z_2$ for any $n \geq 1$.

Solution. Note that $Z(D_{8n}) = \{1, r^{2n}\}$ has order 2, while $Z(D_{4n} \times Z_2) = Z(D_{4n}) \times Z(Z_2)$ has order 4, so D_{8n} cannot be isomorphic to $D_{4n} \times Z_2$ for any $n \geq 1$. ■

Exercise 5.4.14

Let $G = \{(a_{ij}) \in \text{GL}_n(F) \mid a_{ij} = 0 \text{ for } i > j, \text{ and } a_{11} = a_{22} = \cdots = a_{nn}\}$, where F is a field, be the group of upper triangular matrices all of whose diagonal entries are equal. Prove that $G \cong D \times U$, where D is the group of all nonzero multiples of the identity matrix, and U is the group of upper triangular matrices with 1's down the diagonal.

Solution. Note that $I_n \in D$. For any $\lambda, \mu \in F^\times$, then $(\lambda I_n)(\mu I_n)^{-1} = (\lambda I_n)(\mu^{-1} I_n) = (\lambda \mu^{-1}) I_n \in D$, so D is a subgroup of G. For $A, B \in U$, we know that the product still has AB upper triangular with 1's down the diagonal, so U is a subgroup of G. To see that $D \trianglelefteq G$, let $A \in G$ be given. Then A is upper triangular with all diagonal entries equal to some $\lambda \in F^\times$. For any $\mu I_n \in D$, we have

$$A(\mu I_n)A^{-1} = \mu A I_n A^{-1} = \mu A A^{-1} = \mu I_n \in D,$$

so D is normal in G. To see that $U \trianglelefteq G$, let $A \in G$ be given. Then A is upper triangular with all diagonal entries equal to some $\lambda \in F^\times$. We may factor out $\lambda = a_{11}$ from A to get $A = a_{11} X$, where X is upper triangular with 1's down the diagonal, so $X \in U$. For any $Y \in U$, we have

$$AYA^{-1} = a_{11} X Y X^{-1} a_{11}^{-1} = XYX^{-1},$$

where $XYX^{-1} \in U$ since $U \leq G$, so U is normal in G. If $Z \in D \cap U$, then $Z = \lambda I_n$ for some $\lambda \in F^\times$, and Z is upper triangular with 1's down the diagonal, so $\lambda = 1$, hence $Z = I_n$. Thus, $D \cap U = 1$. Lastly, for any $A \in G$, we can factor out the common diagonal entry to get $A = a_{11} X$ for some $X \in U$, so $G = DU \cong D \times U$ by Theorem 5.9. ■

Exercise 5.4.15

If A and B are normal subgroups of G such that G/A and G/B are both abelian, prove that $G/(A \cap B)$ is abelian.

Solution. G/A abelian implies $G' \leq A$, and G/B abelian implies $G' \leq B$, so $G' \leq A \cap B$. Hence, $G/(A \cap B)$ is abelian by Proposition 5.7(4). ■

Exercise 5.4.16

Prove that if K is a normal subgroup of G, then $K' \trianglelefteq G$.

Solution. Let K be a normal subgroup of G. By Proposition 5.7(2), we have $[G, K] \leq K$. Since $K' = [K, K] \leq [G, K]$, we have $K' \leq K$. Moreover, for any $g \in G$ and $x = c_1 c_2 \cdots c_n \in K'$, where $c_i = [k_i, \ell_i]$ for some $k_i, \ell_i \in K$, we have

$$gxg^{-1} = gc_1c_2\cdots c_n g^{-1} = (gc_1g^{-1})(gc_2g^{-1})\cdots(gc_ng^{-1}),$$

where $gc_ig^{-1} = g[k_i, \ell_i]g^{-1} = [gk_ig^{-1}, g\ell_ig^{-1}]$ since K is normal in G, so $gxg^{-1} \in K'$. Thus, $K' \trianglelefteq G$. ■

Exercise 5.4.17

If K is a normal subgroup of G and K is cyclic, prove that $G' \leq C_G(K)$. [Recall that the automorphism group of a cyclic group is abelian.]

Solution. Let K be a normal subgroup of G and K be cyclic. Since K is cyclic, we have $\mathrm{Aut}(K)$ is abelian. Moreover, the homomorphism of G into $\mathrm{Aut}(K)$ given by conjugation has kernel $C_G(K)$, so $G/C_G(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(K)$, which is abelian. Hence, $G' \leq C_G(K)$ by Proposition 5.7(4). ■

Exercise 5.4.18

Let $K_1, K_2, \ldots, K_n$ be non-abelian simple groups, and let $G = K_1 \times K_2 \times \cdots \times K_n$. Prove that every normal subgroup of G is of the form G_I for some subset I of $\{1, 2, \ldots, n\}$ (where G_I is defined in Exercise 5.1.2). [If $N \trianglelefteq G$ and $x = (a_1, \ldots, a_n) \in N$ with some $a_i \neq 1$, then show that there is some $g_i \in G_i$ not commuting with a_i. Show that $[(1, \ldots, g_i, \ldots, 1), x] \in K_i \cap N$, and deduce $K_i \leq N$.]

Solution. Let N be a normal subgroup of G. If $N = 1$, then $N = G_\varnothing$. If $N = G$, then $N = G_{\{1,2,\ldots,n\}}$. Now, assume that $1 < N < G$. Then there exists some $x = (a_1, a_2, \ldots, a_n) \in N$ such that $a_i \neq 1$ for some i. Since K_i is non-abelian simple, there exists some $g_i \in K_i$ such that g_i does not commute with a_i. Consider the element $(1, \ldots, g_i, \ldots, 1) \in G$, where g_i is in the i-th position. We have

$$(1, \ldots, g_i, \ldots, 1)x(1, \ldots, g_i^{-1}, \ldots, 1) = (a_1, \ldots, g_i a_i g_i^{-1}, \ldots, a_n).$$

Hence,

$$(1, \ldots, g_i, \ldots, 1)x(1, \ldots, g_i^{-1}, \ldots, 1)x^{-1} = (1, \ldots, [g_i, a_i], \ldots, 1) \in N.$$

Since $[g_i, a_i]$ is nontrivial and is an element of the simple group K_i, we have that $\langle [g_i, a_i]^{K_i} \rangle \trianglelefteq K_i$. However, simplicity of K_i forces $\langle [g_i, a_i]^{K_i} \rangle = K_i$, so $K_i \leq N$. By repeating this argument for any other nontrivial component of an element of N, we can find some subset I of $\{1, 2, \ldots n\}$ such that $G_I = K_{i_1} \times K_{i_2} \times \cdots K_{i_k} \leq N$, where $\{i_1, i_2, \ldots i_k\} = I$, which shows $G_I \leq N$. On the other hand, if N contains some element $x = (a_1, a_2, \ldots, a_n)$ such that $a_j \neq 1$ for some $j \notin I$, then we can similarly find some element of N that has nontrivial component in the j-th position, which contradicts that $K_j \not\leq N$. Thus, $N \leq G_I$. Therefore, $N = G_I$. ■

Exercise 5.4.19

A group H is called *perfect* if $H' = H$ (i.e., H equals its own commutator subgroup).

(a) Prove that every non-abelian simple group is perfect.
(b) Prove that if H and K are perfect subgroups of a group G, then $\langle H, K \rangle$ is also perfect. Extend this to show that the subgroup of G generated by any collection of perfect subgroups is perfect.
(c) Prove that any conjugate of a perfect subgroup is perfect.
(d) Prove that any group G has a maximal perfect subgroup, and that this subgroup is normal.

Solution.

(a) Let H be a non-abelian simple group. Since H is non-abelian, we have $H' \neq 1$. Since H is simple, the only normal subgroups of H are 1 and H, so we must have $H' = H$.

(b) Let H and K be perfect subgroups of a group G. We want to show that $\langle H, K\rangle' = \langle H, K\rangle$. Since H and K are perfect, we have $H' = H$ and $K' = K$, so $H \leq H'$ and $K \leq K'$. Moreover, since H and K are subgroups of $\langle H, K\rangle$, we have $H' \leq \langle H, K\rangle'$ and $K' \leq \langle H, K\rangle'$, so $H \leq \langle H, K\rangle'$ and $K \leq \langle H, K\rangle'$. Hence, $\langle H, K\rangle = \langle H, K\rangle'$. The extension to any collection of perfect subgroups follows by induction on the number of perfect subgroups in the collection.

(c) Let H be a perfect subgroup of a group G, and let $g \in G$ be given. We want to show that $g^{-1}Hg$ is perfect. Since H is perfect, we have $H' = H$, so $g^{-1}H'g = g^{-1}Hg$. Moreover, since conjugation is an automorphism of G, we have $g^{-1}H'g = (g^{-1}Hg)'$, so $(g^{-1}Hg)' = g^{-1}Hg$. Hence, $g^{-1}Hg$ is perfect.

(d) Let $\mathcal{P}$ be the collection of perfect subgroups of G. Since 1 is a perfect subgroup of G, we have $\mathcal{P}$ is nonempty. Let $\mathcal{C}$ be a chain in $\mathcal{P}$, and let $H = \bigcup_{K\in\mathcal{C}} K$. To see that $H \leq G$, note that for any $x, y \in H$, then there exists $K_x, K_y \in \mathcal{C}$ such that $x \in K_x$ and $y \in K_y$. Without loss of generality, we may assume $K_x \leq K_y$, so $x, y \in K_y$, hence $xy^{-1} \in K_y \leq H$. Thus, H is a subgroup of G. To see that $H \in \mathcal{P}$, observe that for any $x \in H$, then $x \in K$ for some $K \in \mathcal{C}$, so $x \in K' = K$, hence $x \in H'$. Thus, $H \leq H'$. Since $H' \leq H$ trivially, $H = H'$, hence $H \in \mathcal{P}$. By Zorn's Lemma, $\mathcal{P}$ has a maximal element M.

To see that M is normal in G, let $g \in G$ be given. Then $g^{-1}Mg$ is perfect by part (c), so $g^{-1}Mg \in \mathcal{P}$. Since M is perfect, we may use part (b) to get that $\langle M, g^{-1}Mg\rangle$ is perfect, so $\langle M, g^{-1}Mg\rangle \in \mathcal{P}$. Since $M \leq \langle M, g^{-1}Mg\rangle$ and M is maximal in $\mathcal{P}$, we must have $M = \langle M, g^{-1}Mg\rangle$, so $g^{-1}Mg \leq M$. By symmetry of the argument, we also have $M \leq g^{-1}Mg$, so $g^{-1}Mg = M$. Hence, M is normal in G. ■

Exercise 5.4.20

Let $H(F)$ be the Heisenberg group over the field F, cf. Exercise 1.4.11. Find an explicit formula for the commutator $[X, Y]$, where $X, Y \in H(F)$, and show that the commutator subgroup of $H(F)$ equals the center of $H(F)$ (cf. Exercise 2.2.14).

Solution. Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in H(F).$$

Then we have

$$X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}, \quad Y^{-1} = \begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence,

$$\begin{aligned} [X, Y] &= X^{-1}Y^{-1}XY \\ &= \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & af-cd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Recall that the center of $H(F)$ consists of all matrices of the form

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

for some $z \in F$. Clearly, $af - cd \in F$, so $[X, Y] \in Z(H(F))$, hence $H(F)' \leq Z(H(F))$. On the other hand, for any $z \in F$, we may choose $a = 1$, $f = z$, and $c = d = 0$ to get that $Z(H(F)) \leq H(F)'$. Therefore, $H(F)' = Z(H(F))$. ■

5.5 Semidirect Products

Let H and K be groups, let $\varphi\colon K \to \mathrm{Aut}(H)$ be a homomorphism, and identify $H, K \leq G = H \rtimes_\varphi K$.

Exercise 5.5.1

Prove that $C_K(H) = \ker\varphi$ (recall that $C_K(H) = C_G(H) \cap K$).

Solution. Let $k \in C_K(H)$. Then $k \in K$ and $kh = hk$ for all $h \in H$. Then $\varphi(k)(h) = khk^{-1} = h$ for all $h \in H$, so $k \in \ker\varphi$. Conversely, let $k \in \ker\varphi$. Then $\varphi(k)(h) = khk^{-1} = h$ for all $h \in H$, so $kh = hk$ for all $h \in H$, hence $k \in C_K(H)$. Therefore, $C_K(H) = \ker\varphi$. ■

Exercise 5.5.2

Prove that $C_H(K) = N_H(K)$.

Solution. It is clear that $C_H(K) \leq N_H(K)$. Now let $h \in N_H(K)$. Then $hKh^{-1} = K$, so for any $k \in K$, we have $hkh^{-1} \in K$. Since $H \cap K = 1$, and $[h,k] = hkh^{-1}k^{-1} \in H \cap K$, we must have $[h,k] = 1$, so $hk = kh$ for all $k \in K$. Hence, $h \in C_H(K)$, so $N_H(K) \leq C_H(K)$. Therefore, $C_H(K) = N_H(K)$. ■

Exercise 5.5.3

In Example 1 following the proof of Proposition 5.11, prove that every element of $G - H$ has order 2. Prove that G is abelian if and only if $h^2 = 1$ for all $h \in H$.

Solution. Recall that $H \trianglelefteq G$. It is clear to see that $G/H = \{H, Hk\}$ for $k \notin H$, since H consists of elements hk with trivial k component. Then for any $hk \in Hk$, and noting the fact that $kh = h^{-1}k$ for all $h \in H$, we have

$$(hk)^2 = h(kh)k = h(h^{-1}k)k = kk = 1.$$

If $hk = 1$, then $h = k^{-1} \in H \cap K = 1$, so $hk = 1$ if and only if $h = k = 1$. Hence, every element of $G - H$ has order 2.

If G is abelian, then for any $h \in H$ and $k \in K$, we have $hk = kh$. Moreover, $kh = h^{-1}k$, hence $hk = h^{-1}k$, so $h^2 = 1$. Conversely, if $h^2 = 1$ for all $h \in H$, then any $h \in H$ and $k \in K$ commute, because $kh = h^{-1}k = hk$ by $h^2 = 1$. Then for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$, we have

$$(h_1k_1)(h_2k_2) = h_1(h_2k_1)k_2 = (h_2h_1)(k_2k_1) = (h_2k_2)(h_1k_1),$$

so G is abelian. ■

Exercise 5.5.4

Let $p = 2$ and check that the construction of the two non-abelian groups of order p^3 is valid in this case. Prove that *both* resulting groups are isomorphic to D_8.

Solution. Let $U = \langle u \rangle \cong Z_4$ and $V = \langle v \rangle \cong Z_2$. Then $\mathrm{Aut}(U) \cong Z_2$, so there is a unique nontrivial homomorphism $\varphi\colon V \to \mathrm{Aut}(U)$, which sends v to the automorphism of U that sends u to u^{-1}. Then the semidirect product $U \rtimes_\varphi V$ has order 8, and is generated by u and v with relations

$$u^4 = v^2 = 1, \quad vu = u^{-1}v.$$

It is clear that $U \rtimes_\varphi V$ is non-abelian, since $vu \neq uv$. Let $r = u$ and $s = v$. Then $r^4 = s^2 = 1$, and $sr = vu = u^{-1}v = r^{-1}s$, so $U \rtimes_\varphi V$ has the same presentation as D_8, hence $U \rtimes_\varphi V \cong D_8$.

Now let $W = \langle w \rangle \times \langle x \rangle \cong V_4$ and $Y = \langle y \rangle \cong Z_2$. Then $\mathrm{Aut}(W) \cong S_3$. Since S_3 contains 3 transpositions that are conjugate to each other, choose some $\varphi\colon Y \to \mathrm{Aut}(W)$ that sends y to a transposition in $\mathrm{Aut}(W)$. Then the semidirect product $W \rtimes_\varphi Y$ has order 8, and is generated by w, x, and y with relations

$$w^2 = x^2 = y^2 = 1, \quad yw = xy, \quad yx = wy.$$

It is clear that $W \rtimes_\varphi Y$ is non-abelian, since $yw \neq wy$. Let $r = yw$ and $s = y$. Then $s^2 = 1$,

$$r^4 = (r^2)^2 = ((yw)^2)^2 = (xyyw)^2 = (xw)^2 = x^2w^2 = 1,$$

and

$$sr = y(yw) = w = w^{-1} = w^{-1}y^{-1}y = (yw)^{-1}y = r^{-1}s,$$

so $W \rtimes_\varphi Y$ has the same presentation as D_8, hence $W \rtimes_\varphi Y \cong D_8$. ■

Exercise 5.5.5

Let $G = \mathrm{Hol}(Z_2 \times Z_2)$.
(a) Prove that $G = H \rtimes K$, where $H = Z_2 \times Z_2$ and $K \cong S_3$. Deduce that $|G| = 24$.
(b) Prove that G is isomorphic to S_4. [Obtain a homomorphism from G into S_4 by letting G act on the left cosets of K. Use Exercise 5.5.1 to show that this representation is faithful.]

