Solution Manual for Abstract Algebra Theory and Applications

Thomas W. Judson
Stephen F. Austin State University

Robert A. Beezer
University of Puget Sound

DRAFT August 6, 2018 DRAFT

Contents

Chapter 1

Preliminaries

1.3 Exercises

1. Suppose that

$$A = \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\},$$
$$B = \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\},$$
$$C = \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of } 5\}.$$

Describe each of the following sets.

(a) $A \cap B$

(b) $B \cap C$

(c) $A \cup B$

(d) $A \cap (B \cup C)$

Hint. (a) $A \cap B = \{2\}$; (b) $B \cap C = \{5\}$.

Solution.

(a) $A \cap B = \{2\}$

(b) $B \cap C = \{5\}$

(c) $A \cup B = \{x : x \text{ is even or } x \text{ is prime}\}$

(d) $A \cap (B \cup C) = \{2\} \cup \{10x : x \in \mathbb{N}\}$

2. If $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, and $D = \emptyset$, list all of the elements in each of the following sets.

(a) $A \times B$

(b) $B \times A$

(c) $A \times B \times C$

(d) $A \times D$

Hint. (a) $A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3), (c,1), (c,2), (c,3)\}$; (d) $A \times D = \emptyset$.

Solution.

(a) $A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3), (c,1), (c,2), (c,3)\}$

(b) $B \times A = \{(1,a), (2,a), (3,a), (1,b), (2,b), (3,b), (1,c), (2,c), (3,c)\}$

(c) $A \times B \times C = \{(a,1,x),\ (a,2,x),\ (a,3,x),\ (b,1,x),\ (b,2,x),\ (b,3,x),\ (c,1,x),\ (c,2,x),\ (c,3,x)\}$

(d) $A \times D = \emptyset$

3. Find an example of two nonempty sets A and B for which $A \times B = B \times A$ is true.

Solution. If $A = B$, then $A \times B = B \times A$.

4. Prove $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

Solution. To show that $A \subset A \cup \emptyset$, let $x \in A$. Then $x \in A$ or $x \in \emptyset$. Thus, $x \in A \cup \emptyset$. Conversely, if $x \in A \cup \emptyset$, then x is in either A or $\emptyset$. Since $\emptyset$ contains no elements, it must be the case that $x \in A$ and $A \supset A \cup \emptyset$. Therefore, $A \cup \emptyset = A$. The proof for $A \cap \emptyset = \emptyset$ is similar.

5. Prove $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

Solution. Observe that $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. Equivalently, $x \in B$ or $x \in A$, which is the same as $x \in B \cup A$. Therefore, $A \cup B = B \cup A$. The proof is similar for $A \cap B = B \cap A$.

6. Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Hint. If $x \in A \cup (B \cap C)$, then either $x \in A$ or $x \in B \cap C$. Thus, $x \in A \cup B$ and $A \cup C$. Hence, $x \in (A \cup B) \cap (A \cup C)$. Therefore, $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$. Conversely, if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup B$ and $A \cup C$. Thus, $x \in A$ or x is in both B and C. So $x \in A \cup (B \cap C)$ and therefore $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. Hence, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Solution. If $x \in A \cup (B \cap C)$, then either $x \in A$ or $x \in B \cap C$. Thus, $x \in A \cup B$ and $A \cup C$. Hence, $x \in (A \cup B) \cap (A \cup C)$. Therefore, $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$. Conversely, if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup B$ and $A \cup C$. Thus, $x \in A$ or x is in both B and C. So $x \in A \cup (B \cap C)$ and therefore $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. Hence, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

7. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Solution. If $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. So $x \in A$ and either $x \in B$ or $x \in C$. Hence, either we have $x \in A$ and $x \in B$, or we have $x \in A$ and $x \in C$. Thus, $x \in A \cap B$ or $x \in A \cap C$. Therefore, $x \in (A \cap B) \cup (A \cap C)$, and consequently $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Conversely, let $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. It follows that $x \in A$, and either $x \in B$ or $x \in C$. So $x \in A$ and $x \in B \cup C$. Therefore, $x \in A \cap (B \cup C)$. Thus, $A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$, and the two sets are equal.

8. Prove $A \subset B$ if and only if $A \cap B = A$.

Solution. If $A \subset B$ and $x \in A \cap B$, then $x \in A$ and $x \in B$. So $A \cap B \subset A$. To show the reverse inclusion, if $x \in A$, then $x \in B$, since $A \subset B$. Hence, $x \in A \cap B$ and $A \subset A \cap B$. Conversely, if $A \cap B = A$ and $x \in A$, then $x \in A \cap B$. Hence, $x \in B$ and $A \subset B$.

9. Prove $(A \cap B)' = A' \cup B'$.

Solution. Let $x \in (A \cap B)'$. Then $x \notin A \cap B$. So x cannot be in both A and B. Thus, either $x \in A'$ or $x \in B'$. Therefore, $x \in A' \cup B'$ and we have $(A \cap B)' \subset A' \cup B'$. To show the reverse inclusion, suppose that $x \in A' \cup B'$. Then $x \in A'$ or $x \in B'$, and so $x \notin A$ and $x \notin B$. Thus $x \notin A \cap B$ and so $x \in (A \cap B)'$. Hence, $(A \cap B)' \supset A' \cup B'$.

10. Prove $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

Hint. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

Solution. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

11. Prove $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Solution. If $(x, y) \in (A \cup B) \times C$, then $x \in A \cup B$ and $y \in C$. Thus, $x \in A$ or $x \in B$. Therefore, $(x, y) \in A \times C$ or $(x, y) \in B \times C$. Consequently, $(x, y) \in (A \times C) \cup (B \times C)$ and $(A \cup B) \times C \subset (A \times C) \cup (B \times C)$. Conversely, suppose that $(x, y) \in (A \times C) \cup (B \times C)$. Then $(x, y) \in A \times C$ or $(x, y) \in B \times C$. Thus, $x \in A$ or $x \in B$ while $y \in C$. Hence, $x \in A \cup B$ and $y \in C$. Therefore, $(x, y) \in (A \cup B) \times C$, or $(A \times C) \cup (B \times C) \subset (A \cup B) \times C$.

12. Prove $(A \cap B) \setminus B = \emptyset$.

Solution. $(A \cap B) \setminus B = (A \cap B) \cap B' = A \cap (B \cap B') = A \cap \emptyset = \emptyset$.

13. Prove $(A \cup B) \setminus B = A \setminus B$.

Solution. $(A \cup B) \setminus B = (A \cup B) \cap B' = (A \cap B') \cup (B \cap B') = (A \setminus B) \cup \emptyset = A \setminus B$.

14. Prove $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Hint. $A \setminus (B \cup C) = A \cap (B \cup C)' = (A \cap A) \cap (B' \cap C') = (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$.

Solution. $A \setminus (B \cup C) = A \cap (B \cup C)' = (A \cap A) \cap (B' \cap C') = (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$.

15. Prove $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

Solution. $(A \cap B) \setminus (A \cap C) = (A \cap B) \cap (A \cap C)' = (A \cap B) \cap (A' \cup C') = [(A \cap (A' \cup C')] \cap B = [(A \cap A') \cup (A \cap C')] \cap B = (A \cap C') \cap B = A \cap (B \cap C') = A \cap (B \setminus C)$.

16. Prove $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Solution. $(A \setminus B) \cup (B \setminus A) = (A \cap B') \cup (B \cap A') = [(A \cap B') \cup B] \cap [(A \cap B') \cup A'] = (A \cup B) \cap (A' \cup B') = (A \cup B) \cap (A \cap B)' = (A \cup B) \setminus (A \cap B)$.

17. Which of the following relations $f : \mathbb{Q} \to \mathbb{Q}$ define a mapping? In each case, supply a reason why f is or is not a mapping.

(a) $f(p/q) = \dfrac{p+1}{p-2}$

(b) $f(p/q) = \dfrac{3p}{3q}$

(c) $f(p/q) = \dfrac{p+q}{q^2}$

(d) $f(p/q) = \dfrac{3p^2}{7q^2} - \dfrac{p}{q}$

Hint. (a) Not a map since $f(2/3)$ is undefined; (b) this is a map; (c) not a map, since $f(1/2) = 3/4$ but $f(2/4) = 3/8$; (d) this is a map.

Solution. (a) Not a map since $f(2/3)$ is undefined; (b) this is a map; (c) not a map, since $f(1/2) = 3/4$ but $f(2/4) = 3/8$; (d) this is a map.

18. Determine which of the following functions are one-to-one and which are onto. If the function is not onto, determine its range.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$

(b) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2 + 3$

(c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x$

(d) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$

Hint. (a) f is one-to-one but not onto. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (c) f is neither one-to-one nor onto. $f(\mathbb{R}) = \{x : -1 \leq x \leq 1\}$.

Solution. (a) f is one-to-one but not onto. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (b) f is neither one-to-one nor onto. $f(\mathbb{Z}) = \{3, 4, 7, 12, \ldots, n^2 + 3, \ldots\}$. (c) f is neither one-to-one nor onto. $f(\mathbb{R}) = \{x : -1 \leq x \leq 1\}$. (d) f is neither one-to-one nor onto. $f(\mathbb{Z}) = \{0, 1, 4, 9, 16, \ldots, n^2, \ldots\}$.

19. Let $f : A \to B$ and $g : B \to C$ be invertible mappings; that is, mappings such that f^{-1} and g^{-1} exist. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Solution. If $h = g^{-1} \circ f^{-1}$, then $h \circ f \circ g = f \circ g \circ h = \mathrm{id}$. So h is an inverse function for $f \circ g$. Since inverse functions are unique, $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

20.

(a) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is one-to-one but not onto.

(b) Define a function $f : \mathbb{N} \to \mathbb{N}$ that is onto but not one-to-one.

Hint. (a) $f(n) = n + 1$.

Solution. (a) $f(n) = n + 1$; (b)

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (n+1)/2 & \text{if } n \text{ is odd.} \end{cases}$$

Other solutions are possible.

21. Prove the relation defined on $\mathbb{R}^2$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$ is an equivalence relation.

Solution. The relation is reflexive, since $x_1^2 + y_1^2 = x_1^2 + y_1^2$ implies that $(x_1, y_1) \sim (x_1, y_1)$. To show that the relation is symmetric, observe that $(x_1, y_1) \sim (x_2, y_2)$ implies $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Thus, $x_2^2 + y_2^2 = x_1^2 + y_1^2$ and $(x_2, y_2) \sim (x_1, y_1)$. To show that the relation is transitive, let $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then $x_1^2 + y_1^2 = x_2^2 + y_2^2$ and $x_2^2 + y_2^2 = x_3^2 + y_3^2$. Thus, $x_1^2 + y_1^2 = x_3^2 + y_3^2$, and $(x_1, y_1) \sim (x_3, y_3)$.

22. Let $f : A \to B$ and $g : B \to C$ be maps.

(a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.

(b) If $g \circ f$ is onto, show that g is onto.

(c) If $g \circ f$ is one-to-one, show that f is one-to-one.

(d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.

(e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

Hint. (a) Let $x, y \in A$. Then $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Thus, $f(x) = f(y)$ and $x = y$, so $g \circ f$ is one-to-one. (b) Let $c \in C$, then $c = (g \circ f)(x) = g(f(x))$ for some $x \in A$. Since $f(x) \in B$, g is onto.

Solution.

(a) Let $x, y \in A$. Then $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Thus, $f(x) = f(y)$ and $x = y$, so $g \circ f$ is one-to-one.

(b) Let $c \in C$, then $c = (g \circ f)(x) = g(f(x))$ for some $x \in A$. Since $f(x) \in B$, g is onto.

(c) If $f(a) = f(b)$, then $(g \circ f)(a) = (g \circ f)(b)$. Since $g \circ f$ is one-to-one, $a = b$ and f is one-to-one.

(d) Let $g(a) = g(b)$. Since f is onto, there exist elements x and y such that $f(x) = a$ and $f(y) = b$. Consequently, $(g \circ f)(x) = (g \circ f)(y)$. Since $g \circ f$ is one-to-one, $x = y$. Therefore, $a = f(x) = f(y) = b$.

(e) If $a \in A$, there exists a $c \in C$ such that $(g \circ f)(a) = g(f(a)) = c$. If $b \in B$ such that $c = g(f(a)) = g(b)$, then $b = f(a)$, since g is one-to-one.

23. Define a function on the real numbers by

$$f(x) = \frac{x+1}{x-1}.$$

What are the domain and range of f? What is the inverse of f? Compute $f \circ f^{-1}$ and $f^{-1} \circ f$.

Hint. $f^{-1}(x) = (x+1)/(x-1)$.

Solution. $f^{-1}(x) = (x+1)/(x-1)$. The domain and range of f is $\mathbb{R} \setminus \{1\}$.

24. Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$.

(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Give an example in which equality fails.

(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(e) Prove $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

Hint. (a) Let $y \in f(A_1 \cup A_2)$. Then there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Hence, $y \in f(A_1)$ or $f(A_2)$. Therefore, $y \in f(A_1) \cup f(A_2)$. Consequently, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Conversely, if $y \in f(A_1) \cup f(A_2)$, then $y \in f(A_1)$ or $f(A_2)$. Hence, there exists an x in A_1 or A_2 such that $f(x) = y$. Thus, there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Therefore, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, and $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

Solution.

(a) Let $y \in f(A_1 \cup A_2)$. Then there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Hence, $y \in f(A_1)$ or $f(A_2)$. Therefore, $y \in f(A_1) \cup f(A_2)$. Consequently, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Conversely, if $y \in f(A_1) \cup f(A_2)$, then $y \in f(A_1)$ or $f(A_2)$. Hence, there exists an x in A_1 or A_2 such that $f(x) = y$. Thus, there exists an $x \in A_1 \cup A_2$ such that $f(x) = y$. Therefore, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, and $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) If y is in $f(A_1 \cap A_2)$, there exists an $x \in A_1 \cap A_2$ such that $f(x) = y$. So $x \in A_1$ with $f(x) = y$ and $x \in A_2$ with $f(x) = y$. Hence, $x \in f(A_1) \cap f(A_2)$. To show that equality does not hold, let $f(x) = x^2$, $A_1 = [0, 1]$ and $A_2 = [-1, 0]$. Other examples are possible.

(c) If $x \in f^{-1}(B_1 \cup B_2)$, then $f(x) \in B_1 \cup B_2$. So either $f(x) \in B_1$ or $f(x) \in B_2$. Therefore, $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. Consequently, $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$ or $f^{-1}(B_1 \cup B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$. Conversely, let $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Then $x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2)$. So either $x \in f(B_1)$ or $x \in f(B_2)$; hence, $f(x) \in B_1 \cup B_2$. Therefore, $x \in f^{-1}(B_1 \cup B_2)$ and the reverse inclusion is true.

(d) If $x \in f^{-1}(B_1 \cap B_2)$, then $f(x) \in B_1 \cap B_2$. So $f(x) \in B_1$ and $f(x) \in B_2$. Therefore, $x \in f^{-1}(B_1)$ and $x \in f^{-1}(B_2)$. Consequently, $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ or $f^{-1}(B_1 \cap B_2) \subset f^{-1}(B_1) \cap f^{-1}(B_2)$. Conversely, let $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Then $x \in f^{-1}(B_1)$ and $x \in f^{-1}(B_2)$. So $x \in f(B_1)$ and $x \in f(B_2)$; hence, $f(x) \in B_1 \cap B_2$. Therefore, $x \in f^{-1}(B_1 \cap B_2)$ and the reverse inclusion is true.

(e) $f^{-1}(Y \setminus B_1) = f^{-1}(Y \cap B_1') = f^{-1}(Y) \cap f^{-1}(B_1') = X \cap [f^{-1}(B_1)]' = X \setminus f^{-1}(B_1)$

25. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$

(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

Hint. (a) The relation fails to be symmetric. (b) The relation is not reflexive, since 0 is not equivalent to itself. (c) The relation is not transitive.

Solution.

(a) The relation fails to be symmetric.

(b) The relation is not reflexive, since 0 is not equivalent to itself.

(c) The relation is not transitive.

(d) An equivalence relation.

26. Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. Show that $\sim$ is reflexive and transitive but not symmetric.

Solution. Since $a^2 + b^2 \leq a^2 + b^2$, we have $(a, b) \sim (a, b)$, and the relation is reflexive. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $a^2 + b^2 \leq c^2 + d^2$ and $c^2 + d^2 \leq e^2 + f^2$. Thus, $a^2 + b^2 \leq e^2 + f^2$ and $(a, b) \sim (e, f)$. Therefore, the relation is transitive. The relation fails to be symmetric, since $(0, 0) \sim (1, 1)$ but $(1, 1) \not\sim (0, 0)$.

27. Show that an $m \times n$ matrix gives rise to a well-defined map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Solution.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ a_{21}x_1 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix}$$

28. Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$."

Hint. Let $X = \mathbb{N} \cup \{\sqrt{2}\}$ and define $x \sim y$ if $x + y \in \mathbb{N}$.

Solution. The problem is that x may not be equivalent to itself. Consider the following example. Let $X = \mathbb{N} \cup \{\sqrt{2}\}$ and define $x \sim y$ if $x + y \in \mathbb{N}$. Many other counterexamples are possible.

29. **Projective Real Line.** Define a relation on $\mathbb{R}^2 \setminus \{(0, 0)\}$ by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a nonzero real number λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Prove that $\sim$ defines an equivalence relation on $\mathbb{R}^2 \setminus (0, 0)$. What are the corresponding equivalence classes? This equivalence relation defines the projective line, denoted by $\mathbb{P}(\mathbb{R})$, which is very important in geometry.

Solution. The relation is reflexive, since $(x_1, y_1) = (\lambda x_1, \lambda y_1)$ if $\lambda = 1$. If $(x_1, y_1) \sim (x_2, y_2)$, then there exists a nonzero λ such that $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. In this case $(x_2, y_2) = ((1/\lambda)x_1, (1/\lambda)y_1)$. Thus, $(x_2, y_2) \sim (x_1, y_1)$. To show that the relation is transitive, let $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then $(x_1, y_1) = (\lambda x_2, \lambda y_2)$ and $(x_2, y_2) = (\mu x_3, \mu y_3)$. Since $(x_1, y_1) = (\lambda\mu x_3, \lambda\mu y_3)$, $(x_1, y_1) \sim (x_3, y_3)$. The corresponding equivalence classes are straight lines through the origin.

1.5 Sage Exercises

1. This exercise is just about making sure you know how to use Sage. You may be using the Sage Notebook server the online CoCalc service through your web browser. In either event, create a new worksheet. Do some non-trivial computation, maybe a pretty plot or some gruesome numerical computation to an insane precision. Create an interesting list and experiment with it some. Maybe include some nicely formatted text or TEX using the included mini-word-processor of the Sage Notebook (hover until a blue bar appears between cells and then shift-click) or create commentary in cells within CoCalc using the **magics** `%html` or `%md` on a line of their own followed by text in HTML or Markdown syntax (respectively).

Use whatever mechanism your instructor has in place for submitting your work. Or save your worksheet and then trade with a classmate.

Solution. You might get back lists of food items, a bucket list, or a list of campus buildings. Or perhaps an implementation of the Ackermann function and a computation of $A(4, 2)$. Casey Wall submitted this plot:

```
n = 40
colors = rainbow(n)
sum([plot(x^k, (0,1), color=colors[k]) for k in srange(n)])
```

```
Graphics object consisting of 40 graphics primitives
```

Chapter 2

The Integers

2.3 Exercises

1. Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for $n \in \mathbb{N}$.

Hint. The base case, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$ is true. Assume that $S(k) : 1^2 + 2^2 + \cdots + k^2 = [k(k+1)(2k+1)]/6$ is true. Then

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

and so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

Solution. The base case, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$ is true. Assume that $S(k) : 1^2 + 2^2 + \cdots + k^2 = [k(k+1)(2k+1)]/6$ is true. Then

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

and so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

2. Prove that

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

for $n \in \mathbb{N}$.

Solution. The base case, $S(1) : [1^2(1+1)^2]/4 = 1 = 1^3$ is true. Assume $S(k) : 1^3+2^3+\cdots+k^3 = [k^2(k+1)^2]/4$ is true. Then $1^3+2^3+\cdots+k^3+(k+1)^3 = [k^2(k+1)^2]/4 + (k+1)^3 = [(k+1)^2((k+1)+1)^2)]/4$, so $S(k+1)$ is true. Consequently, $S(n)$ is true for all positive integers n.