Solution.
(a) Note that $\mathrm{Aut}(H) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ as it is a non-abelian group of order 6, by Exercise 4.2.10. It follows by definition that $G = H \rtimes K$, where $K \cong S_3$. Hence, $|G| = |H||K| = 4 \cdot 6 = 24$.
(b) Let G act on the left cosets of K in G. From $|G : K| = 4$, we have a homomorphism $\varphi\colon G \to S_4$. Moreover, we have some homomorphism $\psi\colon K \to \mathrm{Aut}(H)$ such that $G \cong H \rtimes_\psi K$. Lastly, we know from Theorem 4.3 that

$$\ker\varphi = \bigcap_{g\in G} gKg^{-1} \trianglelefteq G$$

such that $\ker\varphi \leq K$. Putting $N = \ker\varphi$, then $N = \{1, A_3, K\}$. If $N = K$, then $K \trianglelefteq G$, which is a contradiction since K is not normal in G because ψ is injective. If $N = A_3$, let $n \in N$ be a nonidentity element. Then $hnh^{-1} \in N$ for every h. However, Exercise 5.5.1 says that $\ker\psi = C_K(H)$. Since ψ is injective (an isomorphism, actually), $C_K(H) = 1$, so n does not commute with some $h_0 \in H$, i.e., $nh_0n^{-1} \neq h_0$. However, from $N \trianglelefteq G$, we know that $h_0nh_0^{-1} \in N$.

Observe that $h_0nh_0^{-1} = (h_0nh_0^{-1}n^{-1})n = [h_0, n]n$. Observe that $h_0(nh_0^{-1}n^{-1}) \in H$ by definition of the semidirect product, so $[h_0, n] \in H$. If $[h_0, n] = 1$, then $h_0nh_0^{-1} = n \in N$, contradicting our choice of h_0. Hence, $h_0nh_0^{-1}$ has nontrivial component in H, so $h_0nh_0^{-1} \notin N$, which is a contradiction. Therefore, $N = 1$, so φ is injective, hence $G \cong \varphi(G) \leq S_4$. Since $|G| = |S_4| = 24$, we have $G \cong S_4$. ■

Exercise 5.5.6

Assume that K is a cyclic group, H is an arbitrary group, and φ_1 and φ_2 are homomorphisms from K into $\mathrm{Aut}(H)$ such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite, assume φ_1 and φ_2 are injective. Prove, by constructing an explicit isomorphism, that

$$H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$$

(in particular, if the subgroups $\varphi_1(K)$ and $\varphi_2(K)$ are equal in $\mathrm{Aut}(H)$, then the resulting semidirect products are isomorphic). [Suppose $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$ so that for some $a \in \mathbb{Z}$ we have $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Show that the map

$$\psi\colon H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$$

defined by $\psi((h, k)) = (\sigma(h), k^a)$ is a homomorphism. Show ψ is bijective by constructing a 2-sided inverse.]

Solution. Let $K = \langle k\rangle$ and $\sigma \in \mathrm{Aut}(H)$ such that $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$. Then there exists some $a \in \mathbb{Z}$ such that $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Define the map

$$\psi\colon H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$$

by $\psi((h, k^m)) = (\sigma(h), k^{am})$ for all $h \in H$ and $m \in \mathbb{Z}$. Then for any $(h_1, k^s), (h_2, k^t) \in H \rtimes_{\varphi_1} K$, we have

$$\begin{aligned}
\psi((h_1, k^s)(h_2, k^t)) &= \psi((h_1\varphi_1(k^s)(h_2), k^{s+t})) \\
&= (\sigma(h_1\varphi_1(k^s)(h_2)), k^{a(s+t)}) \\
&= (\sigma(h_1)\sigma(\varphi_1(k^s)(h_2)), k^{as}k^{at}) \\
&= (\sigma(h_1)\varphi_2(k^{as})(\sigma(h_2)), k^{as}k^{at}) \\
&= (\sigma(h_1), k^{as})(\sigma(h_2), k^{at}) \\
&= \psi((h_1, k^s))\psi((h_2, k^t)),
\end{aligned}$$

so ψ is a homomorphism. To see that ψ is bijective, we split into two cases.

(1) Suppose K is infinite. By conjugate subgroups, we know that $\varphi_2(K) = \varphi_2(K^a)$, where $K^a = \{k^a \mid k \in K\}$. Since φ_2 is injective, $K^a = K$, forcing $a = \pm 1$. Then $\theta((h,k)) = (\sigma^{-1}(h), k^a)$ is a 2-sided inverse of ψ, so ψ is bijective.

(2) We first prove a lemma: if $m \mid n$, then the map defined by

$$\nu\colon (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times, \quad \nu(a) = a \pmod m$$

is a surjective homomorphism. We first check that ν is well defined: if $a \equiv b \pmod n$, then $n \mid (a-b)$, so $m \mid (a-b)$, hence $a \equiv b \pmod m$. Next, we check that ν is a homomorphism: for any $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have

$$\nu(ab) = ab \pmod m = (a \pmod m)(b \pmod m) = \nu(a)\nu(b).$$

Finally, we check that ν is surjective: let $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. If $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\nu(a) = a$. If $a \notin (\mathbb{Z}/n\mathbb{Z})^\times$, then $(a,n) \neq 1$. Let c be the product of primes that divide n but not a, let p be a prime that divides n, and put $b = a + cm$. We claim that $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ as follows:

- If $p \mid a$, then $p \nmid c$ by definition of c, hence $p \nmid b$.
- If $p \nmid a$, then $p \mid c$ by definition of c, hence $p \nmid b$.

Thus, $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, and $\nu(b) = b \pmod m = a + cm \pmod m = a$. Hence, ν is surjective.

Suppose $K \cong Z_n$ is finite. Let $|\varphi_1(K)| = |\varphi_2(K)| = m$, where $m \mid n$. Note that $\langle \varphi_1(k) \rangle = \varphi_1(K)$ and $\langle \varphi_2(k) \rangle = \varphi_2(K)$, so $|\varphi_1(k)| = |\varphi_2(k)| = m$. Moreover, $\langle \varphi_2(k)^a \rangle = \varphi_2(K)$, so $|\varphi_2(k)^a| = m$. It follows that $(a,m) = 1$.

Consider the surjective homomorphism $\nu\colon (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ defined in the lemma above. Since $(a,m) = 1$, we have $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, so there exists some $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\nu(b) = b \pmod m = a$. Then $\theta((h,k)) = (\sigma^{-1}(h), k^b)$ is a 2-sided inverse of ψ, so ψ is bijective. ∎

Exercise 5.5.7

This exercise describes thirteen isomorphism types of groups of order 56. (It is not too difficult to show that every group of order 56 is isomorphic to one of these.)

(a) Prove that there are three abelian groups of order 56.

(b) Prove that every group of order 56 has either a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.

(c) Construct the following non-abelian groups of order 56 which have a normal Sylow 7-subgroup and whose Sylow 2-subgroup S is as specified:
- one group when $S \cong Z_2 \times Z_2 \times Z_2$
- two nonisomorphic groups when $S \cong Z_4 \times Z_2$
- one group when $S \cong Z_8$
- two nonisomorphic groups when $S \cong Q_8$
- three nonisomorphic groups when $S \cong D_8$

[For a particular S, two groups are not isomorphic if the kernels of the maps from S into $\mathrm{Aut}(Z_7)$ are not isomorphic.]

(d) Let G be a group of order 56 with a nonnormal Sylow 7-subgroup. Prove that if S is the Sylow 2-subgroup of G then $S \cong Z_2 \times Z_2 \times Z_2$. [Let an element of order 7 act by conjugation on the seven nonidentity elements of S and deduce that they all have the same order.]

(e) Prove that there is a unique group of order 56 with a nonnormal Sylow 7-subgroup. [For existence use the fact that $|GL_3(\mathbb{F}_2)| = 168$; for uniqueness use Exercise 5.5.6.]

Solution.

(a) Note that $56 = 2^3 \cdot 7$. By the Fundamental Theorem of Finite abelian Groups, the partitions of 3 are $3, 2+1, 1+1+1$, so the abelian groups of order 56 are of the form $Z_8 \times Z_7$, $Z_4 \times Z_2 \times Z_7$, and $Z_2 \times Z_2 \times Z_2 \times Z_7$.

(b) Let n_7 be the number of Sylow 7-subgroups of G. Then $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 2^3$, so $n_7 = 1$ or 8. If $n_7 = 1$, then the unique Sylow 7-subgroup is normal. Suppose $n_7 = 8$. Then there are $8 \cdot 6 = 48$ elements of order 7 in G, so the remaining $56 - 48 = 8$ elements of G must be the identity and the elements of a Sylow 2-subgroup. Hence, the Sylow 2-subgroup is unique, so it is normal.

(c) Let $P \in \mathrm{Syl}_7(G)$ such that $P \trianglelefteq G$. Then $P = \langle p \rangle \cong Z_7$, and $\mathrm{Aut}(P) \cong Z_6$.
- If $S \cong Z_2 \times Z_2 \times Z_2$, put $S = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$. Let $\varphi\colon S \to \mathrm{Aut}(P)$ be a homomorphism. We disregard a, b, c being sent to id as that is the trivial homomorphism. Since a, b, c have order 2, they can only be sent to elements of order 1 or 2 in $\mathrm{Aut}(P)$. Put $\alpha \in \mathrm{Aut}(P)$ such that $|\alpha| = 2$, where α is unique since $\mathrm{Aut}(P)$ is cyclic. Then we have the following nontrivial homomorphisms:

$$\varphi_1 = \begin{cases} a \mapsto \alpha, \\ b \mapsto \mathrm{id}, \\ c \mapsto \mathrm{id}, \end{cases} \qquad \varphi_2 = \begin{cases} a \mapsto \alpha, \\ b \mapsto \alpha, \\ c \mapsto \mathrm{id}, \end{cases} \qquad \varphi_3 = \begin{cases} a \mapsto \alpha, \\ b \mapsto \alpha, \\ c \mapsto \alpha, \end{cases}$$

Note that $\ker\varphi_1 = \langle b\rangle \times \langle c\rangle$, $\ker\varphi_2 = \langle ab, c\rangle$, and $\ker\varphi_3 = \langle ab, ac\rangle$. Note that these are all isomorphic to V_4, hence the resulting semidirect products are isomorphic by Exercise 5.5.6. Without loss of generality, consider φ_1. Then a acts on P by sending p to the inversion automorphism of P, or $apa^{-1} = p^{-1}$. It is clear that b and c centralize P and commute with a. Observe that $\langle p, a \mid apa^{-1} = p^{-1}, a^2 = p^7 = 1\rangle \cong D_{14}$ and has trivial intersection with $\langle b\rangle \times \langle c\rangle$, so

$$G \cong P \rtimes_{\varphi_1} S \cong D_{14} \times Z_2 \times Z_2.$$

- Put $S = Z_4 \times Z_2 \cong \langle a\rangle \times \langle b\rangle$. Let $\alpha \in \mathrm{Aut}(P)$ be the unique element of order 2 again. Then we have the following nontrivial homomorphisms:

$$\varphi_1 = \begin{cases} a \mapsto \alpha, \\ b \mapsto \mathrm{id}, \end{cases} \qquad \varphi_2 = \begin{cases} a \mapsto \mathrm{id}, \\ b \mapsto \alpha, \end{cases} \qquad \varphi_3 = \begin{cases} a \mapsto \alpha, \\ b \mapsto \alpha, \end{cases}$$

We have $\ker\varphi_1 = \langle a^2\rangle \times \langle b\rangle$, $\ker\varphi_2 = \langle a\rangle$, and $\ker\varphi_3 = \langle ab\rangle$, where $|ab| = 4$. Note that $\ker\varphi_1 \cong V_4$, while $\ker\varphi_2 \cong \ker\varphi_3 \cong Z_4$. We may consider φ_2 first. Then b acts on P by sending p to the inversion automorphism of P, or $bpb^{-1} = p^{-1}$. It is clear that a centralizes P and commutes with b. Observe that $\langle p, b \mid bpb^{-1} = p^{-1}, b^2 = p^7 = 1\rangle \cong D_{14}$ and has trivial intersection with $\langle a\rangle$, so

$$G \cong P \rtimes_{\varphi_2} S \cong D_{14} \times Z_4.$$

For φ_1, we see that $\langle b\rangle$ centralizes P, and a acts on P by sending p to the inversion automorphism of P. Moreover, consider the subgroup $P_0 = \langle p, a \mid apa^{-1} = p^{-1}, a^4 = p^7 = 1\rangle$. It is easy to see that $P \cap \langle a\rangle = 1$, so $|P_0| = |P||\langle a\rangle| = 28$. Moreover, $pPp^{-1} = P$, and $aPa^{-1} = P$ since $apa^{-1} = p^{-1}$ under the action of φ_1 restricted to $\langle a\rangle$. Hence, $P_0 \cong Z_7 \rtimes Z_4$. It is clear that P_0 is normal in G, and $\langle b\rangle$ centralizes P_0, so

$$G \cong P \rtimes_{\varphi_1} S \cong (Z_7 \rtimes Z_4) \times Z_2.$$

- For $S \cong Z_8$, let $S = \langle s\rangle$. Since $\mathrm{Aut}(P) \cong Z_6$, and $(8, 6) = 2$, the only nontrivial homomorphism $\varphi\colon S \to \mathrm{Aut}(P)$ is the one that sends s to the inversion automorphism α of P. Moreover, cyclicity of S guarantees uniqueness of the homomorphism. Then $sps^{-1} = p^{-1}$, and

$$G \cong P \rtimes_{\varphi} S \cong Z_7 \rtimes Z_8.$$

- Let $S \cong Q_8 = \langle i, j\rangle = \{1, i, i^2, i^3, j, ij, i^2j, i^3j\}$. If we consider the trivial homomorphism, then $G \cong P \times S \cong Z_7 \times Q_8$. Now consider the nontrivial homomorphism that sends some generator of S to α. We have three cases:

$$\varphi_1 = \begin{cases} i \mapsto \alpha, \\ j \mapsto \mathrm{id}, \end{cases} \qquad \varphi_2 = \begin{cases} i \mapsto \mathrm{id}, \\ j \mapsto \alpha, \end{cases} \qquad \varphi_3 = \begin{cases} i \mapsto \alpha, \\ j \mapsto \alpha, \end{cases}$$

We have $\ker\varphi_1 = \langle j\rangle$, $\ker\varphi_2 = \langle i\rangle$, and $\ker\varphi_3 = \langle ij\rangle$. These are all isomorphic to Z_4, so the semidirect products will be isomorphic to each other. Pick φ_1 without loss of generality. Then i acts on P, and $ipi^{-1} = p^{-1}$. Unlike the other cases, j does not centralize P, since $jij^{-1} = i^{-1}$, so $jpj^{-1} = p^{-1}$. Hence, we have

$$G \cong P \rtimes_{\varphi_1} S \cong Z_7 \rtimes Q_8 = \{p, i, j \mid i^4 = j^4 = 1, i^2 = j^2, iji^{-1} = j^{-1}, iji^{-1} = jpj^{-1} = p^{-1}\}$$

Note that nontriviality of the homomorphism implies that some $s \in S$ does not centralize P. If G could be written as a direct product, then S would centralize P, which is a contradiction. Hence, G is not a direct product.

- Let $S \cong D_8 = \langle r, s\rangle = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$. If we consider the trivial homomorphism, then $G \cong P \times S \cong Z_7 \times D_8$. Now consider the nontrivial homomorphism that sends some generator of S to α. We have three cases:

$$\varphi_1 = \begin{cases} r \mapsto \alpha, \\ s \mapsto \mathrm{id}, \end{cases} \qquad \varphi_2 = \begin{cases} r \mapsto \mathrm{id}, \\ s \mapsto \alpha, \end{cases} \qquad \varphi_3 = \begin{cases} r \mapsto \alpha, \\ s \mapsto \alpha, \end{cases}$$

We have $\ker\varphi_1 = \langle r^2, s\rangle$, $\ker\varphi_2 = \langle r\rangle$, and $\ker\varphi_3 = \langle sr, r^2\rangle$. Then $\ker\varphi_1 \cong \ker\varphi_3 \cong V_4$, while $\ker\varphi_2 \cong Z_4$. Hence, the semidirect products corresponding to φ_1 and φ_3 are isomorphic to each other, but not to the semidirect product corresponding to φ_2. Pick φ_1 without loss of generality. Then r acts on P, and $rpr^{-1} = p^{-1}$. Moreover, s centralizes P, hence

$$G \cong P \rtimes_{\varphi_1} S \cong Z_7 \rtimes D_8 = \{p, r, s \mid p^7 = r^4 = s^2 = 1, srs^{-1} = r^{-1}, rpr^{-1} = p^{-1}\}.$$

If we pick φ_2, then s acts on P, and $sps^{-1} = p^{-1}$. Moreover, note that r centralizes P, hence $|rp| = 28$. Since $s(rp)s = srps^{-1} = (srs^{-1})(sps^{-1}) = r^{-1}p^{-1} = (rp)^{-1}$,

$$G \cong P \rtimes_{\varphi_2} S \cong D_{56}.$$

(d) Suppose G has a nonnormal Sylow 7-subgroup. We know that $S \in \mathrm{Syl}_2(G)$ must be normal by part (b). Let $P \in \mathrm{Syl}_7(G)$, and put $P = \langle p \rangle$. Let p act by conjugation on the seven nonidentity elements of S. Note that the stabilizer of any nonidentity element $s \in S$ is a subgroup of P, hence $|G_s| = 1$ or 7. If $|G_s| = 7$, then the orbit is trivial, hence $psp^{-1} = s$, or $p = sps^{-1} \in P$, which contradicts that $|s|$ is a power of 2. Then $|G_s| = 1$, so the orbit $\mathcal{O}_s$ of s has size 7. Since $|S - 1| = 7$, $\mathcal{O}_s$ contains all nonidentity elements of S. Hence, all nonidentity elements of S have the same order.

If they all had order 8, then s^2 would have order 4, but $(s^2)^4 = s^8 = 1$. A similar reasoning eliminates the possibility of order 4. Hence, all nonidentity elements of S have order 2, so $S \cong Z_2 \times Z_2 \times Z_2$.

(e) Let $H = Z_2 \times Z_2 \times Z_2$ and $K = \langle k \rangle \cong Z_7$. Then $\mathrm{Aut}(H) \cong \mathrm{GL}_3(\mathbb{F}_2)$, which has order 168. Let $\varphi \colon K \to \mathrm{Aut}(H)$ be a homomorphism. Since $|K| = 7$, $|\varphi(K)| = 1$ or 7. If $|\varphi(K)| = 1$, then the resulting semidirect product is abelian, which is a contradiction. Hence, $|\varphi(K)| = 7$. Since $\mathrm{Aut}(H)$ has order 168, there exists a unique subgroup of order 7 in $\mathrm{Aut}(H)$, call it ψ. Then $\varphi \colon K \to \mathrm{Aut}(H)$ given by $\varphi(k) = \psi$ is a homomorphism, and the resulting semidirect product $H \rtimes_\varphi K$ has order $|H||K| = 8 \cdot 7 = 56$. We now claim that K is not normal in $H \rtimes_\varphi K$.

If $K \trianglelefteq G$, then $[s, k] \in K$ for all $s \in S$. Moreover, $[s, k] \in S$ since $S \trianglelefteq G$. Hence, $[s, k] \in S \cap K = 1$, so $[s, k] = 1$, or $sk = ks$ for all $s \in S$. Then $\varphi(k) = \mathrm{id}$, which is a contradiction. Hence, K is not normal in $H \rtimes_\varphi K$.

To see that $H \rtimes_\varphi K$ is unique, let $\varphi_1, \varphi_2 \colon K \to \mathrm{Aut}(H)$ be two homomorphisms such that $|\varphi_1(K)| = |\varphi_2(K)| = 7$. Then $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. Since $|\mathrm{Aut}(H) = 2^3 \cdot 3 \cdot 7$, $\varphi_1(K), \varphi_2(K) \in \mathrm{Syl}_7(\mathrm{Aut}(H))$, so they are conjugate by the Sylow theorems. Hence, by Exercise 5.5.6, we have $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$. Therefore, $H \rtimes_\varphi K$ is unique. ■

Exercise 5.5.8

Construct a non-abelian group of order 75. Classify all groups of order 75 (there are three of them). [Use Exercise 5.5.6 to show that the non-abelian group is unique.] (The classification of groups of order pq^2, where p and q are primes with $p < q$ and p not dividing $q - 1$, is quite similar.)

Solution. Let $P \in \mathrm{Syl}_5(G)$ and $Q \in \mathrm{Syl}_3(G)$. Then $|P| = 25$ and $|Q| = 3$. By the Sylow theorems, we have $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 3$, so $n_5 = 1$ or 3. If $n_5 = 1$, then the unique Sylow 5-subgroup is normal. If $n_5 = 3$, then there are $3 \cdot 24 = 72$ elements of order 5 in G, so the remaining $75 - 72 = 3$ elements of G must be the identity and the elements of a Sylow 3-subgroup. Hence, the Sylow 3-subgroup is unique, so it is normal. In either case, we have a normal Sylow subgroup, so $G \cong P \rtimes Q$ or $G \cong Q \rtimes P$. Moreover, $P \cong Z_{25}$ or $Z_5 \times Z_5$, and $Q \cong Z_3$. We then have two cases to consider:

- Suppose $P \cong Z_{25}$. Then $\mathrm{Aut}(P) \cong (\mathbb{Z}/25\mathbb{Z})^\times$, which has order 20. Since $|Q| = 3$, the only homomorphism $\varphi \colon Q \to \mathrm{Aut}(P)$ is the trivial homomorphism, so $G \cong P \rtimes Q \cong P \times Q \cong Z_{25} \times Z_3$.

  If we consider $G \cong Q \rtimes P$, then we have a homomorphism $\varphi \colon P \to \mathrm{Aut}(Q)$. Since $|\mathrm{Aut}(Q)| = 2$, the only homomorphism $\varphi \colon P \to \mathrm{Aut}(Q)$ is the trivial homomorphism, so $G \cong Q \rtimes P \cong Q \times P \cong Z_3 \times Z_{25}$.
- Suppose $P \cong Z_5 \times Z_5$ with $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{F}_5)$, which has order 480. Since $|Q| = 3$, there exists a nontrivial homomorphism $\varphi \colon Q \to \mathrm{Aut}(P)$, which is unique since $|\mathrm{Aut}(P)| = 480$ and $(480, 3) = 3$. We may use similar reasoning as the previous exercise in that $\varphi_1(Q)$ and $\varphi_2(Q)$ are conjugate subgroups of $\mathrm{Aut}(P)$, and $\varphi_1(Q), \varphi_2(Q) \in \mathrm{Syl}_3(\mathrm{Aut}(P))$, so they are conjugate by the Sylow theorems. Hence, by Exercise 5.5.6, we have $P \rtimes_{\varphi_1} Q \cong P \rtimes_{\varphi_2} Q$. Therefore, $P \rtimes_\varphi Q$ is unique, and $G \cong P \rtimes_\varphi Q$ is non-abelian.

  If we consider $G \cong Q \rtimes P$, then we have a homomorphism $\varphi \colon P \to \mathrm{Aut}(Q)$. Since $|\mathrm{Aut}(Q)| = 2$, the only homomorphism $\varphi \colon P \to \mathrm{Aut}(Q)$ is the trivial homomorphism, so $G \cong Q \rtimes P \cong Q \times P \cong Z_3 \times (Z_5 \times Z_5)$.

■

Exercise 5.5.9

Show that the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}$$

is an element of order 5 in $\mathrm{GL}_2(\mathbb{F}_{19})$. Use this matrix to construct a non-abelian group of order 1805, and give a presentation of this group. Classify groups of order 1805 (there are three isomorphism types). [Use Exercise 5.5.6 to prove uniqueness of the non-abelian group.] (A general method for finding elements of prime order in $\mathrm{GL}_n(\mathbb{F}_p)$ is described in the exercises in Section 12.2; this particular matrix of order 5 in $\mathrm{GL}_2(\mathbb{F}_{19})$ appears in **??** of that section as an illustration of the method.)

Solution. Let M be the given matrix. It is easy to calculate that

$$M^5 = \begin{pmatrix} -56 & -209 \\ 209 & 780 \end{pmatrix},$$

where, once entries are taken mod 19, results in I_2, hence $|M| = 5$. Moreover, we know that $1805 = 19^2 \cdot 5$. Since $n_{19} \equiv 1 \pmod{1}9$ and $n_{19} \mid 5$, $n_{19} = 1$, so $P \in \mathrm{Syl}_{19}(G)$ is normal. Moreover, we have $P \cong Z_{361}$ or $P \cong Z_{19} \times Z_{19}$. If $P \cong Z_{361}$, then $\mathrm{Aut}(P) \cong (\mathbb{Z}/361\mathbb{Z})^\times$, which has order $19 \cdot 18 = 342$. Since $|Q| = 5$, the only homomorphism $\varphi \colon Q \to \mathrm{Aut}(P)$ is the trivial homomorphism, so $G \cong P \rtimes Q \cong P \times Q \cong Z_{361} \times Z_5$.

If $P \cong Z_{19} \times Z_{19}$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{F}_{19})$, which has order 123120. If we take φ to be the trivial homomorphism, then $G \cong Z_{19} \times Z_{19} \times Z_5$. Now, since $|Q| = 5$, there exists a nontrivial homomorphism $\varphi \colon Q \to \mathrm{Aut}(P)$, which is unique since $|\mathrm{Aut}(P)| = 123120$ and $(123120, 5) = 5$. We may use similar reasoning as the previous exercise in that $\varphi_1(Q)$ and $\varphi_2(Q)$ are conjugate subgroups of $\mathrm{Aut}(P)$, and $\varphi_1(Q), \varphi_2(Q) \in \mathrm{Syl}_5(\mathrm{Aut}(P))$, so they are conjugate by the Sylow theorems. Hence, by Exercise 5.5.6, we have $P \rtimes_{\varphi_1} Q \cong P \rtimes_{\varphi_2} Q$. Therefore, $P \rtimes_\varphi Q$ is unique, and $G \cong P \rtimes_\varphi Q$ is non-abelian. ■

Exercise 5.5.10

This exercise classifies the groups of order 147 (there are six isomorphism types).

(a) Prove that there are two abelian groups of order 147.

(b) Prove that every group of order 147 has a normal Sylow 7-subgroup.

(c) Prove that there is a unique non-abelian group of order 147 whose Sylow 7-subgroup is cyclic.

(d) Let

$$t_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad t_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

be elements of $\mathrm{GL}_2(\mathbb{F}_7)$. Prove $P = \langle t_1, t_2 \rangle$ is a Sylow 3-subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$, and that $P \cong Z_3 \times Z_3$. Deduce that every subgroup of order 3 is conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to a subgroup of P.

(e) From example 3 in Section 1, the group P has four subgroups of order 3, and these are: $P_1 = \langle t_1 \rangle, P_2 = \langle t_2 \rangle, P_3 = \langle t_1 t_2 \rangle$, and $P_4 = \langle t_1 t_2^2 \rangle$. For $i = 1, 2, 3, 4$, let $G_i = (Z_7 \times Z_7) \rtimes_{\varphi_i} P_i$, where φ_i is an isomorphism of Z_3 with the subgroup P_i of $\mathrm{Aut}(Z_7 \times Z_7)$. For each i, describe G_i in terms of generators and relations. Deduce that $G_1 \cong G_2$.

(f) Prove that G_1 is not isomorphic to either G_3 or G_4. [Show that the center of G_1 has order 7, whereas the centers of G_3 and G_4 are trivial.]

(g) Prove that G_3 is not isomorphic to G_4.

(h) Classify the groups of order 147 by showing that the six nonisomorphic groups described above (two from part (a), one from part (c), and G_1, G_3, and G_4) are all the groups of order 147. [Use Exercise 5.5.6 and part (d).] (The classification of groups of order pq^2, where p and q are primes with $p < q$ and $p \mid q - 1$, is quite similar.)

Solution.

(a) Note that $147 = 3 \cdot 7^2$. By the Fundamental Theorem of Finite abelian Groups, the partitions of 2 are $2, 1 + 1$, so the abelian groups of order 147 are of the form $Z_{49} \times Z_3$ and $Z_7 \times Z_7 \times Z_3$.

(b) Let n_7 be the number of Sylow 7-subgroups of G. Then $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 3$, so $n_7 = 1$. Hence, the unique Sylow 7-subgroup is normal.

(c) Let $P \cong Z_{49}$ and $Q \cong Z_3$. Then $\mathrm{Aut}(P) \cong (\mathbb{Z}/49\mathbb{Z})^\times$, which has order $7 \cdot 6 = 42$. Since $|Q| = 3$, there exists nontrivial homomorphisms $\varphi \colon Q \to \mathrm{Aut}(P)$, where $q \in Q = \langle q \rangle$ is mapped to a generator of the unique subgroup of order 3 in $\mathrm{Aut}(P)$, say α. Then either $q \mapsto \alpha$ or $q \mapsto \alpha^2$. Let $\varphi_1, \varphi_2 \colon Q \to \mathrm{Aut}(P)$ be the two homomorphisms defined by $\varphi_1(q) = \alpha$ and $\varphi_2(q) = \alpha^2$. Since $\varphi_1(Q) = \varphi_2(Q) = \langle \alpha \rangle$, by Exercise 5.5.6, we have $P \rtimes_{\varphi_1} Q \cong P \rtimes_{\varphi_2} Q$. Hence, there is a unique non-abelian group of order 147 whose Sylow 7-subgroup is cyclic.

(d) Recall that $|\mathrm{GL}_2(\mathbb{F}_7)| = (7^2 - 1)(7^2 - 7) = 48 \cdot 42 = 2016 = 2^5 \cdot 3^2 \cdot 7$. Observe that

$$t_1^3 = \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}, \quad t_2^3 = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}, \quad t_1 t_2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = t_2 t_1.$$

Taking entries mod 7, then $t_1^3 = t_2^3 = I_2$, so $|t_1| = |t_2| = 3$. Moreover, $t_1 t_2 = t_2 t_1$, so $P = \langle t_1 \rangle \langle t_2 \rangle$. To see that this is isomorphic to $\langle t_1 \rangle \times \langle t_2 \rangle$, note that $\langle t_1 \rangle \cap \langle t_2 \rangle = 1$. Moreover, commutativity shows that $t_1 \trianglelefteq P$ and $t_2 \trianglelefteq P$, so $P \cong \langle t_1 \rangle \times \langle t_2 \rangle \cong Z_3 \times Z_3$. Since $|P| = 9$, P is a Sylow 3-subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$.

Let R be a subgroup of order 3 in $\mathrm{GL}_2(\mathbb{F}_7)$. Then $R \leq gPg^{-1}$ for some $g \in \mathrm{GL}_2(\mathbb{F}_7)$ by the Sylow theorems. Then $gRg^{-1} \leq P$, so gRg^{-1} is a subgroup of order 3 in P. Hence, every subgroup of order 3 is conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to a subgroup of P.

(e) Let $Z_7 \times Z_7 = \langle a \rangle \times \langle b \rangle$. Then $\mathrm{Aut}(Z_7 \times Z_7) \cong \mathrm{GL}_2(\mathbb{F}_7)$, and P_i is a subgroup of $\mathrm{Aut}(Z_7 \times Z_7)$ for $i = 1, 2, 3, 4$. Let $\varphi_i \colon Z_3 \to P_i$ be an isomorphism. We check each i:

- For $i = 1$, we have $\varphi_1 \colon Z_3 \to P_1$ given by $\varphi_1(q) = t_1$. Then $qaq^{-1} = \varphi_1(q)(a) = t_1(a) = a^2$, and $qbq^{-1} = \varphi_1(q)(b) = t_1(b) = b$. Hence, we have for a naïve presentation of G_1:

$$G_1 = \{a, b, q \mid a^7 = b^7 = q^3 = 1, ab = ba, qaq^{-1} = a^2, qbq^{-1} = b\}.$$

However, note that b is central in G_1 as it commutes with both a and q. It follows that $\langle b\rangle \trianglelefteq G_1$ with $|\langle b\rangle| = 7$. Observe that $\langle b\rangle \cap \langle a, q\rangle = 1$ by construction. To see that $\langle a, q\rangle \trianglelefteq G_1$, observe that $b\langle a, q\rangle b^{-1} = \langle a, q\rangle$ because $b \in Z(G_1)$. Then $G_1 \cong Z_7 \times \langle a, q\rangle$.