3. Prove that $n! > 2^n$ for $n \geq 4$.

Hint. The base case, $S(4) : 4! = 24 > 16 = 2^4$ is true. Assume $S(k) : k! > 2^k$ is true. Then $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

Solution. The base case, $S(4) : 4! = 24 > 16 = 2^4$ is true. Assume $S(k) : k! > 2^k$ is true. Then $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

4. Prove that

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

for $n \in \mathbb{N}$.

Solution. The base case, $S(1) : x = [1(3-1)x]/2$ is true. Assume $S(k) : x+4x+\cdots+(3k-2)x = [k(3k-1)x]/2$ is true. Then $x+4x+\cdots+(3k-2)x+(3(k+1)-2)x = [k(3k-1)x]/2 + (3(k+1)-2)x = [(k+1)(3(k+1)-1)x]/2$ is true, so $S(k+1)$ is true. Therefore, $S(n)$ is true for all positive integers n.

5. Prove that $10^{n+1} + 10^n + 1$ is divisible by 3 for $n \in \mathbb{N}$.

Solution. If $n = 1$, then $10^{n+1}+10^n+1 = 111$ is divisible by 3. Assume that $10^{k+1} + 10^k + 1$ is divisible by 3 for $1 \leq k \leq n$. Then $10^{(n+1)+1} + 10^{n+1} + 1 = 10(10^{n+1} + 10^n + 1) - 9$ is divisible by 3.

6. Prove that $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99 for $n \in \mathbb{N}$.

Solution. If $n = 1$, then $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5 = 495$ is divisible by 99. If we assume the result is true for all k with $1 \leq k \leq n$, then

$$4 \cdot 10^{2(n+1)} + 9 \cdot 10^{2(n+1)-1} + 5 = 10^2(4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5) - 495$$

is divisible by 99.

7. Show that

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k.$$

Solution. Let

$$A_n = \frac{a_1 + \cdots + a_n}{n}$$

and

$$G_n = \sqrt[n]{a_1 \cdots a_n}.$$

If $n = 2$, then $a_1 - 2\sqrt{a_1 a_2} + a_2 = (\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$. Therefore, $(a_1 + a_2)/2 \geq \sqrt{a_1 a_2}$. The next step is to prove the inequality for $n = 2^k$ by induction on k. Now let $2^m \geq n$. Now apply the last step to the 2^m numbers

$$a_1, \cdots, a_n, \underbrace{A_n, \cdots, A_n}_{2^m - n \text{ times}}$$

to show that $G_n \leq A_n$ for n in general.

8. Prove the Leibniz rule for $f^{(n)}(x)$, where $f^{(n)}$ is the nth derivative of f; that is, show that

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x).$$

Hint. Follow the proof in Example 2.4.

Solution. Follow the proof in Example 2.4.

9. Use induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \in \mathbb{N}$.

Solution. The base case, $S(1) : 1 + 2 = 3 = 2^{1+1} - 1$ is true. Assume $S(k) : 1+2+2^2+\cdots+2^k = 2^{k-1}-1$ is true. Then $1+2+2^2+\cdots+2^k+2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2^{(k+1)+1} - 1$, so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

10. Prove that

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for $n \in \mathbb{N}$.

Solution. The base case, $S(1) : 1/2 = 1/(1+1)$ is true. Assume that

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$$

is true. Then

$$\begin{aligned}\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)[(k+1)+1]} &= \frac{k}{k+1} + \frac{1}{(k+1)[(k+1)+1]} \\ &= \frac{k+1}{(k+1)+1}.\end{aligned}$$

so $S(k+1)$ is true. Thus, $S(n)$ is true for all positive integers n.

11. If x is a nonnegative real number, then show that $(1+x)^n - 1 \geq nx$ for $n = 0, 1, 2, \ldots$.

Hint. The base case, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$ is true. Assume $S(k) : (1+x)^k - 1 \geq kx$ is true. Then

$$\begin{aligned}(1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1 \\ &= (1+x)^k + x(1+x)^k - 1 \\ &\geq kx + x(1+x)^k \\ &\geq kx + x \\ &= (k+1)x,\end{aligned}$$

so $S(k+1)$ is true. Therefore, $S(n)$ is true for all positive integers n.

Solution. The base case, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$ is true. Assume $S(k) : (1+x)^k - 1 \geq kx$ is true. Then

$$\begin{aligned}(1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1 \\ &= (1+x)^k + x(1+x)^k - 1 \\ &\geq kx + x(1+x)^k \\ &\geq kx + x \\ &= (k+1)x,\end{aligned}$$

so $S(k+1)$ is true. Therefore, $S(n)$ is true for all positive integers n.

12. **Power Sets.** Let X be a set. Define the **power set** of X, denoted $\mathcal{P}(X)$, to be the set of all subsets of X. For example,

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

For every positive integer n, show that a set with exactly n elements has a power set with exactly 2^n elements.

Solution. The result is certainly true for $|X| = 2$. If $X_2 = \{x_1, x_2\}$, then $\mathcal{P}(X_2) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_1, x_2\}\}$. Now suppose that the result holds for a set with k elements for $k \geq 2$, say $X_k = \{x_1, x_2, \ldots, x_k\}$. The power set of $X_{k+1} = \{x_1, x_2, \ldots, x_{k+1}\}$ consists of all of the sets A and $A \cup \{x_{k+1}\}$, where $A \in \mathcal{P}(X_k)$. Thus, $|\mathcal{P}(x_{k+1})| = 2 \cdot |\mathcal{P}(x_k)| = 2 \cdot 2^k = 2^{k+1}$, and the result follows by induction.

13. Prove that the two principles of mathematical induction stated in Section 2.1 are equivalent.

Solution. It is clear that the Second Principle of Mathematical Induction implies the First Principle of Mathematical Induction. Assume that the First Principle of Mathematical Induction. Let $S(n)$ be a statement about the integers for $n \in \mathbb{N}$ and assume that

(a) $S(n_0)$ is a true statement for some integer n_0;

(b) $S(n_0)$, $S(n_0+1)$, ..., $S(k)$ imply that $S(k+1)$ is true for $k \geq n_0$.

For each $k \geq n_0$, let $T(k)$ be the statement that $S(n_0)$, $S(n_0+1)$, ..., $S(k)$ are true. Apply the First Principle of Mathematical Induction to $T(n)$.

14. Show that the Principle of Well-Ordering for the natural numbers implies that 1 is the smallest natural number. Use this result to show that the Principle of Well-Ordering implies the Principle of Mathematical Induction; that is, show that if $S \subset \mathbb{N}$ such that $1 \in S$ and $n+1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

Solution. It is easy to show that $1 > 0$. Let $S = \{x \in \mathbb{N} : 0 < x < 1\}$. If $S = \emptyset$, then 1 is the smallest positive integer. Otherwise, by the Law of Well-Ordering, there exists a smallest integer n such that $0 < n < 1$. Consequently, $0 < n^2 < n \cdot 1 < 1$. In this case, $n^2 \in S$ and $n^2 < n$, which contradicts the fact that n is the smallest element of S.

To show the Principle of Mathematical Induction, Let $X = \mathbb{N} \setminus S$. If $X = \emptyset$, then we are done. Otherwise, we can choose a smallest element $p \in X$. Since $1 \in S$, $p-1$ is in $\mathbb{N}$ but not in X. However, we know that $p = (p-1)+1$ is in S by the hypothesis of Mathematical Induction. This contradicts the fact that $X \neq \emptyset$.

15. For each of the following pairs of numbers a and b, calculate $\gcd(a,b)$ and find integers r and s such that $\gcd(a,b) = ra + sb$.

(a) 14 and 39

(b) 234 and 165

(c) 1739 and 9923

(d) 471 and 562

(e) 23,771 and 19,945

(f) -4357 and 3754

Solution.

(a) $(14)14 + (-5)39 = 1$

(b) $(12)234 + (-17)165 = 3$

(c) $(3709)1739 + (-650)9923 = 1$

(d) $(-105)471 + (88)562 = 1$

(e) $(881)23771 + (-1050)19945 = 1$

(f) $(-2291)(-4357)+(-2659)3754 = 1$

Other solutions are possible.

16. Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

Solution. If d divides both a and b, then there exist integers u and v such that $a = ud$ and $b = vd$. Thus, $1 = ar + bs = udr + vds = d(ur + vs)$, and $d = \pm 1$.

17. **Fibonacci Numbers.** The Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

We can define them inductively by $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$.

(a) Prove that $f_n < 2^n$.

(b) Prove that $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$, $n \geq 2$.

(c) Prove that $f_n = [(1+\sqrt{5}\,)^n - (1-\sqrt{5}\,)^n]/2^n\sqrt{5}$.

(d) Show that $\lim_{n\to\infty} f_n/f_{n+1} = (\sqrt{5}-1)/2$.

(e) Prove that f_n and f_{n+1} are relatively prime.

Hint. For (a) and (b) use mathematical induction. (c) Show that $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$. (d) Use part (c). (e) Use part (b) and Exercise 2.3.16.

Solution. For (a) and (b) use mathematical induction. (c) Show that $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$. (d) Use part (c). (e) Use part (b) and Exercise 2.3.16.

18. Let a and b be integers such that $\gcd(a, b) = 1$. Let r and s be integers such that $ar + bs = 1$. Prove that

$$\gcd(a, s) = \gcd(r, b) = \gcd(r, s) = 1.$$

Solution. Use Exercise 2.3.16.

19. Let $x, y \in \mathbb{N}$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

Hint. Use the Fundamental Theorem of Arithmetic.

Solution. Use the Fundamental Theorem of Arithmetic.

20. Using the division algorithm, show that every perfect square is of the form $4k$ or $4k + 1$ for some nonnegative integer k.

Solution. If n is even, then it can be written as $2p$ for some $p \in \mathbb{N}$. In this case $n^2 = 4p^2$. Similarly, if n is odd, it can be written as $n = 2p - 1$ for some $p \in \mathbb{N}$. Then $n^2 = (2p-1)^2 = 4p^2 - 4p + 1 = 4(p^2 - p) + 1$.

21. Suppose that a, b, r, s are pairwise relatively prime and that

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

Prove that a, r, and s are odd and b is even.

Solution. First note that $2b^2 = r^2 - s^2 = (r-s)(r+s)$; hence, r and s must both be odd since r and s are relatively prime. So b^2 is even, which says that b is even. Since $a^2 + b^2 = r^2$ is odd, a must be odd.

22. Let $n \in \mathbb{N}$. Use the division algorithm to prove that every integer is congruent mod n to precisely one of the integers $0, 1, \ldots, n-1$. Conclude that if r is an integer, then there is exactly one s in $\mathbb{Z}$ such that $0 \le s < n$ and $[r] = [s]$. Hence, the integers are indeed partitioned by congruence mod n.

Solution. Let $k \in \mathbb{N}$. By the division algorithm, there exist unique integers q and r such that $k = qn + r$, where $0 \le r < n$. Thus $[r] = [k]$.

23. Define the **least common multiple** of two nonzero integers a and b, denoted by $\operatorname{lcm}(a, b)$, to be the nonnegative integer m such that both a and b divide m, and if a and b divide any other integer n, then m also divides n. Prove there exists a unique least common multiple for any two integers a and b.

Hint. Use the Principle of Well-Ordering and the division algorithm.

Solution. Let $S = \{s \in \mathbb{N} : a \mid s,\ b \mid s\}$. Then $S \neq \emptyset$, since $|ab| \in S$. By the Principle of Well-Ordering, S contains a least element m. To show uniqueness, suppose that $a \mid n$ and $b \mid n$ for some $n \in \mathbb{N}$. By the division algorithm, there exist unique integers q and r such that $n = mq + r$, where $0 \le r < m$. Since a and b divide both m, and n, it must be the case that a and b both divide r. Thus, $r = 0$ by the minimality of m. Therefore, $m \mid n$.

24. If $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$, prove that $dm = |ab|$.

Solution. By the Fundamental Theorem of Arithmetic, $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where the p_is are distinct primes and the exponents may possibly be zero. Then $m = \text{lcm}(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ and $d = \gcd(a, b) = p_1^{\delta_1} \cdots p_k^{\delta_k}$, where $\gamma_i = \max(\alpha_i, \beta_i)$ and $\delta_i = \min(\alpha_i, \beta_i)$. Hence, $ab = p_1^{\gamma_1+\delta_1} \cdots p_k^{\gamma_k+\delta_k} = dm$.

25. Show that $\text{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

Solution. Use Exercise 2.3.24.

26. Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$ for integers a, b, and c.

Solution. If $\gcd(a, c) = \gcd(b, c) = 1$, then there exist integers r, s, t, u such that $ar + cs = 1$ and $bt + cu = 1$. Since

$$(ar + cs)(bt + cu) = ab(rt) + c(bst + aru + csu) = 1,$$

it must be the case that $\gcd(ab, c) = 1$.

Conversely, if $\gcd(ab, c) = 1$, there exist integers k and l such that

$$abk + cl = a(bk) + cl = b(ak) + cl = 1.$$

Thus, $\gcd(a, c) = \gcd(b, c) = 1$.

27. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Hint. Since $\gcd(a, b) = 1$, there exist integers r and s such that $ar + bs = 1$. Thus, $acr + bcs = c$.

Solution. Since $\gcd(a, b) = 1$, there exist integers r and s such that $ar+bs = 1$. In addition, since a divides bc, there exists an integer k such that $ak = bc$. Thus,

$$\begin{aligned} c &= c \cdot 1 \\ &= c(ar + bs) \\ &= acr + bcs \\ &= acr + aks \\ &= a(cr + ks), \end{aligned}$$

and $a \mid c$.

28. Let $p \geq 2$. Prove that if $2^p - 1$ is prime, then p must also be prime.

Solution. If $p = rs$ with r and s greater than 1, then

$$2^p - 1 = 2^{rs} - 1 = (2^r - 1)(2^{rs-1} + 2^{rs-2} + \cdots + 2 + 1),$$

which contradicts the fact that $2^p - 1$ is prime.

29. Prove that there are an infinite number of primes of the form $6n + 5$.

Hint. Every prime must be of the form 2, 3, $6n+1$, or $6n+5$. Suppose there are only finitely many primes of the form $6k + 5$.

Solution. Every prime must be of the form 2, 3, $6n + 1$, or $6n + 5$. Suppose there are only finitely many primes of the form $6n + 5$, say $p_1, \ldots, p_k$. If $N = 6p_1 \cdots p_k - 1$, then N is of the form $6n + 5$ and $N > p_i$ for $i = 1, \ldots, k$. Furthermore, N is not divisible by 2, 3, or any of the p_is. Therefore, must be a product of primes the form $6n + 1$. This is impossible since any product numbers of the form $6n + 1$ is still of the form $6n + 1$.

30. Prove that there are an infinite number of primes of the form $4n - 1$.

Solution. Every prime must be of the form 2, $4n+1$, or $4n-1 = 4n+3$. Suppose there are only finitely many primes of the form $4n+3$, say $p_1, \ldots, p_k$. If $N = 4p_1 \cdots p_k - 1$, then N is of the form $4n+3$ and $N > p_i$ for $i = 1, \ldots, k$. Furthermore, N is not divisible by 2 or by any of the p_is. Therefore, must be a product of primes the form $4n+1$. This is impossible since any product numbers of the form $4n+1$ is still of the form $4n+1$.

31. Using the fact that 2 is prime, show that there do not exist integers p and q such that $p^2 = 2q^2$. Demonstrate that therefore $\sqrt{2}$ cannot be a rational number.

Solution. Suppose that p and q are relatively prime and $p^2 = 2q^2$. Then p must be even; therefore, we can write $p = 2r$ for some integer r. Thus, $q^2 = 2p^2$ and q is also even, which contradicts the fact that p and q were relatively prime.

2.6 Sage Exercises

These exercises are about investigating basic properties of the integers, something we will frequently do when investigating groups. Sage worksheets have extensive capabilities for making new cells with carefully formatted text, include support for LaTeX syntax to express mathematics. So when a question asks for explanation or commentary, make a new cell and communicate clearly with your audience.**1**. Use the `next_prime()` command to construct two different 8-digit prime numbers and save them in variables named `a` and `b`.

Solution. One common answer is:

```
a = next_prime(10^7)
b = next_prime(a)
(a, b)
```

```
(10000019, 10000079)
```

2. Use the `is_prime()` method to verify that your primes `a` and `b` are really prime.

3. Verify that 1 is the greatest common divisor of your two primes from the previous exercises.

Solution.

```
gcd(a, b)
```

```
1
```

4. Find two integers that make a "linear combination" of your two primes equal to 1. Include a verification of your result.

Solution.

```
d, r, s = xgcd(a, b)
r, s
```

```
(-166668, 166667)
```

```
r*a + s*b == 1
```

```
True
```

5. Determine a factorization into powers of primes for $c = 4\,598\,037\,234$.

Solution.

```
c = 4598037234
c.factor()
```

```
2 * 3^2 * 7 * 36492359
```

6. Write a compute cell that defines the same value of `c` again, and then defines a candidate divisor of `c` named `d`. The third line of the cell should return `True` if and only if `d` is a divisor of `c`. Illustrate the use of your cell by testing your code with $d = 7$ and in a new copy of the cell, testing your code with $d = 11$.

Solution. Two possible solutions:

```
c = 4598037234
d = 7
c % d == 0
```

```
True
```

```
c = 4598037234
d = 11
d.divides(c)
```

```
False
```

Chapter 3

Groups

3.4 Exercises

1. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3x \equiv 2 \pmod 7$

(b) $5x + 1 \equiv 13 \pmod{23}$

(c) $5x + 1 \equiv 13 \pmod{26}$

(d) $9x \equiv 3 \pmod 5$

(e) $5x \equiv 1 \pmod 6$

(f) $3x \equiv 1 \pmod 6$

Hint. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (c) $18 + 26\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$.

Solution. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (b) $7 + 23\mathbb{Z}$; (c) $18 + 26\mathbb{Z}$; (d) $2 + 5\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$; (f) no solution.

2. Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

Hint. (a) Not a group; (c) a group.

Solution. (a) Not a group; (b) a group; (c) a group; (d) not a group.

3. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

Solution. For $\mathbb{Z}_4$, the Cayley table is

$+$	0	1	3	3
0	0	1	2	3
1	1	2	3	0
2	3	0	1	2
3	0	1	2	3

If id is the identity motion, ρ_1 the reflection about the vertical axis, ρ_2 the refection about the horizontal axis, and ρ_3 a 180° rotation, then the Cayley table for the symmetries of a rectangle is

	id	ρ_1	ρ_2	ρ_3
id	id	ρ_1	ρ_2	ρ_3
ρ_1	ρ_1	id	ρ_3	ρ_2
ρ_2	ρ_2	ρ_3	id	ρ_1
ρ_3	ρ_3	ρ_2	ρ_1	id

Notice that the square of every element is the identity in the symmetry group of a rectangle. This property does not hold in $\mathbb{Z}_4$.

4. Describe the symmetries of a rhombus and prove that the set of symmetries forms a group. Give Cayley tables for both the symmetries of a rectangle and the symmetries of a rhombus. Are the symmetries of a rectangle and those of a rhombus the same?

Solution. The symmetries of a rectangle are described in the solution to Exercise 3.4.3. The symmetries of a rhombus can be described by the following Cayley Table, where id is the identity motion, μ_1 the reflection about one diagonal, μ_2 the refection about the second diagonal axis, and μ_3 a 180° rotation, then the Cayley table for the

	id	μ_1	μ_2	μ_3
id	id	μ_1	μ_2	μ_3
μ_1	μ_1	id	μ_3	μ_2
μ_2	μ_2	μ_3	id	μ_1
μ_3	μ_3	μ_2	μ_1	id

The symmetries are indeed the same as those of the rectangle.

5. Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

Solution. The symmetry group of a square is described by the following Cayley table, where

$$
\begin{aligned}
id &= \text{ the identity} \\
\rho_1 &= \text{ a } 90^\circ \text{ clockwise rotation} \\
\rho_2 &= \text{ a } 180^\circ \text{ clockwise rotation} \\
\rho_3 &= \text{ a } 270^\circ \text{ clockwise rotation} \\
\mu_1 &= \text{ a reflection about the horizontal axis} \\
\mu_2 &= \text{ a reflection about the vertical axis} \\
\mu_3 &= \text{ a reflection about the diagonal} \\
\mu_4 &= \text{ a reflection about the diagonal.}
\end{aligned}
$$

	id	ρ_1	ρ_2	ρ_3	μ_1	μ_2	μ_3	μ_4
id	id	ρ_1	ρ_2	ρ_3	μ_1	μ_2	μ_3	μ_4
ρ_1	ρ_1	ρ_2	ρ_3	id	μ_3	μ_4	μ_2	μ_1
ρ_2	ρ_2	ρ_3	id	ρ_1	μ_2	μ_1	μ_4	μ_3
ρ_3	ρ_3	id	ρ_1	ρ_2	μ_4	μ_3	μ_1	μ_2
μ_1	μ_1	μ_4	μ_2	μ_3	id	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_3	μ_1	μ_4	ρ_2	id	ρ_1	ρ_3
μ_3	μ_3	μ_1	μ_4	μ_2	ρ_1	ρ_3	id	ρ_2
μ_4	μ_4	μ_2	μ_3	μ_1	ρ_3	ρ_1	ρ_2	id

Since the vertices of a square can be permuted 24 ways and there are only 8 symmetries of a square, not every permutation of the vertices is a symmetry.

6. Give a multiplication table for the group $U(12)$.

Hint.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Solution.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution. The identity of S is 0, and $a^{-1} = -a/(a+1)$. To show that the operation is closed, suppose that $a * b = -1$. Then $a * b = a + b + ab$. If $a \neq -1$, then $b = -(a+1)/(a+1) = -1$, which is impossible. It is straightforward to show that the operation is associative.

8. Give an example of two elements A and B in $GL_2(\mathbb{R})$ with $AB \neq BA$.

Hint. Pick two matrices. Almost any pair will work.

Solution. Pick two matrices. Almost any pair will work.

9. Prove that the product of two matrices in $SL_2(\mathbb{R})$ has determinant one.

Solution. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

where $\det A = \det B = 1$. Then

$$AB = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}.$$

Thus,

$$\begin{aligned} \det(AB) &= (ax + bz)(cy + dw) - (ay + bw)(cx + dz) \\ &= (ad - bc)(xw - yz) \\ &= 1. \end{aligned}$$

10. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

is a group under matrix multiplication. This group, known as the **Heisenberg group**, is important in quantum physics. Matrix multiplication in the Heisenberg group is defined by

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{pmatrix}.$$

Solution. This group is actually a subgroup of $SL_3(\mathbb{R})$. If

$$A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix},$$

then

$$B^{-1} = \begin{pmatrix} 1 & -x' & x'z'-y' \\ 0 & 1 & -z' \\ 0 & 0 & 1 \end{pmatrix}$$

and $\det A = 1$. Since

$$AB^{-1} = \begin{pmatrix} 1 & x-x' & x'z'-y'-xz'+y \\ 0 & 1 & z-z' \\ 0 & 0 & 1 \end{pmatrix}$$

is in the Heisenberg group, this group is a subgroup of the special linear group.

11. Prove that $\det(AB) = \det(A)\det(B)$ in $GL_2(\mathbb{R})$. Use this result to show that the binary operation in the group $GL_2(\mathbb{R})$ is closed; that is, if A and B are in $GL_2(\mathbb{R})$, then $AB \in GL_2(\mathbb{R})$.

Solution. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

then

$$\begin{aligned} (\det A)(\det B) &= (ad-bc)(a'd'-b'c') \\ &= aa'dd' - ab'c'd - a'bcd' + bb'cc' \\ &= (aa'+bc')(b'c+dd') - (a'c+c'd)(ab'+bd') \\ &= \det(AB). \end{aligned}$$

12. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n).$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation. This group is important in algebraic coding theory.

Solution. The identity of $\mathbb{Z}_2^n$ is $(0, 0, \ldots, 0)$. The inverse of $(a_1, a_2, \ldots, a_n)$ is itself. It is easy to show that the operation is associative.

13. Show that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under the operation of multiplication.

Solution. The identity of $\mathbb{R}^*$ is 1. The inverse of $a \in \mathbb{R}^*$ is $1/a$. It is easy to show that the operation is associative.

14. Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation $\circ$ on G by $(a, m) \circ (b, n) = (ab, m + n)$. Show that G is a group under this operation.

Solution. The identity of G is $(1, 0)$. If $g = (a, n)$ is in G, then $g^{-1} = (1/a, -n)$. Associativity is straightforward.

15. Prove or disprove that every group containing six elements is abelian.

Hint. There is a nonabelian group containing six elements.

Solution. The symmetries of an equilateral triangle form a group of order six that is not abelian.

16. Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$.

Hint. Look at the symmetry group of an equilateral triangle or a square.

Solution. Look at the symmetry group of an equilateral triangle or a square.

17. Give an example of three different groups with eight elements. Why are the groups different?

Hint. The are five different groups of order 8.

Solution. There are five groups of order 8 that are different: S_3, Q_8, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

18. Show that there are $n!$ permutations of a set containing n items.

Hint. Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

be in S_n. All of the a_is must be distinct. There are n ways to choose a_1, $n-1$ ways to choose a_2, ..., 2 ways to choose a_{n-1}, and only one way to choose a_n. Therefore, we can form σ in $n(n-1)\cdots 2 \cdot 1 = n!$ ways.

Solution. Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

be in S_n. All of the a_is must be distinct. There are n ways to choose a_1, $n-1$ ways to choose a_2, ..., 2 ways to choose a_{n-1}, and only one way to choose a_n. Therefore, we can form σ in $n(n-1)\cdots 2 \cdot 1 = n!$ ways.

19. Show that

$$0 + a \equiv a + 0 \equiv a \pmod{n}$$

for all $a \in \mathbb{Z}_n$.

Solution. Since $n \mid ((a+0) - a)$, it must be true that $a + 0 \equiv a \pmod{n}$ for all $a \in \mathbb{Z}_n$. Similarly, $0 + a \equiv \pmod{n}$.

20. Prove that there is a multiplicative identity for the integers modulo n:

$$a \cdot 1 \equiv a \pmod{n}.$$

Solution. Since $n \mid (a \cdot 1 - a)$, 1 is the multiplicative identity for $\mathbb{Z}_n$.

21. For each $a \in \mathbb{Z}_n$ find an element $b \in \mathbb{Z}_n$ such that

$$a + b \equiv b + a \equiv 0 \pmod{n}.$$

Solution. If $b = n - a$, then $n \mid (b - a)$.

22. Show that addition and multiplication mod n are well defined operations. That is, show that the operations do not depend on the choice of the representative from the equivalence classes mod n.

Solution. Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. We must show that $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, we know that $n \mid (b - a)$ and $n \mid (d - c)$ or $b - a = nr$ and $d - c = ns$. Thus, $(b + d) - (a + c) = n(r + s)$ or n divides $(b + d) - (a + c)$. Consequently, $a + c \equiv b + d \pmod{n}$.

To show that multiplication is well defined, observe that

$$bd = (a + nr)(c + ns) = ac + nas + nrc + n^2rs$$

or $bd - ac = n(as + rc + nrs)$. Thus, $bd - ac$ is divisible by n and $ac \equiv bd \pmod{n}$.

23. Show that addition and multiplication mod n are associative operations.

Solution. Since $n \mid [(a + (b + c)) - ((a + b) + c)]$, modular arithmetic is associative. The proof for associativity for multiplication is the same.

24. Show that multiplication distributes over addition modulo n:

$$a(b + c) \equiv ab + ac \pmod{n}.$$

Solution. Since $n \mid [a(b + c) - (ab + ac)$, multiplication distributes over addition modulo n.

25. Let a and b be elements in a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$.

Hint.

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1}) \cdots (aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b \cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}.\end{aligned}$$

Solution.

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1}) \cdots (aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b \cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}.\end{aligned}$$

26. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

Solution. If $n > 2$, then $\gcd(n, n - 1) = 1$. Hence, $n - 1$ is a unit. However, $(n - 1)^2 = n^2 - 2n + 1$. Thus, $(n - 1)^2 \equiv 1 \pmod{n}$.

27. Prove that the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

Solution. Use Proposition 3.19 and mathematical induction.

28. Prove the remainder of Proposition 3.21: if G is a group and $a, b \in G$, then the equation $xa = b$ has a unique solution in G.

Solution. If $xa = b$, then $x = xaa^{-1} = ba^{-1}$. So $x = ba^{-1}$ is a solution. If x_1 and x_2 are two solutions, then $x_1 a = x_2 a = b$, or $x_1 = x_1 aa^{-1} = x_2 aa^{-1} = x_2$.

29. Prove Theorem 3.23.

Solution. Use mathematical induction.

30. Prove the right and left cancellation laws for a group G; that is, show that in the group G, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for elements $a, b, c \in G$.

Solution. If $ba = ca$, then $baa^{-1} = caa^{-1}$. Therefore, $b = c$. The proof for left cancellation is the same.

31. Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

Hint. Since $abab = (ab)^2 = e = a^2b^2 = aabb$, we know that $ba = ab$.

Solution. Since $abab = (ab)^2 = e = a^2b^2 = aabb$, we know that $ba = ab$.

32. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.

Solution. A counting argument works here since there are an odd number of elements $a, b \in G$ not equal to the identity such that $ab = e$. For some pair $a = b$.

33. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

Solution. Since $abab = (ab)^2 = a^2b^2$, we can conclude that $ab = ba$.

34. Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$. (See Example 3.28 for a short description of the product of groups.)

Solution. The proper nontrivial subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are

$$H_1 = \{(0,0), (0,1), (0,2)\}$$
$$H_2 = \{(0,0), (1,0), (2,0)\}$$
$$H_3 = \{(0,0), (1,1), (2,2)\}.$$

The only proper nontrivial subgroup of $\mathbb{Z}_9$ is $\{0, 3, 6\}$.

35. Find all the subgroups of the symmetry group of an equilateral triangle.

Hint. $H_1 = \{\mathrm{id}\}$, $H_2 = \{\mathrm{id}, \rho_1, \rho_2\}$, $H_3 = \{\mathrm{id}, \mu_1\}$, $H_4 = \{\mathrm{id}, \mu_2\}$, $H_5 = \{\mathrm{id}, \mu_3\}$, S_3.

Solution. $H_1 = \{\mathrm{id}\}$, $H_2 = \{\mathrm{id}, \rho_1, \rho_2\}$, $H_3 = \{\mathrm{id}, \mu_1\}$, $H_4 = \{\mathrm{id}, \mu_2\}$, $H_5 = \{\mathrm{id}, \mu_3\}$, S_3.

36. Compute the subgroups of the symmetry group of a square.

Solution. The proper subgroups are $\{\mathrm{id}\}$, $\{\mathrm{id}, \rho_1, \rho_2, \rho_3\}$, $\{\mathrm{id}, \rho_2, \mu_1, \mu_2\}$, $\{\mathrm{id}, \rho_2, \mu_3, \mu_4\}\{\mathrm{id}, \rho_2\}$, $\{\mathrm{id}, \mu_1\}$, $\{id, \mu_2\}$, $\{\mathrm{id}, \mu_3\}$, $\{\mathrm{id}, \mu_4\}$, where

$id =$ the identity
$\rho_1 =$ a 90° clockwise rotation
$\rho_2 =$ a 180° clockwise rotation
$\rho_3 =$ a 270° clockwise rotation
$\mu_1 =$ a reflection about the horizontal axis
$\mu_2 =$ a reflection about the vertical axis
$\mu_3 =$ a reflection about the diagonal
$\mu_4 =$ a reflection about the diagonal.

37. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$.

Solution. $1 = 2^0 \in H$. If $2^m, 2^n \in H$, then $2^m 2^n = 2^{m+n}$ is in H. If $a = 2^n$ is in H, then $a^{-1} = 2^{-n}$ is in H.

38. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

Solution. Certainly, $0 \in n\mathbb{Z}$. If a and b are in $n\mathbb{Z}$, then $a = np$ and $b = nq$ for some $p, q \in \mathbb{Z}$. Thus, $a+b = np+nq = n(p+q)$ is in $n\mathbb{Z}$. Also, if $a = np \in n\mathbb{Z}$, then $-a = n(-p)$ is in $n\mathbb{Z}$.

39. Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

Solution. Since $|1| = 1$, $1 \in \mathbb{T}$. If $z, w \in \mathbb{T}$, then $|zw| = |z| \cdot |w| = 1$. So zw is in $\mathbb{T}$. Finally, $1/z \in \mathbb{T}$, since $|1/z| = 1/|z| = 1$.

40. Let G consist of the 2×2 matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $SL_2(\mathbb{R})$.

Solution. If

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

then

$$A^{-1} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Also

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = \begin{pmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{pmatrix}.$$

41. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Hint. The identity of G is $1 = 1 + 0\sqrt{2}$. Since $(a + b\sqrt{2}\,)(c + d\sqrt{2}\,) = (ac+2bd)+(ad+bc)\sqrt{2}$, G is closed under multiplication. Finally, $(a+b\sqrt{2}\,)^{-1} = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$.

Solution. The identity of G is $1 = 1 + 0\sqrt{2}$. Since $(a + b\sqrt{2}\,)(c + d\sqrt{2}\,) = (ac+2bd)+(ad+bc)\sqrt{2}$, G is closed under multiplication. Finally, $(a+b\sqrt{2}\,)^{-1} = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$.

42. Let G be the group of 2×2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Prove that H is a subgroup of G.

Solution. The identity

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

is in H. If

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

are in H, then

$$\begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

is also in H, since

$$(a_{11} + b_{11}) + (a_{22} + b_{22}) = (a_{11} + a_{22}) + (b_{11} + b_{22}) = 0.$$

Finally, if

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

then its inverse

$$\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

is in H.

43. Prove or disprove: $SL_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries and determinant one, is a subgroup of $SL_2(\mathbb{R})$.

Solution. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(\mathbb{Z})$, then

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

is also in $SL_2(\mathbb{R})$. The rest of the proof is straightforward.

44. List the subgroups of the quaternion group, Q_8.

Solution. The subgroups of Q_8 are $\{1\}$, $\{\pm 1\}$, $\{\pm 1, \pm I\}$, $\{\pm 1, \pm J\}$, $\{\pm 1, \pm K\}$, and Q_8.

45. Prove that the intersection of two subgroups of a group G is also a subgroup of G.

Solution. Let H and K be subgroups of a group G. Since $e \in H$ and $e \in K$, $e \in H \cap K$. If $a, b \in H \cap K$, then $a, b \in H$ and $a, b \in K$. Hence, $ab^{-1} \in H$ and $ab^{-1} \in K$. Therefore, $ab^{-1} \in H \cap K$, and $H \cap K$ is a subgroup of G.

46. Prove or disprove: If H and K are subgroups of a group G, then $H \cup K$ is a subgroup of G.

Hint. Look at S_3.

Solution. The set $H \cup K$ is not necessarily a subgroup. Consider the subgroups $H = \{\mathrm{id}, \rho_1, \rho_2\}$ and $K = \{\mathrm{id}, \mu_1\}$ contained in S_3. Then $H \cup K$ is not a subgroup of S_3.

47. Prove or disprove: If H and K are subgroups of a group G, then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G. What if G is abelian?

Solution. This is certainly not true in general. Let $H = \{\mathrm{id}, \mu_1\}$ and $K = \{\mathrm{id}, \mu_2\}$ be subgroups of S_3. Then $HK = \{\mathrm{id}, \mu_1, \mu_2, \mu_1\mu_2 = \rho_2\}$ is not a subgroup. If G is abelian, then it is straightforward to show that HK is a subgroup of G. Certainly, the identity is in HK. If $a = h_1k_1$ and $b = h_2k_2$, then

$$ab^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}k_1k_2^{-1}$$

is in HK.

48. Let G be a group and $g \in G$. Show that

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

is a subgroup of G. This subgroup is called the **center** of G.

Solution. If $x, y \in Z(G)$, then $gx = xg$ and $gy = yg$ for all $g \in G$, or, equivalently, $gxg^{-1} = x$ and $gyg^{-1} = y$. Therefore, $xy \in Z(G)$, since $gxyg^{-1} = gxg^{-1}gyg^{-1} = xy$. Also, the identity and x^{-1} are in $Z(G)$ if $x \in Z(G)$.

49. Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

Hint. $ba = a^4b = a^3ab = ab$

Solution. $ba = a^4b = a^3ab = ab$

50. Give an example of an infinite group in which every nontrivial subgroup is infinite.

Solution. The group of integers, $\mathbb{Z}$, under addition.

51. If $xy = x^{-1}y^{-1}$ for all x and y in G, prove that G must be abelian.

Solution. If $xy = x^{-1}y^{-1}$ and we let $y = e$, then $x = x^{-1}$ for all $x \in G$. Therefore, $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$.

52. Prove or disprove: Every proper subgroup of an nonabelian group is nonabelian.

Solution. False, every proper subgroup of S_3 is abelian.

53. Let H be a subgroup of G and

$$C(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Prove $C(H)$ is a subgroup of G. This subgroup is called the **centralizer** of H in G.

Solution. First note that $x \in C_G(H)$ if and only if $h^{-1}xh = h$ for all $h \in H$. We first show that $C_G(H)$ is closed under multiplication. If $x, y \in C_G(H)$, then $xy = (h^{-1}xh)(h^{-1}yh) = h^{-1}xyh$ for all $h \in H$. Thus, $xy \in C_G(H)$. The identity is $C_G(H)$ since $h^{-1}1h = 1 \in H$ for all $h \in H$. Finally, if $x \in C_G(H)$, then $xh = hx$ or all $h \in H$. Thus, $x^{-1}h = hx^{-1}$ for all $h \in H$. Hence, $x^{-1} \in C_G(H)$.

54. Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup of G.

Solution. Certainly, the identity is in gHg^{-1}. If $x \in gHg^{-1}$, then $x^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1}$ for some $h \in H$ and must also be in gHg^{-1}. Finally, if $x = gh_1g^{-1}, y = gh_2g^{-1} \in gHg^{-1}$, then $xy = gh_1h_2g^{-1} \in gHg^{-1}$.

3.7 Sage Exercises

These exercises are about becoming comfortable working with groups in Sage. Sage worksheets have extensive capabilities for making new cells with carefully formatted text, include support for LaTeX syntax to express mathematics. So when a question asks for explanation or commentary, make a new cell and communicate clearly with your audience.**1**. Create the groups `CyclicPermutationGroup(8)` and `DihedralGroup(4)` and name these groups `C` and `D`, respectively. We will understand these constructions better shortly, but for now just understand that both objects you create are actually groups.

Solution.

```
C = groups.permutation.Cyclic(8)
D = groups.permutation.Dihedral(4)
```

2. Check that `C` and `D` have the same size by using the `.order()` method. Determine which group is abelian, and which is not, by using the `.is_abelian()` method.

Solution.

```
C.order(), D.order()
```

```
(8, 8)
```

```
C.is_abelian(), D.is_abelian()
```

```
(True, False)
```

3. Use the `.cayley_table()` method to create the Cayley table for each group.

Solution.

```
C.cayley_table()
```

```
*  a b c d e f g h
 +----------------
a| a b c d e f g h
b| b c d e f g h a
c| c d e f g h a b
d| d e f g h a b c
e| e f g h a b c d
f| f g h a b c d e
g| g h a b c d e f
h| h a b c d e f g
```

```
D.cayley_table()
```

```
*  a b c d e f g h
 +----------------
a| a b c d e f g h
b| b a f h g c e d
c| c e d g h b a f
d| d h g a f e c b
e| e c b f a d h g
f| f g h e d a b c
g| g f a c b h d e
h| h d e b c g f a
```

4. Write a nicely formatted discussion identifying differences between the two groups that are discernible in properties of their Cayley tables. In other words, what is *different* about these two groups that you can "see" in the Cayley tables? (In the Sage notebook, a Shift-click on a blue bar will bring up a mini-word-processor, and you can use use dollar signs to embed mathematics formatted using TEX syntax.)

Solution. Common observations include: symmetry about the diagonal for the abelian group and not for the nonabelian group, a "cyclic" look to the rows of the table for the cyclic group, rows of the table (combined with the heading row) looking like the "two row" notation for permutations (which presages Cayley's Theorem), each element exactly once in each row and each column (Latin square), several elements of order 2 in the dihedral group.

5. For `C` locate the one subgroup of order 4. The group `D` has three subgroups of order 4. Select one of the three subgroups of `D` that has a different structure than the subgroup you obtained from `C`.