If we consider a homomorphism $\psi\colon Z_3 \to \mathrm{Aut}(Z_7)$, then $q \mapsto \alpha$ or $q \mapsto \alpha^2$ such that α generates the unique subgroup of order 3 in $\mathrm{Aut}(Z_7)$. In either case, we have $\langle a, q\rangle \cong Z_7 \rtimes_\psi Z_3$ as it satisfies the relations $qaq^{-1} = a^2$ in the naïve presentation. Hence, we have

$$G_1 \cong Z_7 \times (Z_7 \rtimes_\psi Z_3).$$

- For $i = 2$, simply note that t_2 takes the place of t_1 in the previous case, $aq = qa$, and $qbq^{-1} = b^2$. Hence, we have
$$G_2 = \{a, b, q \mid a^7 = b^7 = q^3 = 1, ab = ba, qaq^{-1} = a, qbq^{-1} = b^2\}.$$
By similar reasoning as the previous case, we have $G_2 \cong Z_7 \times (Z_7 \rtimes_\psi Z_3)$, so $G_1 \cong G_2$.
- For $i = 3$, we have $\varphi_3\colon Z_3 \to P_3$ given by $\varphi_3(q) = t_1t_2$. Then $qaq^{-1} = \varphi_3(q)(a) = t_1t_2(a) = t_1(a) = a^2$, and $qbq^{-1} = \varphi_3(q)(b) = t_1t_2(b) = t_1(b^2) = b^2$. A presentation of G_3 is
$$G_3 = \{a, b, q \mid a^7 = b^7 = q^3 = 1, ab = ba, qaq^{-1} = a^2, qbq^{-1} = b^2\}.$$
- For $i = 4$, we have $\varphi_4\colon Z_3 \to P_4$ given by $\varphi_4(q) = t_1t_2^2$. Then $qaq^{-1} = \varphi_4(q)(a) = t_1t_2^2(a) = t_1(a) = a^2$, and $qbq^{-1} = \varphi_4(q)(b) = t_1t_2^2(b) = t_1(b^4) = b^4$. Then a presentation of G_4 is
$$G_4 = \{a, b, q \mid a^7 = b^7 = q^3 = 1, ab = ba, qaq^{-1} = a^2, qbq^{-1} = b^4\}.$$

(f) The prior discussion showed that $Z(G_1) = \langle b\rangle$, so $|Z(G_1)| = 7$. Now, consider G_3, and let $z \in Z(G_3)$. We first consider when $z \in Z(G_3) \cap (\langle a\rangle \times \langle b\rangle)$. Then $z = a^ib^j$ for some $0 \le i, j \le 6$. Since z commutes with q,

$$a^ib^j = z = qzq^{-1} = qa^ib^jq^{-1} = qaq^{-1}qbq^{-1} = a^{2i}b^{2j}.$$

Then this implies that $2i \equiv i \pmod 7$ and $2j \equiv j \pmod 7$, so $i = j = 0$. Hence, $Z(G_3) \cap (\langle a\rangle \times \langle b\rangle) = 1$. Now, consider when $z \in Z(G_3) - (\langle a\rangle \times \langle b\rangle)$. Then $z = a^ib^jq^k$ for some $0 \le i, j \le 6$ and $1 \le k \le 2$. Since z commutes with a,

$$a^ib^jq^k = z = aza^{-1} = aa^ib^jq^ka^{-1} = a^{i+1}b^jq^ka^{-1} = a^{i+1}b^jq^ka^{-1}.$$

However, since q does not centralize $\langle a\rangle$, this is a contradiction. Hence, $Z(G_3) - (\langle a\rangle \times \langle b\rangle) = 1$, so $Z(G_3) = 1$. A similar argument shows that $Z(G_4) = 1$.

(g) To show that $G_3 \ncong G_4$, we first observe that G_3 and G_4 have the same subgroups of order 7, since $Z_7 \times Z_7$ is the unique Sylow 7-subgroup of both groups. Hence, G_3 and G_4 have the list of subgroups

$$\mathcal{S} = \{\langle a\rangle, \langle b\rangle, \langle ab\rangle, \langle ab^2\rangle, \langle ab^3\rangle, \langle ab^4\rangle, \langle ab^5\rangle, \langle ab^6\rangle\}.$$

Let q act on $\mathcal{S}$ by conjugation. In G_3, for any $\langle ab^i\rangle \in \mathcal{S}$, then

$$q(ab^i)q^{-1} = (qaq^{-1})(qb^iq^{-1}) = a^2b^{2i}.$$

It is clear that $a^2b^{2i} \in \langle ab^i\rangle$, so q stabilizes $\langle ab^i\rangle$. Hence, q stabilizes all subgroups of order 7 in G_3, and each subgroup of order 7 is normal in G_3. In G_4, consider $\langle ab\rangle \in \mathcal{S}$. Then

$$q(ab)q^{-1} = (qaq^{-1})(qbq^{-1}) = a^2b^4 \notin \langle ab\rangle,$$

so q does not stabilize $\langle ab\rangle$. Hence, $\langle ab\rangle$ is not normal in G_4. Since G_3 and G_4 have different numbers of normal subgroups of order 7, $G_3 \ncong G_4$.

(h) By part (b), every group of order 147 has a normal Sylow 7-subgroup. Let $P \in \mathrm{Syl}_7(G)$ and $Q \in \mathrm{Syl}_3(G)$. Since $P \cap Q = 1$ because $(49, 3) = 1$, and $|G| = |P||Q|$, $G = PQ$, and $G \cong P \rtimes Q$. If the homomorphism is trivial, then we have the two abelian groups from part (a). If the homomorphism is nontrivial and P is cyclic, then we have the unique non-abelian group from part (c). If the homomorphism is nontrivial and P is not cyclic, then $\varphi(Q)$ is a subgroup of order 3 in $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{F}_7)$. By part (d), every subgroup of order 3 is conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to a subgroup of P, so by Exercise 5.5.6 we have the three non-abelian groups G_1, G_3, and G_4 from part (e). Hence, the six nonisomorphic groups described above are all the groups of order 147. ■

Exercise 5.5.11

Classify groups of order 28 (there are four isomorphism types).

Solution. Note $28 = 2^2 \cdot 7$. We have the abelian groups $Z_7 \times Z_4$ and $Z_7 \times Z_2 \times Z_2$. Let $P \in \mathrm{Syl}_7(G)$ and $S \in \mathrm{Syl}_2(G)$. Then $|P| = 7$ and $|S| = 4$. By the Sylow theorems, we have $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 4$, so $n_7 = 1$. Hence, the unique Sylow 7-subgroup is normal. Moreover, we have $P \cong Z_7$ and $S \cong Z_4$ or $Z_2 \times Z_2$. We then have two cases to consider:

- Suppose $S \cong Z_4 = \langle s \rangle$. If we consider the trivial homomorphism, then $G \cong P \times S \cong Z_7 \times Z_4$. Now consider the nontrivial homomorphism that sends s to α, a generator of the unique subgroup of order 2 in $\mathrm{Aut}(P)$. Then s acts on P, and $sps^{-1} = p^{-1}$. Hence, we have
$$G \cong P \rtimes S \cong Z_7 \rtimes Z_4 = \{p, s \mid p^7 = s^4 = 1, sps^{-1} = p^{-1}\}.$$
- Suppose $S \cong Z_2 \times Z_2 = \langle s \rangle \times \langle t \rangle$. If we consider the trivial homomorphism, then $G \cong P \times S \cong Z_7 \times (Z_2 \times Z_2)$. Now consider a nontrivial homomorphism that sends some generator of S to α. We have the three homomorphisms
$$\theta_1 = \begin{cases} s \mapsto \alpha, \\ t \mapsto \mathrm{id}, \end{cases} \qquad \theta_2 = \begin{cases} s \mapsto \mathrm{id}, \\ t \mapsto \alpha, \end{cases} \qquad \theta_3 = \begin{cases} s \mapsto \alpha, \\ t \mapsto \alpha, \end{cases}$$
Observe that $\ker \theta_1 = \langle t \rangle$, $\ker \theta_2 = \langle s \rangle$, and $\ker \theta_3 = \langle st \rangle$. Hence, the semidirect products corresponding to θ_1, θ_2, and θ_3 are all isomorphic to each other. Pick θ_1 without loss of generality. Then s acts on P, and $sps^{-1} = p^{-1}$. Moreover, t centralizes P, hence $|tp| = 14$. Since
$$s(tp)s^{-1} = stps^{-1} = (sts^{-1})(sps^{-1}) = tp^{-1} = (tp)^{-1},$$
then
$$G \cong P \rtimes_{\theta_1} S \cong \{p, s, t \mid p^7 = s^2 = t^2 = 1, st = ts, sps^{-1} = p^{-1}, tpt^{-1} = p\} \cong D_{28}.$$ ■

Exercise 5.5.12

Classify the groups of order 20 (there are five isomorphism types).

Solution. We have the abelian groups $Z_5 \times Z_4$ and $Z_5 \times Z_2 \times Z_2$. Let $P \in \mathrm{Syl}_5(G)$ and $S \in \mathrm{Syl}_2(G)$. Then $|P| = 5$ and $|S| = 4$. By the Sylow theorems, we have $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 4$, so $n_5 = 1$. Hence, the unique Sylow 5-subgroup is normal. Moreover, we have $P \cong Z_5$ and $S \cong Z_4$ or $Z_2 \times Z_2$. We then have two cases to consider:

- If $S \cong Z_4 = \langle s \rangle$, then s has four candidates to be sent to: $\mathrm{id}, \alpha, \alpha^2$, or α^3, where $\mathrm{Aut}(Z_5) = \langle \alpha \rangle$. Define the homomorphisms
$$\varphi_1 \colon s \mapsto \mathrm{id}, \quad \varphi_2 \colon s \mapsto \alpha, \quad \varphi_3 \colon s \mapsto \alpha^2, \quad \varphi_4 \colon s \mapsto \alpha^3$$
Since φ_1 is trivial, $G \cong P \rtimes_{\varphi_1} S \cong P \times S \cong Z_5 \times Z_4$. Also observe that $\ker \varphi_2 = \ker \varphi_4 = 1$ while $\ker \varphi_3 = \langle s^2 \rangle$. Then the resulting semidirect products from φ_2 and φ_4 are isomorphic, since $\varphi_2(S) = \varphi_4(S) = \langle \alpha \rangle$, so by Exercise 5.5.6, we have $P \rtimes_{\varphi_2} S \cong P \rtimes_{\varphi_4} S$. Moreover, $\ker \varphi_3 = \langle s^2 \rangle$, which is the unique subgroup of order 2 in $\mathrm{Aut}(P)$, so $P \rtimes_{\varphi_3} S$ is not isomorphic to $P \rtimes_{\varphi_2} S$. Hence, we have two non-abelian groups of order 20, and we have
$$G \cong P \rtimes_{\varphi_2} S \cong \{p, s \mid p^5 = s^4 = 1, sps^{-1} = p^2\} \cong F_{20}.$$
In the case of φ_3, we have $sps^{-1} = p^{-1}$. Then
$$G \cong P \rtimes_{\varphi_3} S \cong \{p, s \mid p^5 = s^4 = 1, sps^{-1} = p^{-1}\} \cong Z_5 \rtimes Z_4.$$
- If $S \cong Z_2 \times Z_2 = \langle s \rangle \times \langle t \rangle$, then we have the trivial homomorphism $\theta_1 \colon S \to \mathrm{Aut}(P)$, which gives $G \cong P \rtimes_{\theta_1} S \cong P \times S \cong Z_5 \times (Z_2 \times Z_2)$. If α^2 is the generator of the unique subgroup of order 2 in $\mathrm{Aut}(P)$, then we have the three nontrivial homomorphisms
$$\theta_2 = \begin{cases} s \mapsto \alpha^2, \\ t \mapsto \mathrm{id}, \end{cases} \qquad \theta_3 = \begin{cases} s \mapsto \mathrm{id}, \\ t \mapsto \alpha^2, \end{cases} \qquad \theta_4 = \begin{cases} s \mapsto \alpha^2, \\ t \mapsto \alpha^2, \end{cases}$$
This is the same situation as in the previous exercise, since $\ker \theta_2 = \langle t \rangle$, $\ker \theta_3 = \langle s \rangle$, and $\ker \theta_4 = \langle st \rangle$. Hence, the semidirect products corresponding to θ_2, θ_3, and θ_4 are all isomorphic to each other. Pick θ_2 without loss of generality. Then s acts on P, and $sps^{-1} = p^{-1}$. Moreover, t centralizes P, hence $|tp| = 10$. Since
$$s(tp)s^{-1} = stps^{-1} = (sts^{-1})(sps^{-1}) = tp^{-1} = (tp)^{-1},$$
then
$$G \cong P \rtimes_{\theta_2} S \cong \{p, s, t \mid p^5 = s^2 = t^2 = 1, st = ts, sps^{-1} = p^{-1}, tpt^{-1} = p\} \cong D_{20}.$$ ■

Exercise 5.5.13

Classify groups of order $4p$, where p is a prime greater than 3. [There are four isomorphism types when $p \equiv 3 \pmod 4$, and five isomorphism types when $p \equiv 1 \pmod 4$.]

Solution. We have a framework for each case of p, namely Exercise 5.5.11 when $p \equiv 3 \pmod 4$, and Exercise 5.5.12 when $p \equiv 1 \pmod 4$. The only difference is that we have $P \in \mathrm{Syl}_p(G)$ and $S \in \mathrm{Syl}_2(G)$, where $|P| = p$ and $|S| = 4$. By the Sylow theorems, we have $n_p \equiv 1 \pmod p$ and $n_p \mid 4$, so $n_p = 1$. Hence, the unique Sylow p-subgroup is normal. Moreover, we have $P = \langle q \rangle \cong Z_p$ and $S \cong Z_4$ or $Z_2 \times Z_2$. We then have two cases to consider:

- If $S \cong Z_4 = \langle s \rangle$, then s has different candidates to be sent to in $\mathrm{Aut}(P) = (\mathbb{Z}/p\mathbb{Z})^\times$, which has order $p-1$. If $p \equiv 3 \pmod 4$, then $p - 1 \equiv 2 \pmod 4$, hence $\varphi(s)$ can only be sent to id or the unique element of order 2 in $\mathrm{Aut}(P)$. If we have the latter case, then $sqs^{-1} = q^{-1}$, and we have

$$G \cong P \rtimes S \cong Z_p \rtimes Z_4 = \{q, s \mid q^p = s^4 = 1, sqs^{-1} = q^{-1}\}.$$

  If $p \equiv 1 \pmod 4$, then $p - 1 \equiv 0 \pmod 4$, hence $\varphi(s)$ can be sent to id or one of the two elements of order 4 in $\mathrm{Aut}(P)$ (which are isomorphic since their images generate the same subgroup), or the unique element of order 2 in $\mathrm{Aut}(P)$. If $\mathrm{Aut}(P) = \langle \alpha \rangle$, let $\rho = \alpha^{(p-1)/4}$, which has order 4. Then we have the three nontrivial homomorphisms

$$\varphi_1 \colon s \mapsto \rho, \quad \varphi_2 \colon s \mapsto \rho^3, \quad \varphi_3 \colon s \mapsto \rho^2.$$

  We know that φ_1 and φ_2 give isomorphic semidirect products, since $\varphi_1(S) = \varphi_2(S) = \langle \rho \rangle$. Hence, we have two non-abelian groups of order $4p$, and we have

$$G \cong P \rtimes_{\varphi_1} S \cong \{q, s \mid q^p = s^4 = 1, sqs^{-1} = q^k\},$$

  for some $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $|k| = 4$. In the case of φ_3, we have $sqs^{-1} = q^{-1}$. Then

$$G \cong P \rtimes_{\varphi_3} S \cong \{q, s \mid q^p = s^4 = 1, sqs^{-1} = q^{-1}\}.$$

- If $S \cong Z_2 \times Z_2 = \langle s \rangle \times \langle t \rangle$, then we have the trivial homomorphism $\theta_1 \colon S \to \mathrm{Aut}(P)$, which gives $G \cong P \rtimes_{\theta_1} S \cong P \times S \cong Z_p \times (Z_2 \times Z_2)$. If ρ^2 is the generator of the unique subgroup of order 2 in $\mathrm{Aut}(P)$, then we have the three nontrivial homomorphisms

$$\theta_2 = \begin{cases} s \mapsto \rho^2, \\ t \mapsto \mathrm{id}, \end{cases} \qquad \theta_3 = \begin{cases} s \mapsto \mathrm{id}, \\ t \mapsto \rho^2, \end{cases} \qquad \theta_4 = \begin{cases} s \mapsto \rho^2, \\ t \mapsto \rho^2, \end{cases}$$

  Again, we know that $\ker \theta_2 = \langle t \rangle$, $\ker \theta_3 = \langle s \rangle$, and $\ker \theta_4 = \langle st \rangle$. Hence, the semidirect products corresponding to θ_2, θ_3, and θ_4 are all isomorphic to each other. Pick θ_2 without loss of generality. Then s acts on P, and $sqs^{-1} = q^{-1}$. Moreover, t centralizes P, hence $|tq| = 2p$. Since

$$s(tq)s^{-1} = stqs^{-1} = (sts^{-1})(sqs^{-1}) = tq^{-1} = (tq)^{-1},$$

  then

$$G \cong P \rtimes_{\theta_2} S \cong \{q, s, t \mid (tq)^2 = s^2 = 1, st = ts, sqs^{-1} = q^{-1}, tqt^{-1} = q\} \cong D_{4p}.$$ ∎

Exercise 5.5.14

This exercise classifies the groups of order 60 (there are thirteen isomorphism types). Let G be a group of order 60, let P be a Sylow 5-subgroup of G, and let Q be a Sylow 3-subgroup of G.

(a) Prove that if P is not normal in G, then $G \cong A_5$. [See Section 4.5.]

(b) Prove that if $P \trianglelefteq G$ but Q is not normal in G, then $G \cong A_4 \times Z_5$. [Show in this case that $P \leq Z(G)$, $G/P \cong A_4$, a Sylow 2-subgroup T of G is normal, and $TQ \cong A_4$.]

(c) Prove that if both P and Q are normal in G, then $G \cong Z_{15} \rtimes T$, where $T \cong Z_4$ or $Z_2 \times Z_2$. Show in this case that there are six isomorphism types when T is cyclic (one abelian), and there are five isomorphism types when T is the Klein 4-group (one abelian). [Use the same ideas as in the classification of groups of order 30 and 20.]

Solution.

(a) Clear, from Corollary 4.22.

(b) If Q is not normal in G, then $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 20$ implies that $n_3 = 4$ or 10. If $n_3 = 10$, then since $P \trianglelefteq G$, we know that PQ_i is a subgroup of G that is cyclic. But then $PQ_i \cap PQ_j = 5$ intersect at P, which means there would be $10 \cdot 10$ elements in G, which would be a contradiction. Hence, $n_3 = 4$. Again, each PQ_i intersect nontrivially at P, and P commutes with the nonidentity elements of each PQ_i. Then there are $5 + 10 \cdot 4 = 45$ elements in $C_G(P)$. Since $C_G(P) \leq G$, $|C_G(P)| = 60$ so that $C_G(P) = G$, showing that $P \leq Z(G)$.

Consider G/P, where $|G/P| = 12$. If we consider π to be the natural projection map from G to G/P, we claim that the map $\psi\colon \mathrm{Syl}_3(G) \to \mathrm{Syl}_3(G/P)$ given by $\psi(Q_i) \to \pi(Q_i)$ is a bijection. Note that this is a well defined map, since $\pi(Q_i) = Q_iP/P$ is a subgroup of G/P, and since $Q_iP \leq G$ with order 15, Q_iP/P has order 3, so $\pi(Q_i) \in \mathrm{Syl}_3(G/P)$. To see that ψ is injective, suppose that $\psi(Q_i) = \psi(Q_j)$, then $Q_iP/P = Q_jP/P$, which implies that $Q_iP = Q_jP$. Since $|Q_iP| = |Q_jP| = 15$, and $n_3(Q_iP) \equiv 1 \pmod 3$ and $n_3(Q_iP) \mid 5$, $n_3(Q_iP) = 1$. Hence, $Q_i = Q_j$, so ψ is injective. Since $n_3(G) = 4$, $|\mathrm{Syl}_3(G/P)| \geq 4$. By injectivity, it must be that ψ is a bijection, hence $n_3(G/P) = 4$. We now consider the classification of groups of order 12, which are Z_{12}, $Z_2 \times Z_6$, D_{12}, A_4, and $Z_3 \rtimes Z_4$.

- We know Z_{12} and $Z_2 \times Z_6$ are abelian, so any group of order 3 in these groups is normal, which is a contradiction.
- For $D_{12} \cong S_3 \times Z_2$, let $\alpha \in S_3$ be a 3-cycle. Then $\langle(\alpha, 1)\rangle$ is a subgroup of order 3. Recall that conjugating α by any cycle in S_3 gives α or α^2, hence $\langle(\alpha, 1)\rangle$ is normal in D_{12}, which is a contradiction.
- For $Z_3 \rtimes Z_4$, we know that Z_3 is normal in this group, which is a contradiction.

Then the only possibility is that $G/P \cong A_4$.

Let $T_1, T_2 \in \mathrm{Syl}_2(G)$ be distinct, and consider T_1P and T_2P. Since $P \leq Z(G)$, $T_iP \cong T_i \times P$ for $i = 1, 2$. If there was some $t \in T_1$ such that $t \in T_2P$, observe that $|t|$ is divisible by 4. Since all nonidentity elements of P have order 5, $t \in T_2$. But T_1 and T_2 are distinct by assumption, hence there must be some $t^* \in T_1$ such that $t^* \notin T_2P$. Then $T_1P \neq T_2P$, and $T_1P/P, T_2P/P \in \mathrm{Syl}_2(G/P)$. Since $n_2(G/P) = 1$, $T_1P/P = T_2P/P$, which implies that $T_1P = T_2P$. But this is a contradiction, so there is a unique Sylow 2-subgroup of G, which we call T.

Consider TQ. It is clear that $T \cap Q = 1$, and $|TQ| = 12$. If $Q \trianglelefteq TQ$, then since $P \leq Z(G)$ also normalizes Q, $Q \trianglelefteq G$, which is a contradiction. Then $n_3(TQ) \neq 1$, and by a similar argument as above, we conclude that $TQ \cong A_4$. If we now consider $\varphi\colon TQ \to \mathrm{Aut}(P)$, note that φ is trivial since TQ is generated by 3-cycles, while $\mathrm{Aut}(P) \cong Z_4$ has no elements of order 3. Then $G \cong P \times TQ \cong Z_5 \times A_4$.

(c) If P and Q are both normal in G, then we have $PQ \trianglelefteq G$. Since $P \cap Q = 1$, $PQ \cong P \times Q \cong Z_5 \times Z_3 \cong Z_{15}$. Put $P = \langle p\rangle$ and $Q = \langle q\rangle$. Let $T \in \mathrm{Syl}_2(G)$, and consider a homomorphism from T to $\mathrm{Aut}(Z_{15})$, where $\mathrm{Aut}(Z_{15}) \cong Z_4 \times Z_2$. From the text, we know that there are exactly 3 automorphisms of order 2:

$$\alpha_1 = \begin{cases} p \mapsto p^{-1} \\ q \mapsto q \end{cases} \qquad \alpha_2 = \begin{cases} p \mapsto p \\ q \mapsto q^{-1} \end{cases} \qquad \alpha_3 = \begin{cases} p \mapsto p^{-1} \\ q \mapsto q^{-1} \end{cases}$$

Moreover, there are 4 automorphisms of order 4:

$$\beta_1 = \begin{cases} p \mapsto p^2 \\ q \mapsto q \end{cases} \qquad \beta_2 = \begin{cases} p \mapsto p^2 \\ q \mapsto q^{-1} \end{cases} \qquad \beta_3 = \begin{cases} p \mapsto p^3 \\ q \mapsto q \end{cases} \qquad \beta_4 = \begin{cases} p \mapsto p^3 \\ q \mapsto q^{-1} \end{cases}$$

However, note that $\langle\beta_1\rangle = \langle\beta_3\rangle$ and $\langle\beta_2\rangle = \langle\beta_4\rangle$, so there are only two distinct subgroups of order 4 in $\mathrm{Aut}(Z_{15})$. Without loss of generality, we may consider the automorphisms $\alpha_1, \alpha_2, \alpha_3, \beta_1$, and β_2. We then have the following cases to consider for the Sylow 2-subgroup T:

- Suppose $T = \langle t\rangle \cong Z_4$. Then we have the trivial homomorphism, which gives $G \cong Z_{15} \times Z_4$. Then we have the nontrivial homomorphisms

$$\varphi_1\colon t \mapsto \alpha_1, \quad \varphi_2\colon t \mapsto \alpha_2, \quad \varphi_3\colon t \mapsto \alpha_3, \quad \varphi_4\colon t \mapsto \beta_1, \quad \varphi_5\colon t \mapsto \beta_2$$

  (1) For $G_1 = Z_{15} \rtimes_{\varphi_1} Z_4$, we have $tpt^{-1} = p^{-1}$ and $tqt^{-1} = q$. Since $q \in G_1$ is centralized, we have the factorization that $\langle p, t\rangle \cong Z_5 \rtimes Z_4$. However, note that $\mathrm{Aut}(Z_5) \cong Z_4$, so we have the presentation

$$G_1 \cong \langle p, t\rangle \times \langle q\rangle \cong \mathrm{Hol}(Z_5) \times Z_3.$$

  (2) For $G_2 = Z_{15} \rtimes_{\varphi_2} Z_4$, we have $tpt^{-1} = p$ and $tqt^{-1} = q^{-1}$. Since $p \in G_2$ is centralized, we have the factorization

$$G_2 \cong \langle q, t\rangle \times \langle p\rangle \cong (Z_3 \rtimes Z_4) \times Z_5.$$

  (3) For $G_3 = Z_{15} \rtimes_{\varphi_3} Z_4$, we have $tpt^{-1} = p^{-1}$ and $tqt^{-1} = q^{-1}$. Then

$$G_3 \cong Z_{15} \rtimes Z_4 = \{p, q, t \mid p^5 = q^3 = t^4 = 1, pq = qp, tpt^{-1} = p^{-1}, tqt^{-1} = q^{-1}\}.$$

  (4) For $G_4 = Z_{15} \rtimes_{\varphi_4} Z_4$, we have $tpt^{-1} = p^2$ and $tqt^{-1} = q$. Since $q \in G_4$ is centralized, we have the factorization

$$G_4 \cong \langle p, t\rangle \times \langle q\rangle \cong F_{20} \times Z_3.$$

(5) For $G_5 = Z_{15} \rtimes_{\varphi_5} Z_4$, we have $tpt^{-1} = p^2$ and $tqt^{-1} = q^{-1}$. Then

$$G_5 \cong \{p, q, t \mid p^5 = q^3 = t^4 = 1, pq = qp, tpt^{-1} = p^2, tqt^{-1} = q^{-1}\} = F_{20} \rtimes Z_3.$$

- Suppose $T = \langle u \rangle \times \langle v \rangle \cong Z_2 \times Z_2$. While this may seem like a lot of cases, observe that $\beta_i^2 = \alpha_1$ for all $i = 1, 2, 3, 4$, since either $q \mapsto q^{-1} \mapsto q$, or $p \mapsto p^2 \mapsto p^4 = p^{-1}$ (p^3 is handled similarly). Hence, we only need to consider the homomorphisms that send u and v to the images of the α_i's in $\mathrm{Aut}(Z_{15})$. Moreover, we know by Exercise 5.5.6 that homomorphisms from the cyclic subgroups of T, i.e., $\langle u \rangle, \langle v \rangle, \langle uv \rangle$, to $\mathrm{Aut}(Z_{15})$ that have conjugate (same, since $\mathrm{Aut}(Z_{15})$ is abelian) images give isomorphic semidirect products. For completeness, we will list all potential nontrivial homomorphisms, but group them by their images in $\mathrm{Aut}(Z_{15})$:
  - With image $\langle \alpha_1 \rangle$, we have the three homomorphisms

$$\theta_1 = \begin{cases} u \mapsto \alpha_1, \\ v \mapsto \mathrm{id}, \end{cases} \qquad \theta_2 = \begin{cases} u \mapsto \mathrm{id}, \\ v \mapsto \alpha_1, \end{cases} \qquad \theta_3 = \begin{cases} u \mapsto \alpha_1, \\ v \mapsto \alpha_1, \end{cases}$$

  - With image $\langle \alpha_2 \rangle$, we have the three homomorphisms

$$\rho_1 = \begin{cases} u \mapsto \alpha_2, \\ v \mapsto \mathrm{id}, \end{cases} \qquad \rho_2 = \begin{cases} u \mapsto \mathrm{id}, \\ v \mapsto \alpha_2, \end{cases} \qquad \rho_3 = \begin{cases} u \mapsto \alpha_2, \\ v \mapsto \alpha_2, \end{cases}$$

  - With image $\langle \alpha_3 \rangle$, we have the three homomorphisms

$$\sigma_1 = \begin{cases} u \mapsto \alpha_3, \\ v \mapsto \mathrm{id}, \end{cases} \qquad \sigma_2 = \begin{cases} u \mapsto \mathrm{id}, \\ v \mapsto \alpha_3, \end{cases} \qquad \sigma_3 = \begin{cases} u \mapsto \alpha_3, \\ v \mapsto \alpha_3, \end{cases}$$

  - With image $V_4 = \langle \alpha_1, \alpha_2 \rangle$ (where $\alpha_1\alpha_2 = \alpha_3$), we have the homomorphisms

$$\tau_1 = \begin{cases} u \mapsto \alpha_1, \\ v \mapsto \alpha_2, \end{cases} \quad \tau_2 = \begin{cases} u \mapsto \alpha_2, \\ v \mapsto \alpha_1, \end{cases} \quad \tau_3 = \begin{cases} u \mapsto \alpha_1, \\ v \mapsto \alpha_3, \end{cases} \quad \tau_4 = \begin{cases} u \mapsto \alpha_3, \\ v \mapsto \alpha_1, \end{cases} \quad \tau_5 = \begin{cases} u \mapsto \alpha_2, \\ v \mapsto \alpha_3, \end{cases} \quad \tau_6 = \begin{cases} u \mapsto \alpha_3, \\ v \mapsto \alpha_2, \end{cases}$$

  Hence, we may consider the semidirect products corresponding to $\theta_1, \rho_1, \sigma_1$, and τ_1 without loss of generality. Then we have

  (1) For $G_\theta = Z_{15} \rtimes_{\theta_1} (Z_2 \times Z_2)$, we have u acting on Z_{15} by α_1, and v centralizing Z_{15}. Then we have the factorization $\langle v \rangle \times \langle p, q, u \rangle$. Observe that q is centralized by u, and p is inverted by u. Hence, we have

$$G_\theta \cong \langle v \rangle \times \langle q \rangle \times \langle p, u \rangle \cong Z_2 \times Z_3 \times D_{10} \cong Z_6 \times D_{10}.$$

  (2) For $G_\rho = Z_{15} \rtimes_{\rho_1} (Z_2 \times Z_2)$, we have u acting on Z_{15} by α_2, and v centralizing Z_{15}. Then we have the factorization $\langle v \rangle \times \langle p, q, u \rangle$. Observe that p is centralized by u, and q is inverted by u. Hence, we have

$$G_\rho \cong \langle v \rangle \times \langle p \rangle \times \langle q, u \rangle \cong Z_2 \times Z_5 \times D_6 \cong Z_{10} \times D_6.$$

  (3) For $G_\sigma = Z_{15} \rtimes_{\sigma_1} (Z_2 \times Z_2)$, we have u acting on Z_{15} by α_3, and v centralizing Z_{15}. Then we have the factorization $\langle v \rangle \times \langle p, q, u \rangle$. Observe that both p and q are inverted by u. Hence, we have

$$G_\sigma \cong \langle v \rangle \times \langle p, q, u \rangle \cong Z_2 \times D_{30}.$$

  However, we can simplify this further by noting that u inverts the element pqv, which has order 30. Hence, we have

$$G_\sigma \cong \langle pqv, u \rangle \cong D_{60}.$$

  (4) For $G_\tau = Z_{15} \rtimes_{\tau_1} (Z_2 \times Z_2)$, we have u acting on Z_{15} by α_1, and v acting on Z_{15} by α_2. Then we have the factorization $\langle p, q, u, v \rangle$. Observe that p is inverted by u and centralized by v, while q is inverted by v and centralized by u. Hence, we have

$$G_\tau \cong \langle p, u \rangle \times \langle q, v \rangle \cong D_{10} \times D_6 \cong D_{10} \times S_6.$$ ∎

Exercise 5.5.15

Let p be an odd prime. Prove that every element of order 2 in $\mathrm{GL}_2(\mathbb{F}_p)$ is conjugate to a diagonal matrix with ± 1's on the diagonal. Classify the groups of order $2p^2$. [If A is a 2×2 matrix with $A^2 = I$ and v_1, v_2 is a basis for the underlying vector space, look at A acting on the vectors $w_1 = v_1 + v_2$ and $w_2 = v_1 - v_2$.]

Solution. If $A = \pm I_2$, then A is already diagonal. We now prove that if every nonzero vector of a 2-dimensional vector space is an eigenvector of A, then A is a scalar matrix. To see this, let e_1 and e_2 be eigenvectors of A corresponding to eigenvalues λ_1 and λ_2, respectively. Consider the vector $e_1 + e_2$, which is also an eigenvector of A with some eigenvalue λ. Then

$$A(e_1 + e_2) = \lambda(e_1 + e_2) \implies \lambda_1 e_1 + \lambda_2 e_2 = \lambda e_1 + \lambda e_2 \implies (\lambda_1 - \lambda)e_1 + (\lambda_2 - \lambda)e_2 = 0.$$

Since e_1 and e_2 are linearly independent, we must have $\lambda_1 = \lambda = \lambda_2$. Hence, A is a scalar matrix.