The `.subgroups()` method will give you a list of all of the subgroups to help you get started. A Cayley table will help you tell the difference between the two subgroups. What properties of these tables did you use to determine the difference in the structure of the subgroups?

Solution. The three subgroups of order 4 in the dihedral group are: one cyclic group of order 4 and two versions of the Klein 4-group.

```
L = C.subgroups()[2]
L.is_cyclic()
```

```
True
```

```
K = D.subgroups()[6]
K.is_isomorphic(KleinFourGroup())
```

```
True
```

6. The `.subgroup(elt_list)` method of a group will create the smallest subgroup containing the specified elements of the group, when given the elements as a list `elt_list`. Use this command to discover the shortest list of elements necessary to recreate the subgroups you found in the previous exercise. The equality comparison, `==`, can be used to test if two subgroups are equal.

Solution.

```
M = C.subgroup(["(1,3,5,7)(2,4,6,8)"])
M.order(), M.is_cyclic(), M.is_subgroup(L)
```

```
(4, True, True)
```

```
J = D.subgroup(["(2,4)", "(1,3)"])
J.order(), J.is_cyclic(), J.is_subgroup(K)
```

```
(4, False, True)
```

Chapter 4

Cyclic Groups

4.4 Exercises

1. Prove or disprove each of the following statements.

(a) All of the generators of $\mathbb{Z}_{60}$ are prime.

(b) $U(8)$ is cyclic.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of subgroups is finite.

Hint. (a) False; (c) false; (e) true.

Solution. (a) False, 49 is a generator. (b) False, every element other than the identity has order 2, yet $|U(8)| = 4$. (c) False. Suppose that $1/p$ is a generator for $\mathbb{Q}$. If q is relatively prime to p, we cannot write $1/q$ as a multiple of $1/p$. (d) False, every proper subgroup of S_3 is cyclic. (e) True, every infinite group has an element of infinite order or an infinite number of elements of finite order.

2. Find the order of each of the following elements.

(a) $5 \in \mathbb{Z}_{12}$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

(e) 72 in $\mathbb{Z}_{240}$

(f) 312 in $\mathbb{Z}_{471}$

Hint. (a) 12; (c) infinite; (e) 10.

Solution. (a) 12; (b) infinite; (c) infinite; (d) 4; (e) 10; (f) 157.

3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(c) All subgroups of $\mathbb{Z}_{12}$

(d) All subgroups of $\mathbb{Z}_{60}$

(e) All subgroups of $\mathbb{Z}_{13}$

(f) All subgroups of $\mathbb{Z}_{48}$

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

Hint. (a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$; (b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$; (c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$; (g) $\{1, 3, 7, 9\}$; (j) $\{1, -1, i, -i\}$.

Solution.

(a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$.

(b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$.

(c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}_{12}$.

(d) $\{0\}$, $\{0, 30\}$, $\{0, 20, 40\}$, $\{0, 15, 30, 45\}$, $\{0, 12, 24, 36, 48\}$, $\{0, 10, 20, 30, 40, 50\}$, $\{0, 8, 16, \ldots, 52\}$, $\{0, 6, 12, \ldots, 54\}$, $\{0, 5, 10, \ldots, 55\}$, $\{0, 4, 8, \ldots, 56\}$, $\{0, 3, 6, \ldots, 57\}$, $\{0, 2, 4, \ldots, 58\}$, $\mathbb{Z}_{12}$.

(e) $\{0\}$.

(f) $\{0\}$, $\{0, 24\}$, $\{0, 16, 32\}$, $\{0, 12, 24, 36\}$, $\{0, 8, 16, 24, 32, 40\}$, $\{0, 6, 12, \ldots, 42\}$, $\{0, 4, 8, \ldots, 44\}$, $\{0, 2, 4, \ldots, 46\}$.

(g) $\{1, 3, 7, 9\}$.

(h) $\{1, 5, 7, 11, 13, 17\}$.

(i) $\{7^k : k \in \mathbb{Z}\}$.

(j) $\{1, -1, i, -i\}$.

(k) $\{2^k i^k\} = \{\ldots, -2^{-1}i, 1, 2i, -2^2, -2^3 i, 2^4, 2^5 i, \ldots\}$ where $k \in \mathbb{Z}$.

(l) $\{1, -1, i, -i, \pm(1 \pm i)/\sqrt{2}\}$.

(m) $\{((2 + \sqrt{3}i)/2)^k : k \in \mathbb{Z}\}$.

4. Find the subgroups of $GL_2(\mathbb{R})$ generated by each of the following matrices.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ (e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

Hint. (a)

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

(c)

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

Solution.

(a)

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

(b)

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1/3\\ 3 & 0\end{pmatrix}.$$

(c)

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

(d) For $n \in \mathbb{Z}$,

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

(e) This is an infinite cyclic group with generator

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

(f) This is a cyclic group of order 12 with generator

$$\begin{pmatrix}\sqrt{3}/2 & 1/2\\ -1/2 & \sqrt{3}/2\end{pmatrix}$$

5. Find the order of every element in $\mathbb{Z}_{18}$.

Solution. Order 1: 0; order 2: 9; order 3: 6, 12; order 6: 3, 15; order 9: 2, 4, 8, 10, 14, 16; order 18: 1, 5, 7, 11, 13, 17.

6. Find the order of every element in the symmetry group of the square, D_4.

Solution. Elements of order 1 are id; elements of order 2 are ρ_2, μ_1, μ_2, μ_3, and μ_4; elements of order 4 are ρ_1 and ρ_3.

7. What are all of the cyclic subgroups of the quaternion group, Q_8?

Solution. Every proper subgroup of Q_8 is cyclic.

8. List all of the cyclic subgroups of $U(30)$.

Solution. The group $U(8)$ consists of elements 1, 7, 11, 13, 17, 19, 23, 29. The cyclic subgroups of $U(8)$ are $\{1\}$, $\{1, 11\}$, $\{1, 19\}$, $\{1, 29\}$, $\{1, 7, 13, 19\}$, $\{1, 17, 19, 23\}$.

9. List every generator of each subgroup of order 8 in $\mathbb{Z}_{32}$.

Solution. There is only one subgroup of order 8 in $\mathbb{Z}_{32}$, and its generators are $4, 12, 20, 28$.

10. Find all elements of finite order in each of the following groups. Here the "$*$" indicates the set with zero removed.

(a) $\mathbb{Z}$ (b) $\mathbb{Q}^*$ (c) $\mathbb{R}^*$

Hint. (a) 0; (b) $1, -1$.

Solution. (a) 0; (b) $1, -1$; (c) $1, -1$.

11. If $a^{24} = e$ in a group G, what are the possible orders of a?

Hint. 1, 2, 3, 4, 6, 8, 12, 24.

Solution. 1, 2, 3, 4, 6, 8, 12, 24.

12. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

Solution. The group $\mathbb{Z}_2$ has one generator, $\mathbb{Z}_3$ has two generators, and $\mathbb{Z}_5$ has four generators. However, there is no cyclic group with 3 generators. This problem is explored more thoroughly in Chapter 6, where the Euler ϕ-function is introduced.

13. For $n \leq 20$, which groups $U(n)$ are cyclic? Make a conjecture as to what is true in general. Can you prove your conjecture?

Solution. The groups $U(n)$ are cyclic for all $n \leq 20$ except $n = 8, 12, 15, 16, 20$. The group of units, $U(n)$ is cyclic if and only if n is 1, 2, 4, p^k, or $2p^k$ for an odd prime number p and $k \geq 1$. While the proof of this fact is more advanced, students can explore and make a conjecture using Sage.

14. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

be elements in $GL_2(\mathbb{R})$. Show that A and B have finite orders but AB does not.

Solution. Both A and B have finite order since

$$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

but AB has infinite order since

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

15. Evaluate each of the following.

(a) $(3 - 2i) + (5i - 6)$

(b) $(4 - 5i) - \overline{(4i - 4)}$

(c) $(5 - 4i)(7 + 2i)$

(d) $(9 - i)\overline{(9 - i)}$

(e) i^{45}

(f) $(1 + i) + \overline{(1 + i)}$

Hint. (a) $-3 + 3i$; (c) $43 - 18i$; (e) i

Solution. (a) $3i - 3$; (b) $8 - i$; (c) $43 - 18i$; (d) 82; (e) i; (f) 2.

16. Convert the following complex numbers to the form $a + bi$.

(a) $2\,\mathrm{cis}(\pi/6)$

(b) $5\,\mathrm{cis}(9\pi/4)$

(c) $3\,\mathrm{cis}(\pi)$

(d) $\mathrm{cis}(7\pi/4)/2$

Hint. (a) $\sqrt{3} + i$; (c) -3.

Solution. (a) $\sqrt{3} + i$; (b) $(5\sqrt{2} + 5\sqrt{2}\,i)/2$; (c) -3; (d) $(\sqrt{2} - \sqrt{2}\,i)/4$.

17. Change the following complex numbers to polar representation.

(a) $1-i$ (c) $2+2i$ (e) $-3i$

(b) -5 (d) $\sqrt{3}+i$ (f) $2i+2\sqrt{3}$

Hint. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (e) $3\,\mathrm{cis}(3\pi/2)$.

Solution. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (b) $5\,\mathrm{cis}\,\pi$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (d) $2\,\mathrm{cis}(\pi/3)$; (e) $3\,\mathrm{cis}(3\pi/2)$; (f) $4\,\mathrm{cis}(\pi/3)$.

18. Calculate each of the following expressions.

(a) $(1+i)^{-1}$ (e) $((1-i)/2)^4$

(b) $(1-i)^6$ (f) $(-\sqrt{2}-\sqrt{2}\,i)^{12}$

(c) $(\sqrt{3}+i)^5$

(d) $(-i)^{10}$ (g) $(-2+2i)^{-5}$

Hint. (a) $(1-i)/2$; (c) $16(i-\sqrt{3}\,)$; (e) $-1/4$.

Solution. (a) $(1-i)/2$; (b) $8i$; (c) $16(i-\sqrt{3}\,)$; (d) -1; (e) $-1/4$; (f) -4096; (g) $(1+i)/256$.

19. Prove each of the following statements.

(a) $|z| = |\overline{z}|$ (d) $|z+w| \le |z| + |w|$

(b) $z\overline{z} = |z|^2$ (e) $|z-w| \ge ||z| - |w||$

(c) $z^{-1} = \overline{z}/|z|^2$ (f) $|zw| = |z||w|$

Solution.

(a) If $z = a+bi$, then $|z|^2 = a^2+b^2 = a^2+(-b)^2 = |\overline{z}|^2$. Thus, $|z| = |\overline{z}|$

(b) Notice that $z\overline{z} = (a+bi)(a-bi) = a^2+b^2 = |z|^2$.

(c) This follows from the fact that

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{\overline{z}z} = \frac{\overline{z}}{|z|^2}.$$

(d) First show that $z\overline{w} + \overline{z}w = z\overline{w} + \overline{z\overline{w}}$ is twice the real part of $z\overline{w}$, then conclude that $z\overline{w} + \overline{z}w \le 2|z\overline{w}| = 2|z||w|$. Now observe that

$$\begin{aligned} 0 &\le |z+w|^2 \\ &= (z+w)\overline{(z+w)} \\ &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w} \\ &= |z|^2 + z\overline{w} + \overline{z}w + |w|^2 \le |z|^2 + 2|z||w| + |w|^2 \\ &= (|z|+|w|)^2. \end{aligned}$$

(e) Since $|z| = |z-w+w| \le |z-w| + |w|$, it follows that $|z| - |w| \le |z-w|$.

(f) This follows from $(|z||w|)^2 = |z|^2|w|^2 = z\overline{z}w\overline{w} = zw\overline{zw} = |zw|^2$.

20. List and graph the 6th roots of unity. What are the generators of this group? What are the primitive 6th roots of unity?

Solution. The 6th roots of unity are $\pm 1, (\pm 1 \pm \sqrt{3}\,)/2$. The primitive 6th roots of unity are $(1 \pm \sqrt{3}\,)/2$.

21. List and graph the 5th roots of unity. What are the generators of this group? What are the primitive 5th roots of unity?

Solution. The 5th roots of unity are $\operatorname{cis}(n\theta)$, where $n = 0, 1, 2, 3, 4$. All 5th roots of unity are primitive except $\operatorname{cis} 0 = 1$.

22. Calculate each of the following.

(a) $292^{3171} \pmod{582}$

(b) $2557^{341} \pmod{5681}$

(c) $2071^{9521} \pmod{4724}$

(d) $971^{321} \pmod{765}$

Hint. (a) 292; (c) 1523.

Solution. (a) 292; (b) 2876; (c) 1523; (d) 206.

23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.

Solution.

(a) If the order of a is n, then $a^n = e$ or equivalently $(a^{-1})^n = (a^n)^{-1} = e$.

(b) If the order of a is n, then $a^n = e$. This is true exactly when

$$(g^{-1}ag)^n = (g^{-1}ag)(g^{-1}ag)\cdots(g^{-1}ag) = g^{-1}a^n g = g^{-1}eg = g^{-1}g = e.$$

(c) We know that $(ab)^n = e$ if and only if $b(ab)^n = (ba)^n b = b$, which is equivalent to $(ba)^n = e$.

24. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

Solution. We must count the integers that are less than pq and are relatively prime to pq. These are the integers that are not multiples of p or q. Since there are $p - 1$ multiples of q and $q - 1$ multiples of p, there are

$$(pq - 1) - (p - 1) - (q - 1) = (p - 1)(q - 1)$$

distinct generators of $\mathbb{Z}_{pq}$.

25. Let p be prime and r be a positive integer. How many generators does $\mathbb{Z}_{p^r}$ have?

Solution. The group $\mathbb{Z}_{p^r}$ has $(p - 1)^r$ distinct generators.

26. Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

Solution. Any subgroup of $\mathbb{Z}_p$ must be cyclic of order dividing p; however, the only numbers that divide p are 1 and p. Hence, any subgroup of $\mathbb{Z}_p$ must either have order 1 or order p.

27. If g and h have orders 15 and 16 respectively in a group G, what is the order of $\langle g \rangle \cap \langle h \rangle$?

Hint. $|\langle g \rangle \cap \langle h \rangle| = 1$.

Solution. Every element in $\langle g \rangle$ must have order 1, 3, 5, or 15. Similarly, every element in $\langle h \rangle$ must have order 1, 2, 4, 8, or 16. Hence, if $a \in \langle g \rangle \cap \langle h \rangle$, then a must have order 1, or $|\langle g \rangle \cap \langle h \rangle| = 1$.

28. Let a be an element in a group G. What is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

Solution. We claim that the element $a^{\text{lcm}(m,n)}$ is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$. Since $m \mid \text{lcm}(m,n)$, it must be the case that $\langle a^{\text{lcm}(m,n)} \rangle \subset \langle a^m \rangle$. Similarly, $\langle a^{\text{lcm}(m,n)} \rangle \subset \langle a^n \rangle$. Thus, $\langle a^{\text{lcm}(m,n)} \rangle \subset \langle a^m \rangle \cap \langle a^n \rangle$. On the other hand, suppose that $b = a^k \in \langle a^m \rangle \cap \langle a^n \rangle$. Then both m and n must divide k. Therefore, $\text{lcm}(m,n) \mid k$, and $a^k \in \langle a^{\text{lcm}(m,n)} \rangle$. Consequently, $\langle a^m \rangle \cap \langle a^n \rangle \subset \langle a^{\text{lcm}(m,n)} \rangle$.

29. Prove that $\mathbb{Z}_n$ has an even number of generators for $n > 2$.

Solution. If a is a generator for $\mathbb{Z}_m$, then $-a$ must also be a generator. We claim that a and $-a$ must be distinct. If not, then the order of a is 2, which tells us that a cannot generate $\mathbb{Z}_n$ since $n > 2$.

30. Suppose that G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m,n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution. If $g \in \langle a \rangle \cap \langle b \rangle$, then the order of g divides m and n. Since $\gcd(m,n) = 1$, the order of g is 1. The only element of order 1 is the identity.

31. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

Hint. The identity element in any group has finite order. Let $g, h \in G$ have orders m and n, respectively. Since $(g^{-1})^m = e$ and $(gh)^{mn} = e$, the elements of finite order in G form a subgroup of G.

Solution. The identity element in any group has finite order. Let $g, h \in G$ have orders m and n, respectively. Since $(g^{-1})^m = e$ and $(gh)^{mn} = e$, the elements of finite order in G form a subgroup of G.

32. Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $\gcd(k,n) = 1$, then y must be a generator of G.

Solution. The proof follows directly from Theorem 4.13.

33. If G is an abelian group that contains a pair of cyclic subgroups of order 2, show that G must contain a subgroup of order 4. Does this subgroup have to be cyclic?

Solution. Let G be an abelian group that contains a pair of cyclic subgroups of order 2, say H and K. Show that HK is a subgroup of order 4. Notice that HK need not be cyclic.

34. Let G be an abelian group of order pq where $\gcd(p,q) = 1$. If G contains elements a and b of order p and q respectively, then show that G is cyclic.

Solution. Let n be the order of ab. Since G is abelian,

$$(ab)^{pq} = (a^p)^q (b^q)^p = e.$$

Therefore, n divides pq. Now,

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

Since $|b| = |b^{-1}| = q$, we know that $|a^n| = p/\gcd(p,n)$ and $|(b^{-1})^n| = q/\gcd(q,n)$. Hence,

$$p \cdot \gcd(q,n) = q \cdot \gcd(p,n).$$

Since $\gcd(p,q) = 1$, p divides $\gcd(p,n)$ and so must also divide n. A similar arguement say that q divides n. Since $\gcd(p,q) = 1$, it must be the case that pq divides n. Therefore, $n = pq$.

35. Prove that the subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Solution. Since $\mathbb{Z}$ is a cyclic group, every subgroup of $\mathbb{Z}$ is also cyclic. the possible generators of these cyclic subgroups are $n \in \mathbb{Z}$. However, these generators generate the subgroups $n\mathbb{Z}$.

36. Prove that the generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

Solution. Use Proposition 3.4.

37. Prove that if G has no proper nontrivial subgroups, then G is a cyclic group.

Hint. If g is an element distinct from the identity in G, g must generate G; otherwise, $\langle g \rangle$ is a nontrivial proper subgroup of G.

Solution. If g is an element distinct from the identity in G, g must generate G; otherwise, $\langle g \rangle$ is a nontrivial proper subgroup of G.

38. Prove that the order of an element in a cyclic group G must divide the order of the group.

Solution. Use Theorem 4.13.

39. Prove that if G is a cyclic group of order m and $d \mid m$, then G must have a subgroup of order d.

Solution. Suppose that $g \in G$ has order m. Then

$$|g^{m/d}| = \frac{|g|}{\gcd(|g|, m/d)} = \frac{m}{\gcd(m, m/d)} = \frac{m}{m/d} = d$$

by Theorem 4.13.

40. For what integers n is -1 an nth root of unity?

Solution. The even integers.

41. If $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ are two nonzero complex numbers, show that

$$zw = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].$$

Solution. This follows from

$$\begin{aligned} zw &= r(\cos\theta + i\sin\theta)s(\cos\phi + i\sin\phi) \\ &= rs[(\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\sin\theta\cos\phi + \sin\phi\cos\theta)] \\ &= rs[\cos(\theta + \phi) + i\sin(\theta + \phi)]. \end{aligned}$$

42. Prove that the circle group is a subgroup of $\mathbb{C}^*$.

Solution. See Exercise 3.4.39 in Chapter 3.

43. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

Solution. If $z = \text{cis}(2\pi k_1/n)$ and $w = \text{cis}(2\pi k_2/n)$, then $zw = \text{cis}(2\pi(k_1 + k_2)/n$ is in $\mathbb{T}$. Furthermore, $z^{-1} = \text{cis}(2\pi(n - k_1)/n)$ and $1 = \text{cis}(0)$.

44. Let $\alpha \in \mathbb{T}$. Prove that $\alpha^m = 1$ and $\alpha^n = 1$ if and only if $\alpha^d = 1$ for $d = \gcd(m, n)$.

Solution. Since $d = \gcd(m, n)$ if and only if there exist integers a and b such that $d = am + bn$, we have

$$\alpha^d = \alpha^{am+bn} = (\alpha^m)^a(\alpha^n)^b = 1.$$

45. Let $z \in \mathbb{C}^*$. If $|z| \neq 1$, prove that the order of z is infinite.

Solution. If $z = r \operatorname{cis} \theta$ and $r \neq 1$, then $z^n = r^n \operatorname{cis} n\theta \neq 1$, since $r^n \neq 1$.