We now take the contrapositive of this, and assume that A is not a scalar matrix. Then there exists a nonzero vector v_1 that is not an eigenvector of A. Let $v_2 = Av_1$. If $v_2 = \lambda v_1$, then $Av_1 = \lambda v_1$, contradicting that v_1 is not an eigenvector of A. Hence, v_1 and v_2 are linearly independent and form a basis of the vector space.

Let $w_1 = v_1 + v_2$ and $w_2 = v_1 - v_2$. Then

$$\begin{aligned} Aw_1 &= A(v_1 + v_2) = Av_1 + Av_2 = v_2 + Av_2 = v_2 + A^2 v_1 = v_2 + v_1 = w_1, \\ Aw_2 &= A(v_1 - v_2) = Av_1 - Av_2 = v_2 - Av_2 = v_2 - A^2 v_1 = v_2 - v_1 = -w_2. \end{aligned}$$

Let $P = \begin{pmatrix} w_1 & w_2 \end{pmatrix}$. Then

$$P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Hence, A is similar to the diagonal matrix with entries 1 and -1.

Let $|G| = 2p^2$, $P \in \mathrm{Syl}_p(G)$, and $Q \in \mathrm{Syl}_2(G)$. Since $n_p \equiv 1 \pmod p$ and $n_p \mid 2$, p being odd implies that $n_p = 1$, hence $P \trianglelefteq G$. Moreover, $|P| = p^2$ implies that $P \cong Z_{p^2}$, or $Z_p \times Z_p$. Put $Q = \langle q \rangle$. We split by cases:

- The abelian case is $Z_{p^2} \times Z_2$. If $P = \langle x \rangle \cong Z_{p^2}$, then $\mathrm{Aut}(P) \cong Z_{p(p-1)}$. Since $|q| = 2$ and p is odd, $p - 1$ is even and $\mathrm{Aut}(P)$ has even order, hence it has a unique subgroup of order 2 generated by some $\alpha \in \mathrm{Aut}(P)$, namely the inversion map. We then have $qxq^{-1} = x^{-1}$. It follows that

$$G \cong \langle x, q \mid x^{p^2} = q^2 = 1, qxq^{-1} = x^{-1} \rangle \cong D_{2p^2}.$$

- The abelian case is $Z_p \times Z_p \times Z_2$. If $P = \langle x \rangle \times \langle y \rangle \cong Z_p \times Z_p$, then $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then there are three homomorphisms from Q to $\mathrm{Aut}(P)$, namely

$$\varphi_1 = \begin{cases} x \mapsto x, \\ y \mapsto y \end{cases} \qquad \varphi_2 = \begin{cases} x \mapsto x^{-1}, \\ y \mapsto y \end{cases} \qquad \varphi_3 = \begin{cases} x \mapsto x, \\ y \mapsto y^{-1} \end{cases} \qquad \varphi_4 = \begin{cases} x \mapsto x^{-1}, \\ y \mapsto y^{-1} \end{cases}$$

  Note that $\varphi_1 = \mathrm{id}$, hence that is the same abelian case as before. Moreover, if we let S be the exchange matrix, then $S\varphi_2(q)S^{-1} = \varphi_3(q)$. Hence, the semidirect products corresponding to φ_2 and φ_3 are isomorphic. We then have the following nonisomorphic groups:
  - $G_2 \cong (Z_p \times Z_p) \rtimes_{\varphi_2} Z_2$ has y centralized, while x is inverted. We then have $\langle y \rangle \times \langle q, x \rangle$, where $\langle q, x \rangle \cong D_{2p}$. Hence,
$$G_2 \cong Z_p \times D_{2p}.$$
  - $G_4 \cong (Z_p \times Z_p) \rtimes_{\varphi_4} Z_2$ has both x and y inverted by q. Hence, it has presentation

$$G_4 \cong \langle x, y, q \mid x^p = y^p = q^2 = 1, qxq^{-1} = x^{-1}, qyq^{-1} = y^{-1} \rangle \cong (Z_p \times Z_p) \rtimes Z_2. \qquad \blacksquare$$

Exercise 5.5.16

Show that there are exactly 4 distinct homomorphisms from Z_2 into $\mathrm{Aut}(Z_8)$. Prove that the resulting semidirect products are the groups $Z_8 \times Z_2$, D_{16}, the quasidihedral group QD_{16} (cf. Exercise 2.5.11), and the modular group M (cf. Exercise 2.5.14).

Solution. Let $Z_8 = \langle a \rangle$ and $Z_2 = \langle b \rangle$. Note that $\mathrm{Aut}(Z_8) \cong (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \cong V_4$. Hence, there are exactly 4 distinct homomorphisms from Z_2 into $\mathrm{Aut}(Z_8)$, given by

$$\varphi_1 \colon b \mapsto a, \quad \varphi_2 \colon b \mapsto a^3, \quad \varphi_3 \colon b \mapsto a^5, \quad \varphi_4 \colon b \mapsto a^7.$$

The resulting semidirect products are:

- $G_1 \cong Z_8 \rtimes_{\varphi_1} Z_2 \cong Z_8 \times Z_2$, since φ_1 is the trivial homomorphism.
- $G_2 \cong Z_8 \rtimes_{\varphi_2} Z_2$ has the automorphism $bab^{-1} = a^3$, hence $G_2 \cong QD_{16}$.
- $G_3 \cong Z_8 \rtimes_{\varphi_3} Z_2$ has the automorphism $bab^{-1} = a^5$, hence $G_3 \cong M$.
- $G_4 \cong Z_8 \rtimes_{\varphi_4} Z_2$ has the inversion map $bab^{-1} = a^{-1}$, hence $G_4 \cong D_{16}$.

By Exercise 5.3.1, we know that the three non-abelian groups are pairwise nonisomorphic. Moreover, $Z_8 \times Z_2$ is abelian and the others are non-abelian, so it is also nonisomorphic to the others. ■

Exercise 5.5.17

Show that for any $n \geq 3$, there are exactly 4 distinct homomorphisms from Z_2 into $\mathrm{Aut}(Z_{2^n})$. Prove that the resulting semidirect groups give 4 nonisomorphic groups of order 2^{n+1}. [Recall Exercise 2.3.21 through Exercise 2.3.23.] (These four groups together with the cyclic group and the generalized quaternion group $Q_{2^{n+1}}$ are all the groups of order 2^{n+1} which possess a cyclic subgroup of index 2.)

Solution. Let $Z_{2^n} = \langle a \rangle$ and $Z_2 = \langle b \rangle$. Recall that $\mathrm{Aut}(Z_{2^n}) \cong Z_2 \times Z_{2^{n-2}}$ for $n \geq 3$. Then the elements of order dividing 2 in $\mathrm{Aut}(Z_{2^n})$ are the elements in $\{0, x\} \times 0, y^{2^{n-2}}$, where x is the generator of Z_2 and y is the generator of $Z_{2^{n-2}}$. Let $(0,0)$ represent the identity automorphism, $(x,0)$ represent the inversion map, $(0, y^{2^{n-2}})$ represent the automorphism $a \mapsto a^{2^{n-1}+1}$, and $(x, y^{2^{n-2}})$ represent the automorphism $a \mapsto a^{2^{n-1}-1}$. Then the four distinct homomorphisms from Z_2 into $\mathrm{Aut}(Z_{2^n})$ are given by

$$\varphi_1 \colon b \mapsto (0,0), \quad \varphi_2 \colon b \mapsto (x,0), \quad \varphi_3 \colon b \mapsto (0, y^{2^{n-2}}), \quad \varphi_4 \colon b \mapsto (x, y^{2^{n-2}}).$$

Then the resulting semidirect products are:

- $G_1 \cong Z_{2^n} \rtimes_{\varphi_1} Z_2 \cong Z_{2^n} \times Z_2$, since φ_1 is the trivial homomorphism.
- $G_2 \cong Z_{2^n} \rtimes_{\varphi_2} Z_2$ has the inversion map $bab^{-1} = a^{-1}$, hence $G_2 \cong D_{2^{n+1}}$.
- $G_3 \cong Z_{2^n} \rtimes_{\varphi_3} Z_2$ has the automorphism $bab^{-1} = a^{2^{n-1}+1}$, hence we have the presentation

$$G_3 \cong \langle a, b \mid a^{2^n} = b^2 = 1, bab^{-1} = a^{2^{n-1}+1} \rangle.$$

- $G_4 \cong Z_{2^n} \rtimes_{\varphi_4} Z_2$ has the automorphism $bab^{-1} = a^{2^{n-1}-1}$, hence we have the presentation

$$G_4 \cong \langle a, b \mid a^{2^n} = b^2 = 1, bab^{-1} = a^{2^{n-1}-1} \rangle.$$

Since G_1 is abelian, it is not isomorphic to the other three groups. To see that the other groups are not pairwise isomorphic, we begin by analyzing the centers of each group.

We first claim that elements of the form $a^i b$ are not in the center of G_2, G_3, or G_4. To see this, observe that $a^i b$ commutes with a in particular, hence $a^{i+1}b = a^i ba$ implies that $ab = ba$, or $bab^{-1} = a$ (where $b = b^{-1}$ since it has order 2). However, this only occurs in G_1, hence $a^i b \notin Z(G_2), Z(G_3), Z(G_4)$. We can conclude that $Z(G_2), Z(G_3), Z(G_4) \subseteq \langle a \rangle$. Note that for a^i to commute with b, then $ba^i b^{-1} = a^i$, or that $a^{ri} = a^i$, where $r = -1, 2^{n-1}+1, 2^{n-1}-1$ for G_2, G_3, G_4, respectively. Equating exponents, it must be that $i(r-1) \equiv 0 \pmod{2}^n$. We analyze each group:

- For G_2, we have $r - 1 = -2$, hence $i \equiv 0 \pmod{2}^{n-1}$. Then $Z(G_2) = \langle a^{2^{n-1}} \rangle \cong Z_2$. (Alternatively, we know that $D_{2^{n+1}} = D_{2k}$ for some even k, and $Z(D_{2k}) = \langle r^k \rangle \cong Z_2$.)
- For G_3, we have $r - 1 = 2^{n-1}$, hence $i \equiv 0 \pmod 2$. Then $Z(G_3) = \langle a^2 \rangle \cong Z_{2^{n-1}}$.
- For G_4, we have $r - 1 = 2^{n-1} - 2$, hence $2i(2^{n-2} - 1) \equiv 0 \pmod{2}^n$. Since $2^{n-2} - 1$ is odd, $i \equiv 0 \pmod{2}^{n-1}$. Then $Z(G_4) = \langle a^{2^{n-1}} \rangle \cong Z_2$.

We see that $Z(G_2) \cong Z(G_4)$, but $Z(G_3)$ is not isomorphic to either of them. Hence, G_3 is not isomorphic to G_2 or G_4. To see that G_2 and G_4 are not isomorphic, we analyze the elements of order 2 in each group. In particular, consider the elements of the form $a^i b$. Then $(a^i b)^2 = a^i ba^i b = a^i ba^i b^{-1} = a^{i+ri} = a^{i(r+1)}$, where r is as above. We analyze each group:

- For G_2, we have $r + 1 = 0$, hence $(a^i b)^2 = a^0 = 1$. Then all elements of the form $a^i b$ have order 2, and there are 2^n such elements.
- For G_4, we have $r + 1 = 2^{n-1}$, hence $(a^i b)^2 = a^{i2^{n-1}}$. Then $(a^i b)^2 = 1$ if and only if $i \equiv 0 \pmod 2$, hence there are 2^{n-1} such elements.

Since G_2 and G_4 have different numbers of elements of order 2, they are not isomorphic. Hence, we have shown that the four groups are pairwise nonisomorphic. ■

Exercise 5.5.18

Show that if H is any group, then there is a group G that contains H as a normal subgroup with the property that for every automorphism σ of H, there is an element $g \in G$ such that conjugation by g when restricted to H is the given automorphism σ, i.e., every automorphism of H is obtained as an inner automorphism of G restricted to H.

Solution. Let H be a group, and let $G = H \rtimes \mathrm{Aut}(H)$, where the action is given by the natural action of $\mathrm{Aut}(H)$ on H. Then H is a normal subgroup of G. Let $\sigma \in \mathrm{Aut}(H)$. Let $g = (1, \sigma) \in G$. Then for any $(h, 1) \in \widetilde{H}$, where $\widetilde{H} \cong H$, then

$$(1, \sigma)(h, 1)(1, \sigma)^{-1} = (\sigma(h), 1).$$

Hence, conjugation by g restricted to H gives the automorphism σ. We remark that $G = \mathrm{Hol}(H)$. ■

Exercise 5.5.19

Let H be a group of order n, let $K = \mathrm{Aut}(H)$, and form $G = \mathrm{Hol}(H) = H \rtimes K$ (where φ is the identity homomorphism). Let G act by left multiplication on the left cosets of K in G, and let π be the associated permutation representation $\pi\colon G \to S_n$.

(a) Prove that the elements of H are coset representatives for the left cosets of K in G, and with this choice of coset representatives, π restricted to H is the regular representation of H.

(b) Prove $\pi(G)$ is the normalizer in S_n of $\pi(H)$. Deduce that, under the regular representation of any finite group H of order n, the normalizer in S_n of the image of H is isomorphic to $\mathrm{Hol}(H)$. [Show $|G| = |N_{S_n}(\pi(H))|$ using Exercise 5.5.1 and Exercise 5.5.2.]

(c) Deduce that the normalizer of the group generated by an n-cycle in S_n is isomorphic to $\mathrm{Hol}(Z_n)$ and has order $n\varphi(n)$.

Solution.

(a) Recall that elements of G are of the form (h, α), where $h \in H$ and $\alpha \in K$. Then the left cosets of K in G are of the form $(h, \alpha)K = (h, 1)(1, \alpha)K = (h, 1)K$. Hence, the elements of H are coset representatives for the left cosets of K in G. Let $\pi\colon G \to S_n$ be the associated permutation representation. Then for any $h_1, h_2 \in H$, we have

$$\pi(h_1)(h_2K) = (h_1, 1)(h_2K) = (h_1h_2, 1)K = (h_1h_2)K.$$

Hence, π restricted to H is the regular representation of H.

(b) Let $N = N_{S_n}(\pi(H))$. To see that π is injective, let $(h, \alpha) \in \ker \pi$. Then for any $h' \in H$, we have

$$(h, \alpha)(h'K) = (h, 1)(1, \alpha)(h'K) = (h, 1)(\alpha(h')K) = (h\alpha(h'), 1)K = h\alpha(h')K.$$

Now let $h\alpha(h') = h'$ for all $h' \in H$. Then in particular, $h' = 1$ gives $h = 1$. Then we have $\alpha(h') = h'$ for all $h' \in H$, hence $\alpha = 1$. Therefore, $(h, \alpha) = (1, 1)$, and π is injective.

To see that $\pi(G) \leq N$, note that $H \trianglelefteq G$. Hence, $ghg^{-1} \in H$ for any $g \in G$ and $h \in H$. Consequently, $\pi(ghg^{-1}) \in \pi(H)$, hence $\pi(g)\pi(h)\pi(g)^{-1} \in \pi(H)$, and $\pi(G) \leq N$. Now let κ be the coset K in G. Let N_κ denote the stabilizer of κ in N. Observe, by definition, that $\pi(H) \trianglelefteq N$. From part (a), we know that $\pi(H)$ acts transitively on the left cosets of K in G, so $N = \pi(H) \cdot N_\kappa$. Moreover, $\pi(H)$ stabilizes no coset, hence $N_\kappa \cap \pi(H) = 1$. Then $N = \pi(H) \rtimes N_\kappa$, and $|N| = n|N_\kappa|$.

Observe that conjugation by elements of N_κ on $\pi(H)$ gives automorphisms of $\pi(H)$. Hence, we have a homomorphism $\psi\colon N_\kappa \to \mathrm{Aut}(\pi(H))$. To see that ψ is injective, let $g \in \ker \psi$. Then $ghg^{-1} = h$ for all $h \in H$, hence g centralizes $\pi(H)$. Moreover, g stabilizes κ, hence $g \in \pi(H)$. Then

$$g(hK) = g(\pi(h)(\kappa)) = \pi(h)(g(\kappa)) = \pi(h)(\kappa) = hK.$$

Hence, $g = 1$, and ψ is injective. Then we have

$$|N_\kappa| \leq |\mathrm{Aut}(\pi(H))| = |\mathrm{Aut}(H)|.$$

Hence, $|N| = n|N_\kappa| \leq n|\mathrm{Aut}(H)| = |G|$. Since π is injective, $|G| = |\pi(G)| \leq |N|$. Hence, $|N| = |G|$, and $\pi(G) = N$.