46. Let $z = \cos\theta + i \sin\theta$ be in $\mathbb{T}$ where $\theta \in \mathbb{Q}$. Prove that the order of z is infinite.

Solution. If $z^n = \cos n\theta + i \sin n\theta = 1$, then $n\theta$ must be a multiple of 2π. This is impossible if $\theta \in \mathbb{Q}$.

4.7 Sage Exercises

This group of exercises is about the group of units mod n, $U(n)$, which is sometimes cyclic, sometimes not. There are some commands in Sage that will answer some of these questions very quickly, but instead of using those now, just use the basic techniques described. The idea here is to just work with elements, and lists of elements, to discern the subgroup structure of these groups.

Sage worksheets have extensive capabilities for making new cells with carefully formatted text, include support for LaTeX syntax to express mathematics. So when a question asks for explanation or commentary, make a new cell and communicate clearly with your audience. Continue this practice in subsequent exercise sets.**1**. Execute the statement `R = Integers(40)` to create the set `[0,1,2,...,39]` This is a group under addition mod 40, which we will ignore. Instead we are interested in the subset of elements which have an inverse under *multiplication* mod 40. Determine how big this subgroup is by executing the command `R.unit_group_order()`, and then obtain a list of these elements with `R.list_of_elements_of_multiplicative_group()`.

Solution.

```
R = Integers(40)
R.unit_group_order()
```

```
16
```

```
R.list_of_elements_of_multiplicative_group()
```

```
[1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39]
```

2. You can create elements of this group by coercing regular integers into `U`, such as with the statement `a = U(7)`. (Don't confuse this with our mathematical notation $U(40)$.) This will tell Sage that you want to view 7 as an element of U, subject to the corresponding operations. Determine the elements of the cyclic subgroup of U generated by 7 with a list comprehension as follows:

```
R = Integers(40)
a = R(7)
[a^i for i in srange(16)]
```

What is the order of 7 in $U(40)$?

Solution.

```
a=R(7)
[a^i for i in srange(1, 5)]
```

```
[7, 9, 23, 1]
```

```
type(R.list_of_elements_of_multiplicative_group()[0])
```

```
<type 'int'>
```

```
type(a)
```

```
<type 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
```

3. The group $U(49)$ is cyclic. Using only the Sage commands described previously, use Sage to find a generator for this group. Now using *only* theorems about the structure of cyclic groups, describe each of the subgroups of $U(49)$ by specifying its order and by giving an explicit generator. Do not repeat any of the subgroups — in other words, present each subgroup *exactly* once. You can use Sage to check your work on the subgroups, but your answer about the subgroups should rely only on theorems and be a nicely written paragraph with a table, etc.

Solution. The group has order 42.

```
R = Integers(49)
T = R.list_of_elements_of_multiplicative_group()
len(T)
```

```
42
```

The element 3 is a generator (there are others, but not 2).

```
gen = 3
a = R(gen)
[a^i for i in srange(1,43)]
```

```
[3, 9, 27, 32, 47, 43, 31,
 44, 34, 4, 12, 36, 10, 30,
 41, 25, 26, 29, 38, 16, 48,
 46, 40, 22, 17, 2, 6, 18,
 5, 15, 45, 37, 13, 39, 19,
 8, 24, 23, 20, 11, 33, 1]
```

Theorems about cyclic groups say that for each divisor of the group order, there is exactly one subgroup of that order. This result is not stated explicitly in this chapter. The following will write an HTML table in the Sage notebook describing these subgroups.

```
sg = [["Divisor/Order", "Generator"]]
sg = sg + [ [d, a^(42/d)] for d in (42).divisors() ]
html.table(sg, header=True)
```

4. The group $U(35)$ is not cyclic. Again, using only the Sage commands described previously, use computations to provide irrefutable evidence of this. How many of the 16 different subgroups of $U(35)$ can you list?

Solution. The group has order 24 and is isomorphic to $\mathbb{Z}_{12} \times \mathbb{Z}_2$. It can be seen to be non-cyclic by computing the order of each element (as above) and observing a maximum order of 12.

We form a maximal subgroup of order 12, $\langle 3 \rangle$, and then a subgroup of order 2, $\langle 6 \rangle$, with a trivial intersection. This is good enough to see that $U(35)$ is an internal direct product of these two subgroups.

```
R = Integers(35)
a = R(3)
[a^i for i in srange(1,13)]
```

```
[3, 9, 27, 11, 33, 29, 17, 16, 13, 4, 12, 1]
```

```
b = R(6)
[b^i for i in srange(1,3)]
```

```
[6, 1]
```

We can build 12 distinct elements that serve as generators of cyclic groups. Students should be able to find these cyclic groups by exhaustive checking (with possibly different generators). We build them from knowledge of the internal direct product representation. Their orders are what you would expect from considering elements of the direct product (which does not necessarily prove they are correct).

```
gens = [a^i*b^j for i in 12.divisors() for j in 2.divisors()]
gens
```

```
[18, 3, 19, 9, 22, 27, 31, 11, 34, 29, 6, 1]
```

```
[x.multiplicative_order() for x in gens]
```

```
[12, 12, 6, 6, 4, 4, 6, 3, 2, 2, 2, 1]
```

There are four non-cyclic subgroups, for a total of 16 subgroups. Of course, one non-cyclic subgroup is the entire group. In practice, it is rare that a student finds any of these. They have orders 4, 8 and 12 and are generated by two elements, 6 and an element of order $2, 4, 6$ from the subgroup $\langle 3 \rangle$ of order 12. Building a Cayley table with a subset of group elements will perform a closure check, so a successful Cayley table, along with inspection (identity, inverses) can verify a subgroup.

```
A = CyclicPermutationGroup(12)
B = CyclicPermutationGroup(2)
G = A.direct_product(B)[0]
[(H.is_cyclic(), H.order()) for H in G.subgroups()]
```

```
[(True, 1), (True, 2), (True, 2), (True, 2),
(True, 3), (True, 4), (False, 4), (True, 4),
(True, 6), (True, 6), (True, 6), (False, 8),
(False, 12), (True, 12), (True, 12), (False, 24)]
```

```
elts = [R(1), a^6, b, a^6*b]
elts
```

```
[1, 29, 6, 34]
```

```
R.multiplication_table(elements=elts)
```

```
*  a b c d
 +--------
a| a b c d
b| b a d c
c| c d a b
d| d c b a
```

```
twelve = [a^i*b^j for i in srange(0,12,2) for j in srange(2)]
twelve
```

```
[1, 6, 9, 19, 11, 31, 29, 34, 16, 26, 4, 24]
```

Closed, with inverses.

```
R.multiplication_table(elements=twelve)
```

```
*  a b c d e f g h i j k l
 +------------------------
a| a b c d e f g h i j k l
b| b a d c f e h g j i l k
c| c d e f g h i j k l a b
d| d c f e h g j i l k b a
e| e f g h i j k l a b c d
f| f e h g j i l k b a d c
g| g h i j k l a b c d e f
h| h g j i l k b a d c f e
i| i j k l a b c d e f g h
j| j i l k b a d c f e h g
k| k l a b c d e f g h i j
l| l k b a d c f e h g j i
```

And no generator.

```
[x.multiplicative_order() for x in twelve]
```

```
[1, 2, 6, 6, 3, 6, 2, 2, 3, 6, 6, 6]
```

5. Again, using only the Sage commands described previously, explore the structure of $U(n)$ for various values of n and see if you can formulate an interesting conjecture about some basic property of this group. (Yes, this is a *very* open-ended question, but this is ultimately the real power of exploring mathematics with Sage.)

Solution. The structure of $U(n)$ is well-known (for example, see Gallian, Chapter 8). In particular, for p an odd prime, the group $U(p^k)$ is cyclic (and of predictable order, given by the Euler *phi*-function). The same can be said for $n = 2p^k$. (See OEIS sequence A033948.) Many students will observe some of this (maybe just for $k = 1$), and few will go further to the case of multiple odd primes. Usually they do not consider high enough values for n. Even if they have written general enough code to make good conjectures, they may only run it up to $n = 50$ and not have enough data to make the best conclusions.

Chapter 5

Permutation Groups

5.3 Exercises

1. Write the following permutations in cycle notation.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Hint. (a) (12453); (c) (13)(25).

Solution. (a) (12453); (b) (14)(35); (c) (13)(25); (d) (24).

2. Compute each of the following.

(a) $(1345)(234)$

(b) $(12)(1253)$

(c) $(143)(23)(24)$

(d) $(1423)(34)(56)(1324)$

(e) $(1254)(13)(25)$

(f) $(1254)(13)(25)^2$

(g) $(1254)^{-1}(123)(45)(1254)$

(h) $(1254)^2(123)(45)$

(i) $(123)(45)(1254)^{-2}$

(j) $(1254)^{100}$

(k) $|(1254)|$

(l) $|(1254)^2|$

(m) $(12)^{-1}$

(n) $(12537)^{-1}$

(o) $[(12)(34)(12)(47)]^{-1}$

(p) $[(1235)(467)]^{-1}$

Hint. (a) (135)(24); (c) (14)(23); (e) (1324); (g) (134)(25); (n) (17352).

Solution. (a) (135)(24); (b) (253); (c) (14)(23); (d) (12)(56); (e) (1324); (f) (13254); (g) (134)(25); (h) (14)(235); (i) (143)(25); (j) (1); (k) 4; (l) 2; (m) (12); (n) (17352); (o) (374); (p) (476)(1532).

3. Express the following permutations as products of transpositions and identify them as even or odd.

(a) (14356)

(b) (156)(234)

(c) (1426)(142)

(d) (17254)(1423)(154632)

(e) (142637)

Hint. (a) (16)(15)(13)(14); (c) (16)(14)(12).

Solution. (a) (16)(15)(13)(14); (b) (15)(56)(23)(34); (c) (16)(14)(12); (d) (17)(13)(16)(12)(14); (e) (12)(17)(16)(14).

4. Find $(a_1, a_2, \ldots, a_n)^{-1}$.

Hint. $(a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, a_{n-1}, \ldots, a_2)$

Solution. $(a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, a_{n-1}, \ldots, a_2)$

5. List all of the subgroups of S_4. Find each of the following sets.

(a) $\{\sigma \in S_4 : \sigma(1) = 3\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

Are any of these sets subgroups of S_4?

Hint. (a) $\{(13), (13)(24), (132), (134), (1324), (1342)\}$ is not a subgroup.

Solution. The subgroups of S_4 are the following:

- Order 1: $\{(1)\}$.
- Order 2: $\{(1), (12)\}$, $\{(1), (13)\}$, $\{(1), (14)\}$, $\{(1), (23)\}$, $\{(1), (24)\}$, $\{(1), (34)\}$, $\{(1), (12)(34)\}$, $\{(1), (13)(24)\}$, $\{(1), (14)(23)\}$.
- Order 3: $\{(1), (123), (132)\}$, $\{(1), (124), (142)\}$, $\{(1), (134), (143)\}$, $\{(1), (234), (243)\}$.
- Order 4: $\{(1), (1234), (13)(24), (1432)\}$, $\{(1), (1243), (14)(23), (1342)\}$, $\{(1), (1324), (12)(34), (1423)$ $\{(1), (12)(34), (13)(24), (14)(23)\}$.
- Order 6: S_3, $\{(1), (12), (14), (24), (124), (142)\}$, $\{(1), (13), (14), (24), (134), (143)\}$, $\{(1), (23), (24), (34), (234), (243)\}$.
- Order 8: D_4, $\{(1), (14), (23), (12)(34), (13)(24), (1243), (14)(23), (1342)\}$, $\{(1), (12), (34), (13)(24), (14)(23), (1324), (12)(34), (1423)\}$.
- Order 12: A_4.

(a) $\{(13), (13)(24), (132), (134), (1324), (1342)\}$ is not a subgroup.

(b) $\{(1), (134), (143), (13), (14), (34)\}$ is a subgroup.

(c) $\{(13), (134)\}$ is not a subgroup.

6. Find all of the subgroups in A_4. What is the order of each subgroup?

Solution. The subgroups of A_4 are the following:

- Order 1: $\{(1)\}$.
- Order 2: $\{(1), (12)(34)\}$, $\{(1), (13)(24)\}$, $\{(1), (14)(23)\}$.
- Order 3: $\{(1), (123), (132)\}$, $\{(1), (124), (142)\}$, $\{(1), (134), (143)\}$, $\{(1), (234), (243)\}$.
- Order 4: $\{(1), (12)(34), (13)(24), (14)(23)\}$.

- Order 12: A_4.

7. Find all possible orders of elements in S_7 and A_7.

Solution. Looking at the possible cycle structures, S_7 has elements of order 1, 2, 3, 4, 5, 6, 7, 10, and 12. A_7 has elements of order 1, 2, 3, 5, 6, and 7.

8. Show that A_{10} contains an element of order 15.

Hint. (12345)(678).

Solution. (12345)(678).

9. Does A_8 contain an element of order 26?

Solution. No, since the order of an element must divide the order of A_8, and 26 does not divide $|A_8| = 8!/2$.

10. Find an element of largest order in S_n for $n = 3, \ldots, 10$.

Solution. If we look for elements of S_n that are the product of disjoint cyclics of lengths that are relatively prime, we see that S_3 has an element of order 3; S_4 has an element of order 4; S_5 has an element of order 6; S_6 has an element of order 6; S_7 has an element of order 12; S_8 has an element of order 15; S_9 has an element of order 20; S_{10} has an element of order 30.

11. What are the possible cycle structures of elements of A_5? What about A_6?

Hint. Permutations of the form

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$$

are possible for A_5.

Solution. Permutations of the form

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$$

are possible for A_5. For A_6, we can have permutations of the form

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3)(a_4, a_5, a_6), (a_1, a_2, a_3, a_4, a_5).$$

12. Let $\sigma \in S_n$ have order n. Show that for all integers i and j, $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{n}$.

Solution. This follows from the fact that $\sigma^i = \sigma^j$ if and only if $\sigma^{i-j} = \mathrm{id}$ if and only if $i \equiv j \pmod{n}$.

13. Let $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \ldots, \sigma_m$.

Solution. A cycle of length n has order n. Let σ and τ are disjoint cycles of length m and n, respectively. If $r = mn$, then $\sigma^r = (1)$ and $\tau^r = (1)$, and $(\sigma\tau)^r = \sigma^r\tau^r = (1)$. Thus, if s is the order of $\sigma\tau$, then s must divide r. So $(\sigma\tau)^s = \sigma^s\tau^s = (1)$, or $\sigma^s = \tau^s = (1)$. Hence, m and n must both divide s. Consequently, $s = \mathrm{lcm}(m, n)$. The general case follows from mathematical induction.

14. Using cycle notation, list the elements in D_5. What are r and s? Write every element as a product of r and s.

Solution. If we number the vertices $1, \ldots, 5$, then the elements of D_5 are (1), $r = (12345)$, (13524), (14253), (15432), $s = (25)(34)$, (13)(45), (15)(24), (12)(35), and (14)(23).

15. If the diagonals of a cube are labeled as Figure 5.26, to which motion of the cube does the permutation (12)(34) correspond? What about the other permutations of the diagonals?

Solution. A double rotation about the center of the cube.

16. Find the group of rigid motions of a tetrahedron. Show that this is the same group as A_4.

Solution. Labeling the vertices of the tetrahedron by 1, 2, 3, 4, there are eight rotations: (123), (132), (124), (142), (134), (143), (234), and (243). There are three motions that interchange opposite edges: (12)(34), (13)(24), and (14)(23). Finally, there is the identity.

17. Prove that S_n is nonabelian for $n \geq 3$.

Hint. Calculate (123)(12) and (12)(123).

Solution. $(123)(12) = (13) \neq (23) = (12)(123)$.

18. Show that A_n is nonabelian for $n \geq 4$.

Solution. $(123)(124) = (13)(24) \neq (14)(23) = (124)(123)$.

19. Prove that D_n is nonabelian for $n \geq 3$.

Solution. Suppose that $sr = rs$. Since $srs = r^{-1}$, $rs = sr = srs^2 = r^{-1}s$. If this is the case, then $r = r^{-1}$, which is impossible for $n \geq 3$.

20. Let $\sigma \in S_n$ be a cycle. Prove that σ can be written as the product of at most $n - 1$ transpositions.

Solution. $(a_1, a_2, a_3, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2)$.

21. Let $\sigma \in S_n$. If σ is not a cycle, prove that σ can be written as the product of at most $n - 2$ transpositions.

Solution. Suppose that $\sigma \in S_n$ is the product of disjoint cycles, say $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$, where $\sigma_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ is of length i_k. Note that $1_k + 2_k + \cdots + r_k \leq n$. By Exercise 5.3.20, we can write each σ_i as the product of $i_k - 1$ transpostions. Thus, we can write, σ as the product of at most $1_k + 2_k + \cdots + r_k - r \leq n - r$ transpositions, where $r \geq 2$.

22. If σ can be expressed as an odd number of transpositions, show that any other product of transpositions equaling σ must also be odd.

Solution. Follow the proof of Theorem 5.6.

23. If σ is a cycle of odd length, prove that σ^2 is also a cycle.

Solution. If n is odd, then $(a_1, a_2, \ldots, a_n)^2 = (a_1, a_3, a_5, \ldots, a_n, a_2, a_4, \ldots, a_{n-1})$.

24. Show that a 3-cycle is an even permutation.

Solution. $(abc) = (ac)(ab)$.

25. Prove that in A_n with $n \geq 3$, any permutation is a product of cycles of length 3.

Hint. Consider the cases $(ab)(bc)$ and $(ab)(cd)$.

Solution. If $\sigma \in A_n$, then it can be written as a product of an even number of transpositions. Any pair of transpostions can be written as a 3-cycle: $(ab)(bc) = (abc)$ and $(ab)(cd) = (abc)(bcd)$.

26. Prove that any element in S_n can be written as a finite product of the following permutations.

(a) $(12), (13), \ldots, (1n)$

(b) $(12), (23), \ldots, (n-1, n)$

(c) $(12), (12\ldots n)$

Solution.

(a) Since $(1a)(1b)(1a) = (ab)$, we can obtain all transpositions.

(b) This follows from part (a), since $(12)(23)(12) = (13)$, $(13)(34)(13) = (14)$, etc.

(c) This follows from part (b), since $(12\cdots n)(12)(12\cdots n)^{-1} = (23)$, $(12\cdots n)(23)(12\cdots n)^{-1} = (34)$, etc.

27. Let G be a group and define a map $\lambda_g : G \to G$ by $\lambda_g(a) = ga$. Prove that λ_g is a permutation of G.

Solution. We need to show that λ_g is one-to-one and onto. If $\lambda_g(a) = \lambda_g(b)$, then $ga = gb$ or $a = b$. Thus, λ is one-to-one. For $a \in G$, $\lambda_g(g^{-1}a) = a$; hence, λ_g is onto.

28. Prove that there exist $n!$ permutations of a set containing n elements.

Solution. Induct on n.

29. Recall that the **center** of a group G is

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

Find the center of D_8. What about the center of D_{10}? What is the center of D_n?

Solution. Every element in D_n can be written as r^i or $r^i s$, where $0 \leq i \leq n-1$. Thus, to find the center of D_n, we must find all $g \in D_n$ such that $r^i g r^{-i} = g$ and $r^i s g s r^i = g$. Since

$$r(r^j s)r^{-1} = r^{j+2}s,$$

any element of the form $r^i s$ cannot be in the center of D_n. However, $r^i r^j r^{-1} = r^j$ and

$$(r^i s)r^j(r^i s)^{-1} = r^{-j}.$$

Therefore, it is only possible for an element g to be in the center of D_n if $g = r^j = r^{-j}$. If n is even, then the center consists is $\{1, r^{n/2}\}$. If n is odd, then the center is trivial. Thus, the center of D_8 is $\{1, r^4\}$ and the center of D_{10} is $\{1, r^5\}$.

30. Let $\tau = (a_1, a_2, \ldots, a_k)$ be a cycle of length k.

(a) Prove that if σ is any permutation, then

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

is a cycle of length k.

(b) Let μ be a cycle of length k. Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.

Hint. For (a), show that $\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma(a_{i+1})$.