(c) Let $\sigma \in S_n$ be an n-cycle. Then $\langle\sigma\rangle \cong Z_n$ acts transitively on the set $\{1, 2, \ldots, n\}$, hence the associated permutation representation is the regular representation of Z_n. Since any subgroup of S_n isomorphic to Z_n are conjugate in S_n, the normalizer of any subgroup generated by an n-cycle is isomorphic to the normalizer of $\langle\sigma\rangle$. By part (b), we have

$$N_{S_n}(\langle\sigma\rangle) \cong N_{S_n}(\pi(Z_n)) \cong \mathrm{Hol}(Z_n).$$

Since $\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, $|N_{S_n}(\langle\sigma\rangle)| = |\mathrm{Hol}(Z_n)| = n\varphi(n)$. ■

Exercise 5.5.20

Let p be an odd prime. Prove that if P is a noncyclic p group, then P contains a normal subgroup U with $U \cong Z_p \times Z_p$. Deduce that, for odd primes p, a p-group that contains a unique subgroup of order p is cyclic. (For $p = 2$, it is a theorem that the generalized quaternion groups Q_{2^n} are the only noncyclic 2-groups which contain a unique subgroup of order 2.) [Proceed by induction on $|P|$. Let Z be a subgroup of order p in $Z(P)$, and let $\overline{P} = P/Z$. If $\overline{P}$ is cyclic, then P is abelian by Exercise 3.1.36–show that the result is true for abelian groups. When $\overline{P}$ is not cyclic, use induction to produce a normal subgroup $\overline{H}$ of $\overline{P}$ with $\overline{H} \cong Z_p \times Z_p$. Let H be the complete preimage of $\overline{H}$ in P, so $|H| = p^3$. Let $H_0 = \{x \in H \mid x^p = 1\}$, so that H_0 is a characteristic subgroup of H of order p^2 or p^3 by Exercise 5.4.9. Show that a suitable subgroup of H_0 gives the desired normal subgroup U.]

Solution. The base case of $n = 2$ is clear, since $P \cong Z_p \times Z_p$ is a noncyclic p-group of order p^2. Let $|P| = p^n$ for some $n > 2$, and assume the result is true for all noncyclic p-groups of order less than p^n. Let $Z \leq Z(P)$ be a subgroup of order p, and let $\overline{P} = P/Z$. If $\overline{P}$ is cyclic, then by Exercise 3.1.36, we have that P is abelian, hence P has at least 2 invariant factors. Then the subgroup generated by the elements of order p in P is a normal subgroup of order p^2, which is isomorphic to $Z_p \times Z_p$. If $\overline{P}$ is not cyclic, then by induction, there exists a normal subgroup $\overline{H} \leq \overline{P}$ with $\overline{H} \cong Z_p \times Z_p$. Let H be the complete preimage of $\overline{H}$ in P, so that $|H| = p^3$. Let

$$H_0 = \{x \in H \mid x^p = 1\}.$$

Then H_0 is a characteristic subgroup of H of order p^2 or p^3 by Exercise 5.4.9. If $|H_0| = p^2$, then H_0 is characteristic in H where $H \trianglelefteq P$, so $H_0 \trianglelefteq P$, and $H_0 \cong Z_p \times Z_p$, and we can take $U = H_0$. If $|H_0| = p^3$, let P act on H by conjugation. Since $Z \leq Z(P)$, we may have P act on $\overline{H}$ by conjugation. We use the class equation, but we instead consider the action of P on $\overline{H}$ by conjugation. Since $|\overline{H}| = p^2$, the class equation gives

$$|\overline{H}| = |C_{\overline{H}}(P)| + \sum_{i=1}^{k} |P : C_P(\bar{x}[i])|,$$

where $\bar{x}[1], \ldots, \bar{x}[k]$ are representatives of the nonsingleton orbits of the P-conjugation on $\overline{H}$. Note that $|P : C_P(\bar{x}[i])|$ is a power of p, hence $|C_{\overline{H}}(P)| \equiv |\overline{H}| \equiv 0 \pmod{p}$. Since $\bar{1} \in C_{\overline{H}}(P)$, $|C_{\overline{H}}(P)| \geq p$. Then there exists some $\bar{h} \in C_{\overline{H}}(P)$ with $\bar{h} \neq \bar{1}$. Let $h \in H$ be the preimage of $\bar{h}$ in H. Then $h \notin Z$, and $h^p \in Z$. Let $U = \langle h, Z \rangle$. Then $|U| = p^2$. Since $Z \trianglelefteq P$ is clear, we observe that for any $g \in P$, $ghg^{-1} \in \bar{h} \subseteq U$, hence $U \trianglelefteq P$. Moreover, $h^p = 1$, since $H_0 = H$, and $|h| = p$ with $h \notin Z$, hence $\langle h \rangle \cap Z = 1$. Lastly, $Z \leq Z(P)$ implies that h commutes with all of Z. Then $U \cong Z_p \times Z_p$, and we are done. ∎

Exercise 5.5.21

Let p be an odd prime, and let P be a p-group. Prove that if every subgroup of P is normal, then P is abelian. (Note that Q_8 is a non-abelian 2-group with this property, so the result is false for $p = 2$.) [Use the preceding exercises and Exercise 5.4.15.]

Solution. We proceed by induction on $|P|$. The base case of $|P| = p$ is clear, since $P \cong Z_p$ is abelian. Suppose $|P| > p$ and every subgroup of P is normal, and assume the result is true for all p-groups of order less than $|P|$. If P is cyclic, then P is abelian. Otherwise, by Exercise 5.5.20, there exists a normal subgroup $U \trianglelefteq P$ with $U \cong Z_p \times Z_p$. Then there are distinct subgroups H and K of order p in U, normal in P, and have trivial intersection.

Observe that $|\mathrm{Aut}(H)| = p - 1$. Having P act on H by conjugation gives a homomorphism $\varphi \colon P \to \mathrm{Aut}(H)$. Since $|P|$ is a power of p, and $|\mathrm{Aut}(H)| = p - 1$ is not divisible by p, we have that φ is the trivial homomorphism, so $H \leq Z(P)$. By symmetry, $K \leq Z(P)$. Then P/H is a p-group of order less than $|P|$ in which every subgroup is normal, hence by induction, P/H is abelian. By Exercise 5.4.15, P/H and P/K abelian implies that $P/(H \cap K) = P/1 \cong P$ is abelian, and we are done. ∎

Exercise 5.5.22

Let F be a field, let n be a positive integer, and let G be a group of upper triangular matrices in $\mathrm{GL}_n(F)$ (cf. Exercise 2.1.16)

(a) Prove that G is the semidirect product $U \rtimes D$, where U is the set of upper triangular matrices with 1's down the diagonal (cf. Exercise 2.1.17), and D is the set of diagonal matrices in $\mathrm{GL}_n(F)$.

(b) Let $n = 2$. Recall that $U \cong F$, and $D \cong F^\times \times F^\times$ (cf. Exercise 3.1.11). Describe the homomorphism from D into $\mathrm{Aut}(U)$ explicitly in terms of these isomorphisms, i.e., show how each element of $F^\times \times F^\times$ acts as an automorphism on F.

Solution.

(a) We first show that $U \trianglelefteq G$. Let $A \in G$ and $B \in U$. Then A and B are upper triangular matrices, so ABA^{-1} is also an upper triangular matrix. If a_{ii} is the ith diagonal entry of A, then the ith diagonal entry of ABA^{-1} is the product of the ith diagonal entries of A, B, and A^{-1}, which is $a_{ii} \cdot 1 \cdot a_{ii}^{-1} = 1$. Hence, $ABA^{-1} \in U$, and $U \trianglelefteq G$. Moreover, $U \cap D = \{I_n\}$, since the only upper triangular matrix with 1's down the diagonal that is also diagonal is the identity matrix. Additionally, for any $A \in G$ with diagonal entries $a_{11}, \ldots, a_{nn}$, let $D_0 = \mathrm{diag}(a_{11}, \ldots, a_{nn})$. Then $D_0 \in D$. Put $U_0 = D_0^{-1}A$. Then U_0 has diagonal entries $a_{ii}a_{ii}^{-1} = 1$, so $U_0 \in U$. Hence, $A = D_0U_0 \in DU = UD$, and $G = UD$.

(b) By Exercise 3.1.11, we have $U \cong F$ and $D \cong F^\times \times F^\times$ via the maps ψ and π_1. For any $\mathrm{diag}(a, b) \in D$ and $x \in F$, we have

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ab^{-1}x \\ 0 & 1 \end{pmatrix}.$$

Hence, the homomorphism from D into $\mathrm{Aut}(U)$ is given by

$$\mathrm{diag}(a, b) \mapsto (x \mapsto ab^{-1}x).$$

Note that this is the conjugation homomorphism $\varphi\colon D \to \mathrm{Aut}(U)$ given by $\varphi(d)(u) = dud^{-1}$ for $d \in D$ and $u \in U$. ■

Exercise 5.5.23

[Wreath Products] Let K and L be groups, let n be a positive integer, let $\rho\colon K \to S_n$ be a homomorphism and let H be the direct product of n copies of L. In Exercise 5.1.8, an injective homomorphism ψ from S_n into $\mathrm{Aut}(H)$ was constructed by letting the elements of S_n permute the n factors of H. The composition $\psi \circ \rho$ is a homomorphism from G into $\mathrm{Aut}(H)$. The **wreath product** of L by K is the semidirect product $H \rtimes K$ with respect to this homomorphism and is denoted by $L \wr K$.
(This wreath product depends on the choice of permutation representation ρ of K–if none is given explicitly, ρ is assumed to be the left regular representation of K.)

(a) Assume K and L are finite groups and ρ is the left regular representation of K. Find $|L \wr K|$ in terms of $|K|$ and $|L|$.

(b) Let p be a prime, let $K = L = Z_p$ and let ρ be the left regular representation of K. Prove that $Z_p \wr Z_p$ is a non-abelian group of order p^{p+1} and is isomorphic to a Sylow p-subgroup of S_{p^2}.
[The p copies of Z_p whose direct product makes up H may be represented by p disjoint p-cycles; these are cyclically permuted by K.]

Solution.

(a) The left regular representation of K is a homomorphism $\rho\colon K \to S_{|K|}$. Then H is the direct product of $|K|$ copies of L, so $|H| = |L|^{|K|}$. We then have

$$|L \wr K| = |H \rtimes K| = |H||K| = |L|^{|K|}|K|.$$

(b) From the above, we know that $|Z_p \wr Z_p| = |Z_p|^{|Z_p|}|Z_p| = p^p \cdot p = p^{p+1}$. Let H be the direct product of p copies of Z_p, and put $K = \langle k \rangle \cong Z_p$. Let $H = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_p \rangle$, where $|h_i| = p$ for all i. To see that $Z_p \wr Z_p$ is non-abelian, we show that k does not commute with h_1. Let $\rho\colon K \to S_p$ be the left regular representation of K. Then $\rho(k)$ is the p-cycle $(1\ 2\ \cdots p)$. Then $\rho(k)$ permutes the p factors of H, so $kh_1k^{-1} = h_2 \neq h_1$.

Consider the integers $1, 2, \ldots, p^2$. Split these integers into p blocks of size p:

$$S_i = \{(i-1)p + 1, (i-1)p + 2, \ldots, ip\} \quad \text{for } i = 1, 2, \ldots, p.$$

Consider the p-cycle σ_i whose entries are the elements of S_i in increasing order. Then σ_i is a p-cycle, and the σ_i are disjoint for $i = 1, 2, \ldots, p$. Additionally, put

$$\tau_i = (i\ p+i\ 2p+i\ \cdots (p-1)p+i) \quad \text{for } i = 1, 2, \ldots, p.$$

Then define the map $\varphi\colon Z_p \wr Z_p \to S_{p^2}$ given by

$$\varphi|_{\langle h_i \rangle}\colon h_i \mapsto \sigma_i, \quad \varphi|_K\colon k \mapsto \tau_1\tau_2\cdots\tau_p.$$

Then φ is a homomorphism, since $\varphi(k)$ permutes the p factors of H in the same way that k permutes the p factors of H. To see that this satisfies the semidirect product, we have

$$\varphi(k)\varphi(h_i)\varphi(k)^{-1} = (\tau_1\tau_2\cdots\tau_p)\sigma_i(\tau_1\tau_2\cdots\tau_p)^{-1} = (\tau_1\tau_2\cdots\tau_p)\sigma_i(\tau_p^{-1}\tau_{p-1}^{-1}\cdots\tau_1^{-1}).$$

Using associativity, we may consider the first middle terms, i.e., $(\tau_p\sigma_i\tau_p^{-1})$. Conjugating σ_i by τ_p sends the pth entry of σ_i to the pth entry of σ_{i+1} while fixing all other entries. Conjugating by τ_{p-1} sends the $(p-1)$th entry of σ_i to the $(p-1)$th entry of σ_{i+1} while fixing all other entries. Continuing in this way and conjugating σ_i by all remaining τ_j gives σ_{i+1}, where $i+1$ is taken modulo p.

To see that φ is injective, note that every element of $Z_p \wr Z_p$ is of the form hk' for some $h \in H$ and $k' \in K$. Suppose $\varphi(hk') = 1$. Then $\varphi(h)\varphi(k') = 1$, hence $\varphi(k') = \varphi(h)^{-1}$. Since $\varphi(h)$ permutes elements within each block S_i, so does $\varphi(h)^{-1}$. It follows that $\varphi(k')$ must fix every block S_i. However, $\varphi(k')$ acts as a p-cycle on the p blocks, so $\varphi(k')$ fixes all blocks if and only if $k' = 1$. Then $\varphi(h) = 1$. Since the σ_i are pairwise disjoint cycles of length p, $\varphi(h) = 1$ if and only if $h = 1$.

Calculating the order of a Sylow p-subgroup of S_{p^2}, we have $|S_{p^2}| = p^2!$. Using the formula in Exercise 0.2.8, the largest power of p dividing $p^2!$ is

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

Since $p^2/p^i < 1$ for all $i > 2$, then $\lfloor p^2/p^i \rfloor = 0$ for all $i > 2$. Hence, the largest power of p dividing $p^2!$ is $p+1$, and the order of a Sylow p-subgroup of S_{p^2} is p^{p+1}. Since $|\varphi(Z_p \wr Z_p)| = |Z_p \wr Z_p| = p^{p+1}$, we have that $\varphi(Z_p \wr Z_p)$ is a Sylow p-subgroup of S_{p^2}. ∎

Exercise 5.5.24

Let n be an integer > 1. Prove the following classification: every group of order n is abelian if and only if $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, where $p_1, \ldots, p_r$ are distinct primes, $\alpha_i = 1$ or 2 for all $i \in \{1, \ldots, r\}$ and p_i does not divide $p_j^{\alpha_j} - 1$ for all i and j. [See Exercise 4.5.56.]

Solution.

$\boxed{\Rightarrow}$ Suppose some $\alpha_i \geq 3$. Then there exists a non-abelian group of order p_i^3 by the classification of groups of order p^3. Then the direct product of this group with the cyclic groups of order $p_j^{\alpha_j}$ for $j \neq i$ is a non-abelian group of order n. Hence, $\alpha_i \leq 2$ for all i.

Now suppose there exist i and j such that p_i divides $p_j^{\alpha_j} - 1$. By Proposition 4.17, the automorphism group of $Z_{p_j^{\alpha_j}}$ has order $p_j^{\alpha_j - 1}(p_j - 1)$. We have two cases for α_j:

- If $\alpha_j = 1$, then $p_j^{\alpha_j} - 1 = p_j - 1$, and p_i divides $p_j - 1$. Using Cauchy's theorem, we have that $\mathrm{Aut}(Z_{p_j})$ has an element of order p_i. Then we may form the non-abelian group $Z_{p_j} \rtimes Z_{p_i}$ of order $p_j p_i$.
- If $\alpha_j = 2$, then $p_i \mid p_j^2 - 1$. Note that $Z_{p_j} \times Z_{p_j}$ has automorphism group isomorphic to $\mathrm{GL}_2(\mathbb{F}_{p_j})$. Then $|\mathrm{Aut}(Z_{p_j} \times Z_{p_j})| = |\mathrm{GL}_2(\mathbb{F}_{p_j})| = (p_j^2 - 1)(p_j^2 - p_j) = p_j(p_j - 1)^2(p_j + 1)$, which is divisible by p_i. Again, we may use Cauchy's theorem to find an element of order p_i in $\mathrm{Aut}(Z_{p_j} \times Z_{p_j})$, and form the non-abelian group $(Z_{p_j} \times Z_{p_j}) \rtimes Z_{p_i}$ of order $p_j^2 p_i$.

In either case, we may form a direct product of the non-abelian group with the cyclic groups of order $p_k^{\alpha_k}$ for $k \neq i, j$ to obtain a non-abelian group of order n.