Solution.

(a) First note that

$$\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma\tau(\sigma^{-1}\sigma)(a_i) = \sigma\tau(a_i) = \sigma(a_{i+1}).$$

If we choose b to be different from $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)$, then $\sigma^{-1}(b) \neq a_i$ for $i = 1, 2, \ldots, k$. We must show that $\sigma\tau\sigma^{-1}(b) = b$. However,

$$\sigma\tau\sigma^{-1}(b) = \sigma\sigma^{-1}(b) = b.$$

(b) If $\mu = (b_1, \ldots, b_k)$, define σ on $\{a_1, a_2, \ldots, a_k\}$ as $\sigma(a_1) = b_1, \sigma(a_2) = b_2, \ldots, \sigma(a_k) = b_k$ and to be any bijection on the complement of $\{a_1, a_2, \ldots, a_k\}$. By part(a), $\sigma\tau\sigma^{-1} = \mu$.

31. For α and β in S_n, define $\alpha \sim \beta$ if there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that $\sim$ is an equivalence relation on S_n.

Solution. This result holds for any group and not just S_n. The relation is reflexive since $(1)\alpha(1) = \alpha$. If $\alpha \sim \beta$ then there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Since $\sigma^{-1}\beta(\sigma^{-1})^{-1} = \alpha$, we know that $\beta \sim \alpha$. To show that the relation is transitive, suppose that $\alpha \sim \beta$ and $\beta \sim \gamma$. Then there there exist $\sigma, \tau \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$ and $\tau\beta\tau^{-1} = \gamma$. Combining these two equations, we see that

$$\gamma = \tau\beta\tau^{-1} = \tau\sigma\alpha\sigma^{-1}\tau^{-1} = (\tau\sigma)\alpha(\tau\sigma)^{-1}$$

or $\alpha \sim \gamma$.

32. Let $\sigma \in S_X$. If $\sigma^n(x) = y$, we will say that $x \sim y$.

(a) Show that $\sim$ is an equivalence relation on X.

(b) If $\sigma \in A_n$ and $\tau \in S_n$, show that $\tau^{-1}\sigma\tau \in A_n$.

(c) Define the **orbit** of $x \in X$ under $\sigma \in S_X$ to be the set

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Compute the orbits of each of the following elements in S_5:

$$\alpha = (1254)$$
$$\beta = (123)(45)$$
$$\gamma = (13)(25).$$

(d) If $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, prove that $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. The orbits under a permutation σ are the equivalence classes corresponding to the equivalence relation $\sim$.

(e) A subgroup H of S_X is **transitive** if for every $x, y \in X$, there exists a $\sigma \in H$ such that $\sigma(x) = y$. Prove that $\langle\sigma\rangle$ is transitive if and only if $\mathcal{O}_{x,\sigma} = X$ for some $x \in X$.

Solution.

(a) This is a straightforward verification of the definitions. The relation is reflexive since $\sigma^0(x) = x$. If $x \sim y$, then $\sigma^n(x) = y$ and $\sigma^{-n}(y) = x$. Thus, $y \sim x$ and the relation is symmetric. To show that the relation is transitive, let $x \sim y$ and $y \sim z$. Then

$$\sigma^{m+n}(x) = \sigma^n(\sigma^m(x) = \sigma^n(y) = z.$$

Therefore, $x \sim z$.

(b) Suppose that τ is the product of transpositions $\tau = \tau_1\tau_2\cdots\tau_k$. Then $\tau^{-1} = \tau_k\tau_{k-1}\cdots\tau_1$ can be expressed as a product of the same number of transpositions. Therefore, τ and τ^{-1} must both be even permutations or both be odd permutations. Hence, $\tau^{-1}\sigma\tau \in A_n$ since it can be expressed as an even number of permutations.

(c)

$$\begin{aligned}\mathcal{O}_{1,\alpha} &= \{1,2,4,5\}\\ \mathcal{O}_{3,\alpha} &= \{3\}\\ \mathcal{O}_{1,\beta} &= \{1,2,3\}\\ \mathcal{O}_{4,\beta} &= \{4,5\}\\ \mathcal{O}_{1,\gamma} &= \{1,3\}\\ \mathcal{O}_{2,\gamma} &= \{2,5\}\\ \mathcal{O}_{4,\gamma} &= \{4\}.\end{aligned}$$

(d) Suppose that $z \in \mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma}$. Then $x \sim z$ and $y \sim z$. Thus, $x \sim y$ and $\mathcal{O}_{x,\sigma} \supset \mathcal{O}_{y,\sigma}$. Similarly, $\mathcal{O}_{x,\sigma} \subset \mathcal{O}_{y,\sigma}$.

(e) Let $x, y \in X$. If $\langle\sigma\rangle$ is transitive, then there exists a $\tau \in S_X$ such that $\tau(x) = y$. But $\tau = \sigma^n$ for some n. Consequently, $\mathcal{O}_{x,\sigma} = X$. Conversely, suppose that $\mathcal{O}_{x,\sigma} = X$ for some $x \in X$, and let $y \in X$. Then $\sigma^n(x) = y$ for some n.

33. Let $\alpha \in S_n$ for $n \geq 3$. If $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$, prove that α must be the identity permutation; hence, the center of S_n is the trivial subgroup.

Solution. If α commutes with all elements if S_n and α is not the identiry, then there exist $a, b \in \{1, 2, \ldots, n\}$ such that $a \neq b$ and $\alpha(a) = b$. Choose c to be some other element that a or b. Then $(bc)\sigma(a) = c$ but $\sigma(bc)(a) = b$, contradicting the assumption that α is in the center of S_n. Hence, the center is trivial.

34. If α is even, prove that α^{-1} is also even. Does a corresponding result hold if α is odd?

Solution. Both statements are true and follow from the fact that $[(a_1a_2)\ldots(a_{n-1}a_n)]^{-1} = (a_{n-1}a_n)\ldots(a_1a_2)$.

35. Show that $\alpha^{-1}\beta^{-1}\alpha\beta$ is even for $\alpha, \beta \in S_n$.

Solution. Use Exercise 5.3.34.

36. Let r and s be the elements in D_n described in Theorem 5.23

(a) Show that $srs = r^{-1}$.

(b) Show that $r^k s = sr^{-k}$ in D_n.

(c) Prove that the order of $r^k \in D_n$ is $n/\gcd(k, n)$.

Solution.

(a) If a rigid motion moves vertex i to vertex j, then vertex $i+1$ will either be moved to vertex $j+1$ or $j-1$. Thus, every rigid motion of a regular n-gon is determined by what happens on two adjacent vertices. Without loss of generality, we simply need to check where vertex 1 is moved along with its adjacent vertices, 2 and n. However,

$$\begin{aligned}srs(1) = sr(1) = s(2) = n = r^{-1}(1)\\ srs(2) = sr(n) = s(1) = 1 = r^{-1}(2)\\ srs(n) = sr(2) = s(3) = n-1 = r^{-1}(n).\end{aligned}$$

(b) To show that $r^k s = sr^{-k}$ in D_n, we will induct on k. The case $k = 1$ is true from part (a). Now assume that $r^k s = sr^{-k}$. From part (a) we know that $rs = sr^{-1}$; therefore,

$$r^{k+1}s = rr^k s = rsr^{-k} = sr^{-1}r^{-k} = sr^{-(k+1)}.$$

(c) Noting that r has order n, the order of $r^k \in D_n$ is $n/\gcd(k, n)$ by Theorem 4.13.

5.5 Sage Exercises

These exercises are designed to help you become familiar with permutation groups in Sage.**1**. Create the full symmetric group S_{10} with the command `G = SymmetricGroup(10)`.

Solution.

```
G = SymmetricGroup(10)
G
```

```
Symmetric group of order 10! as a permutation group
```

2. Create elements of `G` with the following (varying) syntax. Pay attention to commas, quotes, brackets, parentheses. The first two use a string (characters) as input, mimicking the way we write permuations (but with commas). The second two use a list of tuples.

- `a = G("(5,7,2,9,3,1,8)")`
- `b = G("(1,3)(4,5)")`
- `c = G([(1,2),(3,4)])`
- `d = G([(1,3),(2,5,8),(4,6,7,9,10)])`

(a) Compute a^3, bc, $ad^{-1}b$.

(b) Compute the orders of each of these four individual elements (`a` through `d`) using a single permutation group element method.

(c) Use the permutation group element method `.sign()` to determine if a, b, c, d are even or odd permutations.

(d) Create two cyclic subgroups of G with the commands:

- `H = G.subgroup([a])`
- `K = G.subgroup([d])`

List, and study, the elements of each subgroup. Without using Sage, list the order of each subgroup of K. Then use Sage to construct a subgroup of K with order 10.

(e) More complicated subgroups can be formed by using two or more generators. Construct a subgroup L of G with the command `L = G.subgroup([b,c])`. Compute the order of L and list all of the elements of L.

Solution.

```
a = G("(5,7,2,9,3,1,8)")
b = G("(1,3)(4,5)")
c = G([(1,2),(3,4)])
d = G([(1,3),(2,5,8),(4,6,7,9,10)])
```

```
a^3
```

```
(1,7,3,5,9,8,2)
```

```
b*c
```

```
(1,4,5,3,2)
```

```
a*d^-1*b
```

```
(1,4,10,9,3)(2,7,8)(5,6)
```

```
d.order()
```

```
30
```

```
d.sign()
```

```
-1
```

```
H = G.subgroup([d])
J = G.subgroup([d^3])
J.order()
```

```
10
```

```
J.is_subgroup(H)
```

```
True
```

```
L = G.subgroup([b,c])
L.order()
```

```
10
```

Troy Cornelius observes that `L` is a dihedral group, and due to Exercise 9.3.55, we know that as a non-abelian group of order $10 = 2 \cdot 5$, this must be the case. Students can observe the two generators as reflections of the pentagon with vertices labeled in the order $1, 2, 3, 5, 4$.

3. Construct the group of symmetries of the tetrahedron (also the alternating group on 4 symbols, A_4) with the command `A=AlternatingGroup(4)`. Using tools such as orders of elements, and generators of subgroups, see if you can find *all of* the subgroups of A_4 (each one exactly once). Do this without using the `.subgroups()` method to justify the correctness of your answer (though it might be a convenient way to check your work).

Provide a nice summary as your answer—not just piles of output. So use Sage as a tool, as needed, but basically your answer will be a concise paragraph and/or table. This is the one part of this assignment without clear, precise directions, so spend some time on this portion to get it right. Hint: no subgroup of A_4 requires more than two generators.

Solution. The $12 = 1 + 3 \cdot 1 + 4\dot{2}$ elements of the group generate cyclic subgroups of orders $1, 2, 3$ numbering $1 + 3 + 4 = 8$. A ninth subgroup is generated by any two of the elements of order 2 and the tenth subgroup is the entire group, and can be generated by an element of order 2 and an element of order 3.

```
A = AlternatingGroup(4)
sg = A.subgroups()
[H.order() for H in sg]
```

```
[1, 2, 2, 2, 3, 3, 3, 3, 4, 12]
```

```
r = A("(1,2)(3,4)")
s = A("(1,3)(2,4)")
t = A("(1,2,3)")
four = A.subgroup([r,s])
twelve = A.subgroup([r,t])
four.order(), twelve.order()
```

```
(4, 12)
```

4. The subsection Motion Group of a Cube describes the 24 symmetries of a cube as a subgroup of the symmetric group S_8 generated by three quarter-turns. Answer the following questions about this symmetry group.

(a) From the list of elements of the group, can you locate the ten rotations about axes? (Hint: the identity is easy, the other nine never send any symbol to itself.)

(b) Can you identify the six symmetries that are a transposition of diagonals? (Hint: `[g for g in cube if g.order() == 2]` is a good preliminary filter.)

(c) Verify that any two of the quarter-turns (`above`, `front`, `right`) are sufficient to generate the whole group. How do you know each pair generates the entire group?

(d) Can you express one of the diagonal transpositions as a product of quarter-turns? This can be a notoriously difficult problem, especially for software. It is known as the "word problem."

(e) Number the six faces of the cube with the numbers 1 through 6 (any way you like). Now consider the same three symmetries we used before (quarter-turns about face-to-face axes), but now view them as permutations of the six faces. In this way, we construct each symmetry as an element of S_6. Verify that the subgroup generated by these symmetries is the whole symmetry group of the cube. Again, rather than using three generators, try using just two.

Solution. There are 16 elements of orders $1, 2, 4$. The identity is one, six are quarter-turns about the face-center axes, three are half-turns about the face-center axes, and the remaining six are elements of order 2 that transpose diagonals. We find all of them at once, but it should be easy to distinguish the types methodically.

```
S = SymmetricGroup(8)
above = S("(1,2,3,4)(5,6,7,8)")
front = S("(1,4,8,5)(2,3,7,6)")
```

```
right = S("(1,2,6,5)(3,7,8,4)")
cube = S.subgroup([above, front, right])
cube.order()
```

```
24
```

```
cube.is_isomorphic(SymmetricGroup(4))
```

```
True
```

```
[x for x in cube if x^4 == cube("()")]
```

```
[(), (1,2,3,4)(5,6,7,8),
(1,2,6,5)(3,7,8,4), (1,4,8,5)(2,3,7,6),
(1,6)(2,5)(3,8)(4,7), (1,3)(2,4)(5,7)(6,8),
(1,8)(2,7)(3,6)(4,5), (1,7)(2,3)(4,6)(5,8),
(1,4)(2,8)(3,5)(6,7), (1,5,6,2)(3,4,8,7),
(1,5,8,4)(2,6,7,3), (1,7)(2,6)(3,5)(4,8),
(1,7)(2,8)(3,4)(5,6), (1,4,3,2)(5,8,7,6),
(1,5)(2,8)(3,7)(4,6), (1,2)(3,5)(4,6)(7,8)]
```

Any subgroup of order 24 must be the entire group.

```
H = S.subgroup([above, front])
H.order()
```

```
24
```

Sage has a routine to solve the word problem in permutation groups, as a method on permutation group elements (`.word_problem()`). It takes a bit of effort to decode the output. Students at this point will want to just experiment and recognize how hard the problem can be. We demonstrate a solution for one diagonal-swapper element.

```
diagonal = S("(1,7)(2,3)(4,6)(5,8)")
diagonal in cube
```

```
True
```

```
above*front^-1*above == diagonal
```

```
True
```

Finally, as a permutation group on six symbols (the faces).

```
K = SymmetricGroup(6)
above=K("(1,5,3,6)")
front=K("(2,5,4,6)")
right=K("(1,2,3,4)")
F = K.subgroup([above, front])
F.is_isomorphic(cube)
```

```
True
```

5. Save your work, and then see if you can crash your Sage session by building the subgroup of S_{10} generated by the elements `b` and `d` of orders 2 and 30 from above. *Do not submit* the list of elements of `N` as part of your submitted worksheet.

```
N = G.subgroup([b,d])
N.list()
```

What is the order of N?

Solution.

```
N = G.subgroup([b,d])
N.order()
```

```
80640
```

Students may be surprised that two non-commuting elements of such relatively small orders will generate such a large subgroup. However, the elements of `N` constitute just a bit more than 2% of S_{10}.

Chapter 6

Cosets and Lagrange's Theorem

6.4 Exercises

1. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?

Hint. The order of g and the order h must both divide the order of G.

Solution. The order of g and the order h must both divide the order of G. The smallest number that 5 and 7 both divide is $\text{lcm}(5, 7) = 35$.

2. Suppose that G is a finite group with 60 elements. What are the orders of possible subgroups of G?

Hint. The possible orders must divide 60.

Solution. The possible orders are $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

3. Prove or disprove: Every subgroup of the integers has finite index.

Hint. This is true for every proper nontrivial subgroup.

Solution. This is true for every proper nontrivial subgroup. Every nontrivial subgroup of $\mathbb{Z}$ must be of the form $n\mathbb{Z}$ for $n = 1, 2, \ldots$. Thus, $[\mathbb{Z} : n\mathbb{Z}] = n$. The index of the trivial subgroup consisting of zero is of course infinite.

4. Prove or disprove: Every subgroup of the integers has finite order.

Hint. False.

Solution. This is false if we require the subgroup to be nontrivial.

5. List the left and right cosets of the subgroups in each of the following.

(a) $\langle 8 \rangle$ in $\mathbb{Z}_{24}$

(b) $\langle 3 \rangle$ in $U(8)$

(c) $3\mathbb{Z}$ in $\mathbb{Z}$

(d) A_4 in S_4

(e) A_n in S_n

(f) D_4 in S_4

(g) $\mathbb{T}$ in $\mathbb{C}^*$

(h) $H = \{(1), (123), (132)\}$ in S_4

Hint. (a) $\langle 8 \rangle$, $1 + \langle 8 \rangle$, $2 + \langle 8 \rangle$, $3 + \langle 8 \rangle$, $4 + \langle 8 \rangle$, $5 + \langle 8 \rangle$, $6 + \langle 8 \rangle$, and $7 + \langle 8 \rangle$; (c) $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$.

Solution.

(a) $\langle 8 \rangle$, $1 + \langle 8 \rangle$, $2 + \langle 8 \rangle$, $3 + \langle 8 \rangle$, $4 + \langle 8 \rangle$, $5 + \langle 8 \rangle$, $6 + \langle 8 \rangle$, and $7 + \langle 8 \rangle$.

(b) $\langle 3\rangle = \{1, 3\}$, $5 + \langle 3\rangle = \{5, 7\}$.

(c) $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$.

(d) A_4, $(12)A_4 = A_4(12)$.

(e) A_n, $(12)A_n = A_n(12)$.

(f) The left cosets are D_4, $(12)D_4$, and $(14)D_4$. The right cosets are D_4, $D_4(12)$, and $D_4(14)$.

(g) $r \operatorname{cis} \theta$ for a fixed $r \in \mathbb{R}$ and $0 \leq \theta < 2\pi$.

(h) The left cosets are H, $(12)H$, $(14)H$, $(24)H$, $(34)H$, $(124)H$, $(142)H$, $(143)H$. The right cosets are H, $H(12)$, $H(14)$, $H(24)$, $H(34)$, $H(124)$, $H(142)$, and $H(234)$.

6. Describe the left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$. What is the index of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$?

Solution. The left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$ are $aSL_2(\mathbb{R})$, where $a \in \mathbb{R}$. The index of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$ is infinite.

7. Verify Euler's Theorem for $n = 15$ and $a = 4$.

Hint. $4^{\phi(15)} \equiv 4^8 \equiv 1 \pmod{15}$.

Solution. $4^{\phi(15)} \equiv 4^8 \equiv 1 \pmod{15}$.

8. Use Fermat's Little Theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

Solution. If $p = 4n + 3$ is prime, then $|U(p)| = p - 1 = 4n + 2$. Thus, $|U(p)|$ is not divisible by 4. If $x^2 \equiv -1 \pmod{p}$, then x has order 4 in $U(p)$. However, this says that $4 \mid |U(p)|$, which is a contradiction.

9. Show that the integers have infinite index in the additive group of rational numbers.

Solution. The cosets of $\mathbb{Z}$ in $\mathbb{Q}$ are $r + \mathbb{Z}$ for $0 \leq r < 1$.

10. Show that the additive group of real numbers has infinite index in the additive group of the complex numbers.

Solution. The cosets of $\mathbb{R}$ in $\mathbb{C}$ are $ai + \mathbb{R}$ for $a \in \mathbb{R}$.

11. Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. Prove that the following conditions are equivalent.

(a) $g_1 H = g_2 H$

(b) $Hg_1^{-1} = Hg_2^{-1}$

(c) $g_1 H \subset g_2 H$

(d) $g_2 \in g_1 H$

(e) $g_1^{-1} g_2 \in H$

Solution. We must show that (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e).

- (a) $\Leftrightarrow$ (b): We will work out (a) $\Rightarrow$ (b) in detail. Let $x \in Hg_1^{-1}$. We must show that $x \in Hg_2^{-1}$. Indeed, if $x \in Hg_1^{-1}$, then there exists $h_1 \in H$ such that $x = h_1 g_1^{-1}$. Consequently, $xg_1 = h_1 \in H$. Therefore, $(xg_1)^{-1} = g_1^{-1} x^{-1} = h_2$ is also in H since H is a subgroup of G. Thus, $x^{-1} = g_1 h_2$ is in both $g_1 H$ and $g_2 H$, since $g_1 H = g_2 H$. Since $x^{-1} \in g_2 H$,

there exists $h_3 \in H$ such that $x^{-1} = g_2 h_3$. Since $g_2^{-1}x^{-1} = h_3 \in H$, we know that

$$(g_2^{-1}x^{-1})^{-1} = xg_2 = h_4$$

is in H or $x = h_4 g_2^{-1} \in Hg_2^{-1}$. We have now shown that $Hg_1^{-1} \subset Hg_2^{-1}$. A symmetric argument shows that $Hg_2^{-1} \subset Hg_1^{-1}$. Therefore, $Hg_1^{-1} = Hg_2^{-1}$. A similar arguement works for (b) $\Rightarrow$ (a).

- (a) $\Rightarrow$ (c): This follows from the definition of equality of sets.
- (a) $\Rightarrow$ (d): Suppose that $g_1 H = g_2 H$. Then $g_2 = g_2 e \in g_2 H = g_1 H$.
- (c) $\Rightarrow$ (d): Let $x = g_1 h_1 \in g_1 H$. Since $g_1 H \subset g_2 H$, there exists $h_2 \in H$ such that $x = g_1 h_1 = g_2 h_2$. Since $g_2 = g_1 h_1 h_2^{-1}$, we know that $g_2 \in g_1 H$.
- (d) $\Rightarrow$ (a): Let $x = g_1 h_1 \in g_1 H$. We must show that $x \in g_2 H$. Since $g_2 \in g_1 H$, we can write $g_2 = g_1 h_2$ for some $h_2 \in H$. Since $g_1 = g_2 h_2^{-1}$, we know that $x = g_2 h_2^{-1} h_1 \in g_2 H$ and $g_1 H \subset g_2 H$. Similarly, $g_2 H \subset g_1 H$.
- (d) $\Rightarrow$ (e): If $g_2 \in g_1 H$, then $g_2 = g_1 h$ for some $h \in H$. Consequently, $g_1^{-1} g_2 = h \in H$.
- (e) $\Rightarrow$ (c): Let $g_1^{-1} g_2 \in H$. Then there exists $h \in H$ such that $g_1^{-1} g_2 = h$ and $g_2 = g_1 h \in g_1 H$. Thus, $g_1 H \subset g_2 H$.

12. If $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, show that right cosets are identical to left cosets. That is, show that $gH = Hg$ for all $g \in G$.

Hint. Let $g_1 \in gH$. Show that $g_1 \in Hg$ and thus $gH \subset Hg$.

Solution. Let $g_1 \in gH$. Then there exists an $h \in H$ such that $g_1 = gh = ghg^{-1}g$. Thus, $g_1 \in Hg$ and $gH \subset Hg$. Similarly, $Hg \subset gH$. Therefore, $gH = Hg$.

13. What fails in the proof of Theorem 6.8 if $\phi : \mathcal{L}_H \to \mathcal{R}_H$ is defined by $\phi(gH) = Hg$?

Solution. The map $\phi : \mathcal{L}_H \to \mathcal{R}_H$ may not be well-defined.

14. Suppose that $g^n = e$. Show that the order of g divides n.

Solution. Use Proposition 4.12.

15. Show that any two permutations $\alpha, \beta \in S_n$ have the same cycle structure if and only if there exists a permutation γ such that $\beta = \gamma\alpha\gamma^{-1}$. If $\beta = \gamma\alpha\gamma^{-1}$ for some $\gamma \in S_n$, then α and β are **conjugate**.

Solution. We first show that conjugation preserves cycle structure. If α and γ are two permutations in S_n, where $\alpha = \alpha_1\alpha_2\cdots\alpha_m$ is the product of disjoint cycles, then

$$\gamma\alpha\gamma^{-1} = \gamma\alpha_1\alpha_2\cdots\alpha_m\gamma^{-1} = (\gamma\alpha_1\gamma^{-1})(\gamma\alpha_2\gamma^{-1})\cdots(\gamma\alpha_m\gamma^{-1}).$$

By Theorem 6.16, each $\gamma\alpha_i\gamma^{-1}$ is a cycle of the same length as α_i. Furthermore, as in the proof of Theorem 6.16,

$$\gamma\alpha_i\gamma^{-1} = (\gamma(a_{i_1}), \gamma(a_{i_2}), \ldots, \gamma(a_{i_k})),$$

where $\alpha_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_k})$. Since $\gamma \in S_n$, the cycles $\gamma\alpha_i\gamma^{-1}$ must be disjoint.

Conversely, Suppose that α and β have the same cycle structure. We may assume that

$$\alpha = \alpha_1\alpha_2\cdots\alpha_m$$
$$\beta = \beta_1\beta_2\cdots\beta_m,$$

where α_i and β_i have the same length. If $\alpha_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ and $\beta_i = (b_{i_1}, b_{i_2}, \ldots, b_{i_k})$, define γ by $\gamma(a_{i_j}) = b_{i_j}$. Then

$$\gamma\alpha_i\gamma^{-1}(b_{i_j}) = \gamma\alpha_i(a_{i_j}) = \gamma(a_{i_{j+1}}) = b_{i_{j+1}}.$$

Thus, α and β are conjugate.

16. If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2.

Solution. Since $|G| = 2n$, there are an odd number of elements in G that are not the identity. Now pair each of these elements with their inverses.

17. Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

Solution. If $a \notin H$, then $a^{-1} \notin H$ and $a^{-1} \in aH = a^{-1}H = bH$. Thus, there exist $h_1, h_2 \in H$ such that $a^{-1}h_1 = bh_2$. Consequently, $ab = h_1h_2^{-1} \in H$.

18. If $[G : H] = 2$, prove that $gH = Hg$.

Solution. If $[G : H] = 2$, then H has only two left cosets, say H and gH, and two right cosets, say H and Hg. Since both left and right cosets partition G, it must be the case that $gH = Hg$.

19. Let H and K be subgroups of a group G. Prove that $gH \cap gK$ is a coset of $H \cap K$ in G.

Hint. Show that $g(H \cap K) = gH \cap gK$.

Solution. If $x \in gH \cap gK$, then $x \in gH$ and $x \in gK$. Therefore, there exist elements $h \in H$ and $k \in K$ such that $x = gh = gk$. Consequently, $g^{-1}x$ is in both H and K. Thus, $g^{-1}x \in H \cap K$ or $x \in g(H \cap K)$. Hence, $gH \cap gK \subset g(H \cap K)$.

Now suppose that $x \in g(H \cap K)$. Then $x = ga$ for some $a \in H \cap K$. Thus, $x = ga$ is in both gH and gK, or $x \in gH \cap gK$. Therefore, $g(H \cap K) \subset gH \cap gK$.

20. Let H and K be subgroups of a group G. Define a relation $\sim$ on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are called **double cosets**. Compute the double cosets of $H = \{(1), (123), (132)\}$ in A_4.

Solution. The relation is reflexive since $a \sim a$, or $eae = a$. If $a \sim b$, then there exist $h \in H$ and $k \in K$ such that $hak = b$. This implies that $h^{-1}bk^{-1} = a$ or $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1ak_1 = b$ and $h_2bk_2 = c$. Hence, $h_2h_1ak_1k_2 = c$ or $a \sim c$. If $H = \{(1), (123), (132)\}$ and $K = (12)(34)$ are subgroups of A_4, then the double cosets of H and K are $H(1)K$ and $H(13)(24)K$.

21. Let G be a cyclic group of order n. Show that there are exactly $\phi(n)$ generators for G.

Solution. This follows directly from Corollary 4.14.

22. Let $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes. Prove that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Hint. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$ (Exercise 2.3.26 in Chapter 2).

Solution. If p is prime, then the only possible values of $\gcd(p^e, m)$ are $1, p, p^2, \ldots, p^e$. Thus, if $\gcd(p^e, m) \neq 1$, then m must be a multiple of p. There are exactly p^{e-1} multiples of p that are less than or equal to p^e: $p, 2p, 3p, \ldots, p^{e-1}p =$

p^e. Consequently, there are $p^e - p^{e-1}$ numbers that are relatively prime to p^e, and

$$\phi\left(p^e\right) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right).$$

To show the general case we must use the fact that f $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$ (Exercise 2.3.26 in Chapter 2). Thus, if $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, then

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}\right)\\
&= \phi\left(p_1^{e_1}\right)\phi\left(p_2^{e_2}\right)\cdots\phi\left(p_k^{e_k}\right)\\
&= p^{e_1}\left(1-\frac{1}{p_1}\right)p^{e_2}\left(1-\frac{1}{p_2}\right)\cdots p^{e_k}\left(1-\frac{1}{p_k}\right)\\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

23. Show that

$$n = \sum_{d|n}\phi(d)$$

for all positive integers n.

Solution. If G is a cyclic group of order n and g is a generator for G, then $h = g^{n/d}$ has order d. In fact, all of the elements $g^{kn/d}$ have order d, where $\gcd(k,d) = 1$. If $(g^i)^d = e$, then $n \mid di$. Consequently, $i = dj/n$ for some j. The only elements of order d are the elements $h^{kn/d}$, where $\gcd(k,d) = 1$. Therefore, there are $\phi(d)$ elements in G of order d. Every element of G has order d for some divisor of d of n. For each such divisor, there are $\phi(d)$ elements of order d. Summing $\sum_{d|n}\phi(d)$ over all divisors d of n, each element in G is counted exactly once. Thus, $n = \sum_{d|n}\phi(d)$.

6.6 Sage Exercises

The following exercises are less about cosets and subgroups, and more about using Sage as an experimental tool. They are designed to help you become both more efficient, and more expressive, as you write commands in Sage. We will have many opportunities to work with cosets and subgroups in the coming chapters. These exercises do not contain much guidance, and get more challenging as they go. They are designed to explore, or confirm, results presented in this chapter or earlier chapters.

Important: You should answer each of the last three problems with a single (complicated) line of Sage that concludes by outputting `True`. A "single line" means you will have several Sage commands packaged up together in complicated ways. It does not mean several Sage commands seperated by semi-colons and typed in on a single line. Be sure include some intermediate steps used in building up your solution, but using smaller ranges of values so as to not overwhelm the reader with lots of output. This will help you, and the grader of your work, have some confidence that the final version is correct.

When you check integers below for divisibility, remember that `range()` produces plain integers, which are quite simple in their functionality. The `srange()` command produces Sage integers, which have many more capabilities. (See the last exercise for an example.) And remember that a list comprehension is a very compact way to examine many possibilities at once.**1**. Use `.subgroups()` to find an example of a group G and an integer m, so that (a) m divides the order of G, and (b) G has no subgroup of order m. (Do not use

the group A_4 for G, since this is in the text.) Provide a single line of Sage code that has all the logic to produce the desired m as its output. (You can give your group a simple name on a prior line and then just reference the group by name.) Here is a very simple example that might help you structure your answer.

```
a = 5
b = 10
c = 6
d = 13
a.divides(b)
```

```
True
```

```
not (b in [c,d])
```

```
True
```

```
a.divides(b) and not (b in [c,d])
```

```
True
```

Solution. Obviously, trying a cyclic group is a bad idea. Most students seem to locate S_5 as another good example.

```
G = SymmetricGroup(5)
[m for m in G.order().divisors() if not m in [H.order() for
    H in G.subgroups()]]
```

```
[15, 30, 40]
```

2. Verify the truth of Fermat's Little Theorem (either variant) using the composite number $391 = 17 \cdot 23$ as the choice of the base (either a or b), and for p assuming the value of every prime number between 100 and 1000.

Build up a solution slowly — make a list of powers (start with just a few primes), then make a list of powers reduced by modular arithmetic, then a list of comparisons with the predicted value, then a check on all these logical values resulting from the comparisons. This is a useful strategy for many similar problems. Eventually you will write a single line that performs the verification by eventually printing out `True`. Here are some more hints about useful functions.

```
a = 20
b = 6
a.mod(b)
```

```
2
```

```
prime_range(50, 100)
```

```
[53, 59, 61, 67, 71, 73, 79, 83, 89, 97]
```

```
all([True, True, True, True])
```

```
True
```

```
all([True, True, False, True])
```

```
False
```

Solution. In this solution we illustrate the iterative process of building up a one-line answer. We use a small range of primes while preparing, and step up to a much larger rangefor the last command.

```
[391^p for p in prime_range(10, 30)]
```

```
[326545972241270073519271047 91,
 499226747822176101096996770755 2871,
 116682271665240995398700190007771 5033650612231,
 178385023744537086175486837485694820595392484875 11,
 416932183469155632321565453207153159904473650785018605089271,
 148979312051002328104356742363210374050137615783680207088025809007332979991 1]
```

```
[(391^p).mod(p) for p in prime_range(10, 30)]
```

```
[6, 1, 0, 11, 0, 14]
```

```
[(391^p).mod(p) == (391).mod(p) for p in prime_range(10, 30)]
```

```
[True, True, True, True, True, True]
```

```
all([(391^p).mod(p) == (391).mod(p) for p in prime_range(10,
    30)])
```

```
True
```

```
all([(391^p).mod(p) == (391).mod(p) for p in
    prime_range(100, 1000)])
```

```
True
```

3. Verify that the group of units mod n has order $n-1$ when n is prime, again for all primes between 100 and 1000. As before, your output should be simply `True`, just once, indicating that the statement about the order is true for all the primes examined. As before, build up your solution slowly, and with a smaller range of primes in the beginning. Express your answer as a single line of Sage code.

Solution.

```
all([len(Integers(p).list_of_elements_of_multiplicative_group())
    == p-1
     for p in prime_range(100, 1000)])
```

```
True
```

4. Verify Euler's Theorem for all values of $0 < n < 100$ and for $1 \leq a \leq n$. This will require nested `for` statements with a conditional. Again, here is a small example that might be helpful for constructing your one line of Sage code. Note the use of `srange()` in this example.

```
[a/b for a in srange(9) for b in srange(1,a) if gcd(a,b)==1]
```

```
[2, 3, 3/2, 4, 4/3, 5, 5/2, 5/3, 5/4, 6, 6/5,
 7, 7/2, 7/3, 7/4, 7/5, 7/6, 8, 8/3, 8/5, 8/7]
```

Solution. The `.mod()` method could be used, as above, or the $power_mod()$ function. Instead, this solution from Anna Dovzhik, uses divisiblity by n for her condition.

If the condition is written to check equality with 1, such as `power_mod(a, euler_phi(n), n) == 1`, then the test will fail when $n = 1$, so look carefully for solutions where the range begins at 2.

```
all([n.divides(a^euler_phi(n)-1)
        for n in srange(1, 100)
        for a in srange(1, n+1)
        if gcd(a,n) == 1])
```

```
True
```

5. The symmetric group on 7 symbols, S_7, has $7! = 5040$ elements. Consider the following questions without employing Sage, based on what we know about orders of elements of permutation groups (Exercise 5.3.13).

- What is the maximum possible order?
- How many elements are there of order 10?
- How many elements are there of order 1?
- How many elements are there of order 2?
- What is the smallest positive integer for which there is no element with that order?

These questions will be easier if you are familiar with using binomial coefficients for counting in similarly complex situations. But either way, give some serious thought to each question (and maybe a few of your own) before firing up Sage.

Now, compute how many elements there are of each order using the `.order()` method, and then embed this into a list comprehension which creates a single list of these counts. You can check your work (or check Sage) by wrapping this list in `sum()` and hopefully getting 5040.

Comment on the process of studying these questions first without any computational aid, and then again with Sage. For which values of n do you think Sage would be too slow and your mind quicker?

Solution.

```
[len([x for x in SymmetricGroup(7) if x.order() == k ]) for
    k in range(15)]
```

```
[0, 1, 231, 350, 840, 504, 1470, 720, 0, 0, 504, 0, 420, 0, 0]
```

```
sum([len([x for x in SymmetricGroup(7) if x.order() == k ])
    for k in range(15)])
```

```
5040
```

Chapter 7

Introduction to Cryptography

7.3 Exercises

1. Encode IXLOVEXMATH using the cryptosystem in Example 1.

Hint. LAORYHAPDWK

Solution. LAORYHAPDWK

2. Decode ZLOOA WKLVA EHARQ WKHA ILQDO, which was encoded using the cryptosystem in Example 1.

Solution. Will this be on the final?

3. Assuming that monoalphabetic code was used to encode the following secret message, what was the original message?

```
APHUO EGEHP PEXOV FKEUH CKVUE CHKVE APHUO
EGEHU EXOVL EXDKT VGEFT EHFKE UHCKF TZEXO
VEZDT TVKUE XOVKV ENOHK ZFTEH TEHKQ LEROF
PVEHP PEXOV ERYKP GERYT GVKEG XDRTE RGAGA
```

What is the significance of this message in the history of cryptography?

Hint. Hint: V = E, E = X (also used for spaces and punctuation), K = R.

Solution. This is a stanza in "The Charge of the Light Brigade", a poem by Alfred Lord Tennyson about the Charge of the Light Brigade at the Battle of Balaclava during the Crimean War. The phrase "the world wonders" was used as as security padding in an encrypted message sent from Admiral Chester Nimitz to Admiral William Halsey, Jr. on October 25, 1944 during the Battle of Leyte Gulf.

The Charge of the Light Brigade

Half a league, half a league,
Half a league onward,
All in the valley of Death
Rode the six hundred.
"Forward, the Light Brigade!
Charge for the guns!" he said:
Into the valley of Death
Rode the six hundred.

"Forward, the Light Brigade!"
Was there a man dismay'd?
Not tho' the soldier knew
Someone had blunder'd:
Theirs not to make reply,
Theirs not to reason why,
Theirs but to do and die:
Into the valley of Death
Rode the six hundred.

Alfred Lord Tennyson

The last 10 characters are padding.

4. What is the total number of possible monoalphabetic cryptosystems? How secure are such cryptosystems?

Hint. $26! - 1$

Solution. The total number of possible monoalphabetic cryptosystems is $26! - 1$. While such cryptosystems are not likely to be broken by random guessing, they can be broken using statistical analysis.

5. Prove that a 2×2 matrix A with entries in $\mathbb{Z}_{26}$ is invertible if and only if $\gcd(\det(A), 26) = 1$.

Solution. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & 26 - b \\ 26 - c & a \end{pmatrix}.$$

We know that $(ad - bc)^{-1}$ exists exactly when $\gcd(\det(A), 26) = 1$.

6. Given the matrix

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix},$$

use the encryption function $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ to encode the message CRYPTOLOGY, where $\mathbf{b} = (2, 5)^{\mathrm{t}}$. What is the decoding function?

Solution. CRYPTOLOGY encodes as 2203 0215 0600 1112 1006. The decoding function is

$$f(\mathbf{p}) = A^{-1}\mathbf{p} - A^{-1}\mathbf{b},$$

where

$$A^{-1} = \begin{pmatrix} 3 & 22 \\ 24 & 3 \end{pmatrix}.$$

7. Encrypt each of the following RSA messages x so that x is divided into blocks of integers of length 2; that is, if $x = 142528$, encode 14, 25, and 28 separately.

(a) $n = 3551, E = 629, x = 31$

(b) $n = 2257, E = 47, x = 23$

(c) $n = 120979, E = 13251, x = 142371$

(d) $n = 45629, E = 781, x = 231561$

Hint. (a) 2791; (c) 112135 25032 442.

Solution.

(a) 2791

(b) 769

(c) 112135 25032 442

(d) 4438 16332 31594

8. Compute the decoding key D for each of the encoding keys in Exercise 7.

Solution. (a) $3551 = 53 \cdot 67$; (b) $2257 = 37 \cdot 61$; (c) $120979 = 311 \cdot 389$; (d) $45629 = 103 \cdot 443$.

9. Decrypt each of the following RSA messages y.

(a) $n = 3551, D = 1997, y = 2791$

(b) $n = 5893, D = 81, y = 34$

(c) $n = 120979, D = 27331, y = 112135$

(d) $n = 79403, D = 671, y = 129381$

Hint. (a) 31; (c) 14.

Solution.

(a) 31

(b) 2014

(c) 14

(d) 21712

10. For each of the following encryption keys (n, E) in the RSA cryptosystem, compute D.

(a) $(n, E) = (451, 231)$

(b) $(n, E) = (3053, 1921)$

(c) $(n, E) = (37986733, 12371)$

(d) $(n, E) = (16394854313, 34578451)$

Hint. (a) $n = 11 \cdot 41$; (c) $n = 8779 \cdot 4327$.

Solution.