$\boxed{\Leftarrow}$ We proceed by induction on $|G| = n$. If $r = 1$, then $n = p$ or p^2. Since any group of order p or p^2 is abelian, we are done. If $r = 2$, then $n = p_1^{\alpha_1}p_2^{\alpha_2}$, where $\alpha_i = 1$ or 2 for $i = 1, 2$. If $P_i \in \mathrm{Syl}_{p_i}(G)$, then $n_{p_i} \equiv 1 \pmod{p}_i$ and $n_{p_i} \mid p_j^{\alpha_j}$

for $j \neq i$. Since p_i does not divide $p_j^{\alpha_j} - 1$, we have that $n_{p_i} = 1$ for $i = 1, 2$. Hence, P_1 and P_2 are normal in G, and $G = P_1 \times P_2$ is abelian.

Suppose $n > p^2$ with $r \geq 3$, and assume the result is true for all integers less than n with the same property on their prime factorization. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $\alpha_i = 1$ or 2 for all i, and p_i does not divide $p_j^{\alpha_j} - 1$ for all i and j. Let G be a group of order n. Note that every proper subgroup of G has order less than n, and hence is abelian by the induction hypothesis. By Exercise 4.5.56, we know that G is solvable, hence $G' < G$ and G' is abelian.

We now claim that G' is a p-group for some prime p. Suppose not, and let q be a prime dividing $|G'|$. Since G' is abelian, it has a unique Sylow q-subgroup Q. Since Q is unique, then $Q \operatorname{char} G' \trianglelefteq G$. Then $Q \trianglelefteq G$ so that G/Q is a proper quotient of G. Since G/Q is a proper quotient of G, it is abelian by the induction hypothesis. Then $G' \leq Q$, which contradicts that G' has multiple prime factors. Hence, G' is a p-group for some prime p.

Now for each prime p_i dividing $|G|$, let $P_i \in \operatorname{Syl}_{p_i}(G)$, and consider $G'P_i$. Then $|G'P_i|$ divides $|G'|p_i^{\alpha_i}$, which is strictly less than $|G|$ since $r \geq 3$. By the induction hypothesis, $G'P_i$ is abelian. Since $G'P_i/G'$ is a subgroup of the abelian group G/G', then $G'P_i/G' \trianglelefteq G/G'$, hence $G'P_i \trianglelefteq G$ by the Correspondence Theorem. Since $G'P_i$ is abelian, P_i is its unique Sylow p_i-subgroup, so $P_i \operatorname{char} G'P_i \trianglelefteq G$. Then $P_i \trianglelefteq G$ for all i, and $G = P_1 \times P_2 \times \cdots \times P_r$ is abelian. ■

Exercise 5.5.25

Let $H(\mathbb{F}_p)$ be the Heisenberg group over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (cf. Exercise 5.4.20). Prove that $H(\mathbb{F}_2) \cong D_8$, and that $H(\mathbb{F}_p)$ has exponent p and is isomorphic to the first non-abelian group in Example 7.

Solution. That $H(\mathbb{F}_2) \cong D_8$ follows from Exercise 2.4.12. Using the formulation in Exercise 1.4.11, we know that for any $(a, b, c) \in H(\mathbb{F}_p)$, then

$$(a, b, c)^p = \left(pa, \frac{p(p-1)ac}{2} + pb, pc\right) = (0, 0, 0) \in H(\mathbb{F}_p),$$

showing that $H(\mathbb{F}_p)$ has exponent p since p is an odd prime. Finally, to see that $H(\mathbb{F}_p)$ is isomorphic to the given example, consider the matrices

$$X = (1, 0, 0), \quad A = (0, 1, 0), \quad B = (0, 0, 1).$$

Since $H(\mathbb{F}_p)$ has exponent p, then $X^p = A^p = B^p = 1$. We also have the following relations:

$$\begin{aligned} XAX^{-1} &= (1,0,0)(0,1,0)(-1,0,0) = (0,1,1) = AB, \\ XBX^{-1} &= (1,0,0)(0,0,1)(-1,0,0) = (0,0,1) = B, \\ AB &= (0,1,0)(0,0,1) = (0,1,1) = (0,0,1)(0,1,0) = BA. \end{aligned}$$

Recall that $(Z_p \times Z_p) \rtimes Z_p$ has presentation

$$\langle x, a, b \mid x^p = a^p = b^p = 1, ab = ba, xax^{-1} = ab, xbx^{-1} = b \rangle.$$

The map $\varphi \colon H(\mathbb{F}_p) \to (Z_p \times Z_p) \rtimes Z_p$ given by $\varphi(X) = x$, $\varphi(A) = a$, and $\varphi(B) = b$ is clearly a surjective homomorphism, and since $|H(\mathbb{F}_p)| = p^3 = |(Z_p \times Z_p) \rtimes Z_p|$, we have that φ is an isomorphism. ■

6 Further Topics in Group Theory

6.1 p-Groups, Nilpotent Groups, and Solvable Groups

Exercise 6.1.1

Prove that $Z_i(G)$ is a characteristic subgroup of G for all i.

Exercise 6.1.2

Prove Parts 2 and 4 of Theorem 1 for G a finite nilpotent group, not necessarily a p-group.

Exercise 6.1.3

If G is finite, prove that G is nilpotent if and only if it has a normal subgroup of each order dividing $|G|$, and is cyclic if and only if it has a unique subgroup of each order dividing $|G|$.

Exercise 6.1.4

Prove that a maximal subgroup of a finite nilpotent group has prime index.

Exercise 6.1.5

Prove Parts 2 and 4 of Theorem 1 for G an infinite nilpotent group.

Exercise 6.1.6

Show that if $G/Z(G)$ is nilpotent then G is nilpotent.

Exercise 6.1.7

Prove that subgroups and quotient groups of nilpotent groups are nilpotent (your proof should work for infinite groups). Give an explicit example of a group G which possesses a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.

Exercise 6.1.8

Prove that if p is a prime and P is a non-abelian group of order p^3 then $|Z(P)| = p$ and $P/Z(P) \cong Z_p \times Z_p$.

Exercise 6.1.9

Prove that a finite group G is nilpotent if and only if whenever $a, b \in G$ with $(|a|, |b|) = 1$ then $ab = ba$. [Use Part 4 of Theorem 3.]

Exercise 6.1.10

Prove that D_{2n} is nilpotent if and only if n is a power of 2. [Use Exercise 9.]

Exercise 6.1.11

Give another proof of Proposition 5 under the additional assumption that G is abelian by invoking the Fundamental Theorem of Finite abelian Groups.

Exercise 6.1.12

Find the upper and lower central series for A_4 and S_4.

Exercise 6.1.13

Find the upper and lower central series for A_n and S_n, $n \geq 5$.

Exercise 6.1.14

Prove that G^i is a characteristic subgroup of G for all i.

Exercise 6.1.15

Prove that $Z_i(D_{2^n}) = D_{2^n}^{n-1-i}$.

Exercise 6.1.16

Prove that $\mathbb{Q}$ has no maximal subgroups. [Recall Exercise 21, Section 3.2.]

Exercise 6.1.17

Prove that $G^{(i)}$ is a characteristic subgroup of G for all i.

Exercise 6.1.18

Show that if G'/G'' and G''/G''' are both cyclic then $G'' = 1$. [You may assume $G''' = 1$. Then G/G'' acts by conjugation on the cyclic group G''.]

Exercise 6.1.19

Show that there is no group whose commutator subgroup is isomorphic to S_4. [Use the preceding exercise.]

Exercise 6.1.20

Let p be a prime, let P be a p-subgroup of the finite group G, let N be a normal subgroup of G whose order is relatively prime to p and let $\overline{G} = G/N$. Prove the following:

(a) $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)}$ [Use Frattini's Argument.]

(b) $C_{\overline{G}}(\overline{P}) = \overline{C_G(P)}$. [Use part (a).]

Exercise 6.1.21

Prove that $\Phi(G)$ is a characteristic subgroup of G.

Exercise 6.1.22

Prove that if $N \trianglelefteq G$ then $\Phi(N) \leq \Phi(G)$. Give an explicit example where this containment does not hold if N is not normal in G.

Exercise 6.1.23

Compute $\Phi(S_3)$, $\Phi(A_4)$, $\Phi(S_4)$, $\Phi(A_5)$ and $\Phi(S_5)$.

Exercise 6.1.24

Say an element x of G is a *nongenerator* if for every proper subgroup H of G, $\langle x, H\rangle$ is also a proper subgroup of G. Prove that $\Phi(G)$ is the set of nongenerators of G (here $|G| > 1$).

Exercise 6.1.25

Let G be a finite group. Prove that $\Phi(G)$ is nilpotent. [Use Frattini's Argument to prove that every Sylow subgroup of $\Phi(G)$ is normal in G.]

Exercise 6.1.26

Let p be a prime, let P be a finite p-group and let $\overline{P} = P/\Phi(P)$.

(a) Prove that $\overline{P}$ is an elementary abelian p-group. [Show that $P' \leq \Phi(P)$ and that $x^p \in \Phi(P)$ for all $x \in P$.]

(b) Prove that if N is any normal subgroup of P such that P/N is elementary abelian then $\Phi(P) \leq N$. State this (universal) property in terms of homomorphisms and commutative diagrams.

(c) Let $\overline{P}$ be elementary abelian of order p^r (by (a)). Deduce from Exercise 24 that if $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_r}$ are any basis for the r-dimensional vector space $\overline{P}$ over $\mathbb{F}_p$ and if x_i is any element of the coset $\overline{x_i}$, then $P = \langle x_1, x_2, \ldots, x_r\rangle$. Show conversely that if $y_1, y_2, \ldots, y_s$ is any set of generators for P, then $s \geq r$ (you may assume that every minimal generating set for an r-dimensional vector space has r elements, i.e., every basis has r elements). Deduce Burnside's Basis Theorem: a set $y_1, \ldots, y_s$ is a minimal generating set for P if and only if $\overline{y_1}, \ldots, \overline{y_s}$ is a basis of $\overline{P} = P/\Phi(P)$. Deduce that any minimal generating set for P has r elements.

(d) Prove that if $P/\Phi(P)$ is cyclic then P is cyclic. Deduce that if P/P' is cyclic then so is P.

(e) Let σ be any automorphism of P of prime order q with $q \neq p$. Show that if σ fixes the coset $x\Phi(P)$ then σ fixes some element of this coset (note that since $\Phi(P)$ is characteristic in P every automorphism of P induces an automorphism of $P/\Phi(P)$). [Use the observation that σ acts a permutation of order 1 or q on the p^a elements in the coset $x\Phi(P)$.]

(f) Use parts (e) and (c) to deduce that every nontrivial automorphism of P of order prime to p induces a nontrivial automorphism on $P/\Phi(P)$. Deduce that any group of automorphisms of P which has order prime to p is isomorphic to a subgroup of $\mathrm{Aut}(\overline{P}) = GL_r(\mathbb{F}_p)$.

Exercise 6.1.27

Generalize part (d) of the preceding exercise as follows: let p be a prime, let P be a p-group and let $\overline{P} = P/\Phi(P)$ be elementary abelian of order p^r. Prove that P has exactly $\dfrac{p^r - 1}{p - 1}$ maximal subgroups. [Since every maximal subgroup of P contains $\Phi(P)$, the maximal subgroups of P are, by the Lattice Isomorphism Theorem, in bijective correspondence with the maximal subgroups of the elementary abelian group $\overline{P}$. It therefore suffices to show that the number of maximal subgroups of an elementary abelian p-group of order p^r is as stated above. One way of doing this is to use the result that an abelian group is isomorphic to its dual group (cf. Exercise 14 in Section 5.2) so the number of subgroups of index p equals the number of subgroups of order p.]

Exercise 6.1.28

Prove that if p is a prime and $P = Z_p \times Z_{p^2}$ then $|\Phi(P)| = p$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.

Exercise 6.1.29

Prove that if p is a prime and P is a non-abelian group of order p^3 then $\Phi(P) = Z(P)$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.

Exercise 6.1.30

Let p be an odd prime, let $P_1 = Z_p \times Z_{p^2}$ and let P_2 be the non-abelian group of order p^3 which has an element of order p^2. Prove that P_1 and P_2 have the same lattice of subgroups.

Exercise 6.1.31

For any group G a *minimal normal subgroup* is a normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M. Prove that every minimal normal subgroup of a finite solvable group is an elementary abelian p-group for some prime p. [If M is a minimal normal subgroup of G, consider its characteristic subgroups: M' and $\langle x^p \mid x \in M \rangle$.]

Exercise 6.1.32

Prove that every maximal subgroup of a finite solvable group has prime power index. [Let H be a maximal subgroup of G and let M be a minimal normal subgroup of G — cf. the preceding exercise. Apply induction to G/M and consider separately the two cases: $M \leq H$ and $M \not\leq H$.]

Exercise 6.1.33

Let π be any set of primes. A subgroup H of a finite group is called a *Hall π-subgroup* of G if the only primes dividing $|H|$ are in the set π and $|H|$ is relatively prime to $|G : H|$. (Note that if $\pi = \{p\}$, Hall π-subgroups are the same as Sylow p-subgroups. Hall subgroups were introduced in Exercise 10 of Section 3.3). Prove the following generalization of Sylow's Theorem for solvable groups: if G is a finite solvable group then for every set π of primes, G has a Hall π-subgroup and any two Hall π-subgroups (for the same set π) are conjugate in G. [Fix π and proceed by induction on $|G|$, proving both existence and conjugacy at once. Let M be a minimal normal subgroup of G, so M is a p-group for some prime p. If $p \in \pi$, apply induction to G/M. If $p \notin \pi$, reduce to the case $|G| = p^\alpha n$, where $p^\alpha = |M|$ and n is the order of a Hall π-subgroup of G. In this case let N/M be a minimal normal subgroup of G/M, so N/M is a q-group for some prime $q \neq p$. Let $Q \in \mathrm{Syl}_q(N)$. If $Q \trianglelefteq G$ argue as before with Q in place of M. If Q is not normal in G, use Frattini's Argument to show $N_G(Q)$ is a Hall π-subgroup of G and establish conjugacy in this case too.]

Exercise 6.1.34

Let p be a prime dividing the order of the finite solvable group G. Assume G has no nontrivial normal subgroups of order prime to p. Let P be the largest normal p-subgroup of G (cf. Exercise 37, Section 4.5). Note that Exercise 31 above shows that $P \neq 1$. Prove that $C_G(P) \leq P$, i.e., $C_G(P) = Z(P)$. [Let $N = C_G(P)$ and use the preceding exercise to show $N = Z(P) \times H$ for some Hall π-subgroup H of N — here π is the set of all prime divisors of $|N|$ except for p. Show $H \trianglelefteq G$ to obtain the desired conclusion: $H = 1$.]

Exercise 6.1.35

Prove that if G is a finite group in which every proper subgroup is nilpotent, then G is solvable. [Show that a minimal counterexample is simple. Let M and N be distinct maximal subgroups chosen with $|M \cap N|$ as large as possible and apply Part 2 of Theorem 3 to show that $M \cap N = 1$. Now apply the methods of Exercise 53 in Section 4.5.]

Exercise 6.1.36

Let p be a prime, let V be a nonzero finite dimensional vector space over the field of p elements and let ϕ be an element of $GL(V)$ of order a power of p (i.e., V is a nontrivial elementary abelian p-group and ϕ is an automorphism of V of p-power order). Prove that there is some nonzero element $v \in V$ such that $\phi(v) = v$, i.e., ϕ has a nonzero fixed point on V.

Exercise 6.1.37

Let V be a finite dimensional vector space over the field of 2 elements and let ϕ be an element of $GL(V)$ of order 2. (i.e., V is a nontrivial elementary abelian 2-group and ϕ is an automorphism of V of order 2). Prove that the map $v \mapsto v + \phi(v)$ is a homomorphism from V to itself. Show that every element in the image of this map is fixed by ϕ. Deduce that the subspace of elements of V which are fixed by ϕ has dimension $\geq \frac{1}{2}$(dimension V). (Note that if G is the semidirect product of V with $\langle\phi\rangle$, where $V \trianglelefteq G$ and ϕ acts by conjugation on V by sending each $v \in V$ to $\phi(v)$, then the fixed points of ϕ on V are $C_V(\phi)$ and the above map is simply the commutator map: $v \mapsto [v, \phi]$. In this terminology the problem is to show that $|C_V(\phi)|^2 \geq |V|$.)

Exercise 6.1.38

Use the preceding exercise to prove that if P is a 2-group which has a cyclic center and M is a subgroup of index 2 in P, then the center of M has rank ≤ 2. [The group G/M of order 2 acts by conjugation on the $\mathbb{F}_2$ vector space: $\{z \in Z(M) \mid z^2 = 1\}$ and the fixed points of this action are in the center of P.]