(a) $n = 11 \cdot 41$

(b) $n = 43 \cdot 17$

(c) $n = 8779 \cdot 4327$

(d) $n = 118861 \cdot 137933$

11. Encrypted messages are often divided into blocks of n letters. A message such as `THE WORLD WONDERS WHY` might be encrypted as `JIW OCFRJ LPOEVYQ IOC` but sent as `JIW OCF RJL POE VYQ IOC`. What are the advantages of using blocks of n letters?

Solution. Using blocks of n letters makes it difficult to guess word size. Knowing the size of each word would be an aid in breaking the cryptosystem.

12. Find integers n, E, and X such that

$$X^E \equiv X \pmod{n}.$$

Is this a potential problem in the RSA cryptosystem?

Solution. Let $X = 225$, $E = 256$, and $n = 45629$.

13. Every person in the class should construct an RSA cryptosystem using primes that are 10 to 15 digits long. Hand in (n, E) and an encoded message. Keep D secret. See if you can break one another's codes.

Solution. Various solutions possible.

7.6 Sage Exercises

1. Construct a keypair for Alice using the first two primes greater than 10^{12}. For your choice of E, use a single prime number and use the smallest possible choice.

Output the values of n, E, and D for Alice. Then use Sage commands to verify that Alice's encryption and decryption keys are multiplicative inverses.

Solution. 3 and 5 are not relatively prime to m, so cannot be used as E.

```
pA1 = next_prime(10^12)
pA2 = next_prime(pA1)
nA = pA1*pA2
mA = euler_phi(nA)
EA = 7
DA = inverse_mod(EA, mA)
nA, EA, DA
```

```
(1000000000100000000002379, 7, 142857142871142857143183)
```

```
(DA*EA).mod(mA)
```

```
1
```

2. Construct a keypair for Bob using the first two primes greater than $2 \cdot 10^{12}$. For your choice of E, use a single prime number and use the smallest possible choice. Output the values of n, E, and D for Alice.

Encode the word `Math` using ASCII values in the same manner as described in this section (keep the capitalization as shown). Create a signed message of this word for communication from Alice to Bob. Output the three integers: the message, the signed message and the signed, encrypted message.

Solution.

```
pB1 = next_prime(2*10^12)
pB2 = next_prime(pB1)
nB = pB1*pB2
mB = euler_phi(nB)
EB = 3
DB = inverse_mod(EB, mB)
nB, EB, DB
```

```
(4000000000252000000000369, 3, 2666666666832000000000163)
```

```
word = 'Math'
message = sum( [ord(word[i])*128^i for i in range(4)] )
signed = power_mod(message, DA, nA)
encrypted = power_mod(signed, EB, nB)
message, signed, encrypted
```

```
(220016845, 3069421371172381473534 97,
    3647527136466047967324540)
```

3. Demonstrate how Bob converts the message received from Alice back into the word `Math`. Output the value of the intermediate computations and the final human-readable message.

Solution.

```
decrypted = power_mod(encrypted, DB, nB)
received = power_mod(decrypted, EA, nA)
text = map(chr, received.digits(base=128))
decrypted, received, ''.join(text)
```

```
(3069421371172381473534 97, 220016845, 'Math')
```

4. Create a new signed message from Alice to Bob. Simulate the message being tampered with by adding 1 to the integer Bob receives, before he decrypts it. What result does Bob get for the letters of the message when he decrypts and unsigns the tampered message?

Solution.

```
word = 'Moon'
message = sum( [ord(word[i])*128^i for i in range(4)] )
signed = power_mod(message, DA, nA)
encrypted = power_mod(signed, EB, nB)

tampered = encrypted + 1

decrypted = power_mod(tampered, DB, nB)
received = power_mod(decrypted, EA, nA)
text = map(chr, received.digits(base=128))
text
```

```
['\x04', '8', '\x03', 'f', '-', '?', 'F', '\x1e', "'", 'p',
    'N', '\x04']
```

5. Classroom Exercise. Organize a class into several small groups. Have each group construct key pairs with some minimum size (digits in n). Each group should keep their private key to themselves, but make their public key available to everybody in the room. It could be written on the board (error-prone) or maybe pasted in a public site like pastebin.com. Then each group can send a signed message to another group, where the groups could be arranged logically in a circular fashion for this purpose. Of course, messages should be posted publicly as well. Expect a success rate somewhere between 50% and 100%.

If you do not do this in class, grab a study buddy and send each other messages in the same manner. Expect a success rate of 0%, 50% or 100%.

Chapter 8

Algebraic Coding Theory

8.5 Exercises

1. Why is the following encoding scheme not acceptable?

Information	0	1	2	3	4	5	6	7	8
Codeword	000	001	010	011	101	110	111	000	001

Solution. 1 and 8 are encoded into the same 3-tuple.

2. Without doing any addition, explain why the following set of 4-tuples in $\mathbb{Z}_2^4$ cannot be a group code.

$$(0110) \quad (1001) \quad (1010) \quad (1100)$$

Hint. This cannot be a group code since $(0000) \notin C$.

Solution. This cannot be a group code since $(0000) \notin C$.

3. Compute the Hamming distances between the following pairs of n-tuples.

(a) $(011010), (011100)$

(b) $(11110101), (01010100)$

(c) $(00110), (01111)$

(d) $(1001), (0111)$

Hint. (a) 2; (c) 2.

Solution. (a) 2; (b) 3; (c) 2; (d) 3.

4. Compute the weights of the following n-tuples.

(a) (011010)

(b) (11110101)

(c) (01111)

(d) (1011)

Hint. (a) 3; (c) 4.

Solution. (a) 3; (b) 6; (c) 4; (d) 3.

5. Suppose that a linear code C has a minimum weight of 7. What are the error-detection and error-correction capabilities of C?

Solution. The code can detect 6 or fewer errors. The code can also correct up to 3 errors.

6. In each of the following codes, what is the minimum distance for the code? What is the best situation we might hope for in connection with error detection and error correction?

(a) (011010) (011100) (110111) (110000)

(b) (011100) (011011) (111011) (100011) (000000) (010101) (110100) (110011)

(c) (000000) (011100) (110101) (110001)

(d) (0110110) (0111100) (1110000) (1111111) (1001001) (1000011) (0001111) (0000000)

Hint. (a) $d_{\min} = 2$; (c) $d_{\min} = 1$.

Solution. (a) $d_{\min} = 2$; (b) $d_{\min} = 1$; (c) $d_{\min} = 1$; (d) $d_{\min} = 2$. We can detect but not correct single errors in (a) and (d).

7. Compute the null space of each of the following matrices. What type of (n, k)-block codes are the null spaces? Can you find a matrix (not necessarily a standard generator matrix) that generates each code? Are your generator matrices unique?

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Hint.

(a) $(00000), (00101), (10011), (10110)$

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

(b) $(000000), (010111), (101101), (111010)$

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

Solution.

(a) $(00000), (00101), (10011), (10110)$

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

(b) $(000000), (010111), (101101), (111010)$

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

(c) $(00011), (00111), (11010), (11110), (11001), (11101), (00000), (00100)$

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

(d) (0000000), (1110000), (1101001), (0011001), (0101010), (1011010), (1000011), (0110011), (1001100), (0111100), (0100101), (1010101), (1100110), (0010110), (0001111), (1111111)

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

8. Construct a $(5, 2)$-block code. Discuss both the error-detection and error-correction capabilities of your code.

Solution. The matrix

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

generates the single error-detecting code $(00000), (01111), (10111), (11000)$.

9. Let C be the code obtained from the null space of the matrix

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

Decode the message

$$01111 \quad 10101 \quad 01110 \quad 00011$$

if possible.

Hint. Multiple errors occur in one of the received words.

Solution. Multiple errors occur in one of the received words so it is not possible to decode the message.

10. Suppose that a 1000-bit binary message is transmitted. Assume that the probability of a single error is p and that the errors occurring in different bits are independent of one another. If $p = 0.01$, what is the probability of more than one error occurring? What is the probability of exactly two errors occurring? Repeat this problem for $p = 0.0001$.

Solution. For $p = 0.01$, the probability of more than one error is 0.999. The probability of exactly two errors is 0.00220. For $p = 0.0001$, the probability of more than one error is 0.00467. The probability of exactly two errors is 0.00452.

11. Which matrices are canonical parity-check matrices? For those matrices that are canonical parity-check matrices, what are the corresponding standard generator matrices? What are the error-detection and error-correction capabilities of the code generated by each of these matrices?

(a)
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Hint. (a) A canonical parity-check matrix with standard generator matrix

$$G = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(c) A canonical parity-check matrix with standard generator matrix

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

Solution.

(a) A canonical parity-check matrix with standard generator matrix

$$G = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(b) A canonical parity-check matrix with standard generator matrix

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

(c) A canonical parity-check matrix with standard generator matrix

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

(d) A canonical parity-check matrix with standard generator matrix

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

12. List all possible syndromes for the codes generated by each of the matrices in Exercise 8.5.11.

Hint. (a) All possible syndromes occur.

Solution. In each case all possible syndromes occur.

13. Let

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

Compute the syndrome caused by each of the following transmission errors.

(a) An error in the first bit.

(b) An error in the third bit.

(c) An error in the last bit.

(d) Errors in the third and fourth bits.

Solution. (a) $(001)^t$; (b) $(101)^t$; (c) $(111)^t$; (d) $(011)^t$.

14. Let C be the group code in $\mathbb{Z}_2^3$ defined by the codewords (000) and (111). Compute the cosets of C in $\mathbb{Z}_2^3$. Why was there no need to specify right or left cosets? Give the single transmission error, if any, to which each coset corresponds.

Solution.

$$C = \{(000), (111)\}$$
$$(001) + C = \{(001), (110)\}$$

$$(010) + C = \{(010), (101)\}$$
$$(100) + C = \{(100), (011)\}$$

15. For each of the following matrices, find the cosets of the corresponding code C. Give a decoding table for each code if possible.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Hint. (a) C, $(10000)+C$, $(01000)+C$, $(00100)+C$, $(00010)+C$, $(11000)+C$, $(01100) + C$, $(01010) + C$. A decoding table does not exist for C since this is only a single error-detecting code.

Solution.

(a) C, $(10000) + C$, $(01000) + C$, $(00100) + C$, $(00010) + C$, $(11000) + C$, $(01100) + C$, $(01010) + C$.

(b) C, $(00001) + C$, $(00100) + C$, $(10000) + C$, $(00101) + C$, $(10001) + C$, $(10100) + C$, $(10101) + C$.

(c) C, $(00001) + C$, $(01000) + C$, $(10000) + C$.

(d) C, $(0000001)+C$, $(0000010)+C$, $(0000100)+C$, $(0001000)+C$, $(0010000)+C$, $(0100000) + C$, $(1000000) + C$.

16. Let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ be binary n-tuples. Prove each of the following statements.

(a) $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$

(b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z})$

(c) $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$

Solution. First note that $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}-\mathbf{y})$, since both sides of the equation are equal to the number of positions in which $\mathbf{x}$ and $\mathbf{y}$ differ. Hence, (c) is true. (a) is true, since $d(\mathbf{x}, \mathbf{0}) = w(\mathbf{x} - \mathbf{0}) = w(\mathbf{x})$. (c) is true, since $d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z}) = w((\mathbf{x} + \mathbf{z}) - (\mathbf{y} + \mathbf{z})) = w(\mathbf{x} - \mathbf{y}) = d(\mathbf{x} - \mathbf{y})$.

17. A **metric** on a set X is a map $d : X \times X \to \mathbb{R}$ satisfying the following conditions.

(a) $d(\mathbf{x}, \mathbf{y}) \geq 0$ for all $\mathbf{x}, \mathbf{y} \in X$;

(b) $d(\mathbf{x}, \mathbf{y}) = 0$ exactly when $\mathbf{x} = \mathbf{y}$;

(c) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;

(d) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

In other words, a metric is simply a generalization of the notion of distance. Prove that Hamming distance is a metric on $\mathbb{Z}_2^n$. Decoding a message actually reduces to deciding which is the closest codeword in terms of distance.

Solution. (a), (b), and (c) follow directly from the definition of $d(\mathbf{x}, \mathbf{y})$. (d) follows from the fact that if $\mathbf{x}$ and $\mathbf{y}$ disagree on the ith position and $\mathbf{x}$ and $\mathbf{z}$ agree, then $\mathbf{y}$ and $\mathbf{z}$ must disagree.

18. Let C be a linear code. Show that either the ith coordinates in the codewords of C are all zeros or exactly half of them are zeros.

Solution. If X is the set of codewords in C whose ith coordinate is 1 and Y is the set of codewords in C whose ith coordinate is 0, then $X \cup Y = C$. If X is nonempty, then there exists an $\mathbf{a} \in X$ whose ith coordinate is 1. If we define the map $f : X \to Y$ defined by $f : \mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$, then this map is a bijection since $f(f(\mathbf{x})) = \mathbf{x}$.

19. Let C be a linear code. Show that either every codeword has even weight or exactly half of the codewords have even weight.

Hint. Let $\mathbf{x} \in C$ have odd weight and define a map from the set of odd codewords to the set of even codewords by $\mathbf{y} \mapsto \mathbf{x} + \mathbf{y}$. Show that this map is a bijection.

Solution. Let $\mathbf{x} \in C$ have odd weight and define a map from the set of odd codewords to the set of even codewords by $f : \mathbf{y} \mapsto \mathbf{x} + \mathbf{y}$. Since

$$f(f(\mathbf{y})) = f(\mathbf{x} + \mathbf{y}) = \mathbf{x} + \mathbf{x} + \mathbf{y} = \mathbf{y},$$

the inverse function of f is itself. Hence, f is bijective.

20. Show that the codewords of even weight in a linear code C are also a linear code.

Solution. This follows from the fact that a codeword of even weight must be the sum of an even number of n-tuples of weight 1.

21. If we are to use an error-correcting linear code to transmit the 128 ASCII characters, what size matrix must be used? What size matrix must be used to transmit the extended ASCII character set of 256 characters? What if we require only error detection in both cases?

Solution. For 128 characters we need at least an 1×8 canonical parity-check for error-detection and an 11×4 canonical parity-check for error-correction. For 256 characters we need at least an 1×9 canonical parity-check for error-detection and an 12×4 canonical parity-check for error-correction.

22. Find the canonical parity-check matrix that gives the even parity check bit code with three information positions. What is the matrix for seven information positions? What are the corresponding standard generator matrices?

Solution. Use the parity-check matrices (1111) and (11111111), respectively. the generator matrices are

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

and

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

respectively.

23. How many check positions are needed for a single error-correcting code with 20 information positions? With 32 information positions?

Hint. For 20 information positions, at least 6 check bits are needed to ensure an error-correcting code.

Solution. For 20 information positions, at least 6 check bits are needed to ensure an error-correcting code. For 32 information positions, at least 7 check bits are needed to ensure an error-correcting code.

24. Let $\mathbf{e}_i$ be the binary n-tuple with a 1 in the ith coordinate and 0's elsewhere and suppose that $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Show that $H\mathbf{e}_i$ is the ith column of the matrix H.

Solution. Follows directly from the definition of matrix multiplication.

25. Let C be an (n, k)-linear code. Define the **dual** or **orthogonal code** of C to be

$$C^\perp = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in C\}.$$

(a) Find the dual code of the linear code C where C is given by the matrix

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

(b) Show that $C^\perp$ is an $(n, n-k)$-linear code.

(c) Find the standard generator and parity-check matrices of C and $C^\perp$. What happens in general? Prove your conjecture.

Solution.

(a) If C is the null space of

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

then

$$C = \{(00000), (01101), (10111), (11010)\}$$
$$C^\perp = \{(00000), (11001), (10010), (01011), (11100), (00101), (01110), (10111)\}$$

(b) For C and $C^\perp$ in (a), this is easy to see. For C and $C^\perp$ in general, this follows from part (c)

(c) The standard generator and parity-check matrices for C are

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix},$$

respectively. The standard generator and parity-check matrices for $C^\perp$ are G^t and H^t, respectively. This is true in general.

26. Let H be an $m \times n$ matrix over $\mathbb{Z}_2$, where the ith column is the number i written in binary with m bits. The null space of such a matrix is called a **Hamming code**.

(a) Show that the matrix

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

generates a Hamming code. What are the error-correcting properties of a Hamming code?

(b) The column corresponding to the syndrome also marks the bit that was in error; that is, the ith column of the matrix is i written as a binary number, and the syndrome immediately tells us which bit is in error. If the received word is (101011), compute the syndrome. In which bit did the error occur in this case, and what codeword was originally transmitted?

(c) Give a binary matrix H for the Hamming code with six information positions and four check positions. What are the check positions and what are the information positions? Encode the messages (101101) and (001001). Decode the received words (0010000101) and (0000101100). What are the possible syndromes for this code?

(d) What is the number of check bits and the number of information bits in an (m, n)-block Hamming code? Give both an upper and a lower bound on the number of information bits in terms of the number of check bits. Hamming codes having the maximum possible number of information bits with k check bits are called **perfect**. Every possible syndrome except **0** occurs as a column. If the number of information bits is less than the maximum, then the code is called **shortened**. In this case, give an example showing that some syndromes can represent multiple errors.

Solution.

(a) The null space of H is a Hamming code that has the ability to correct single errors.

(b) An error occurred in the first bit. The original codeword was (001011).

(c)

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

Check positions occur in columns 1, 2, 4, and 8. Information positions occur in columns 3, 5, 6, 7, 9, and 10. The messages (101101) and (001001) are encoded to (0010011101) and (0001010101), respectively. The received words (0010000101) and (0000101100), have errors in the first and tenth bits, respectively.

(d) If H is given by an $r \times s$ matrix, then H can have at most $2^{s-r} - r - 1$ information positions.

8.8 Sage Exercises

1. Create the (binary) Golay code with the `codes.GolayCode()` constructor. Read the documentation to be sure you build the binary version (not ternary), and do not build the extended version (which is the default).

(a) Use Sage methods to compute the length, dimension and minimum distance of the code.

(b) How many errors can this code detect? How many can it correct?

(c) Find a nonzero codeword and introduce three errors by adding a vector with three 1's (your choice) to create a received message. Show that the message is decoded properly.

(d) Recycle your choices from the previous part, but now add one more error. Does the new received message get decoded properly?

Solution.

```
G = codes.GolayCode(GF(2), extended=False)
G.length(), G.dimension(), G.minimum_distance()
```

```
(23, 12, 7)
```

We grab the second element of the code (the first is the zero vector) and for convenience place errors in the first three bits.

```
message = G.list()[1]
error = vector([1,1,1] + 20*[0])
received = message + error
received
```

```
(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0,
    0, 0, 0)
```

```
G.decode_to_code(received) == message
```

```
True
```

We flip the fourth bit from a `0` to a `1` to introduce a fourth error. Since the Golay code is a perfect code (see below), no matter what choices are made, this will move the received message closer to *some other* codeword and the decoding will be incorrect.

```
received[3] = 1
G.decode_to_code(received) == message
```

```
False
```

2. One technique for improving the characteristics of a code is to add an overall parity-check bit, much like the lone parity-check bit of the ASCII code described in Example 8.3. Such codes are referred to as the **extended** version of the original.

(a) Construct the (binary) Golay code and obtain the parity-check matrix. Use Sage commands to enlarge this matrix to create a new parity check matrix that has an additional overall parity-check bit. You may find the matrix methods `.augment()` and `.stack()` useful, as well as the constructors `zero_vector()` and `ones_matrix()` (remembering that we specify the binary entries as being from the field `GF(2)`.)

Create the extended code by supplying your enlarged parity-check matrix to the `codes.from_parity_check_matrix()` constructor and compute the length, dimension and minimum distance of the extended code.

(b) How are the properties of this new code better? At what cost?

(c) Now create the extended (binary) Golay code with the Sage constructor `codes.GolayCode()` and the correct keyword to obtain the extended version. With luck, the sorted lists of your codewords and Sage's codewords will be equal. If not, the linear code method `.is_permutation_equivalent()` should return `True` to indicate that your code and Sage's are just rearrangements of each other.

Solution. A typical approach is to add a column of zeros to the end of the parity-check matrix, and then a row of all 1's. This will create the same extended code as Sage's. To fully test the equivalence routine, we will place the check bit *within* the matrix.

```
G = codes.GolayCode(GF(2), extended=False)
C = G.parity_check_matrix()
EC_cols =
    C[:,0:8].augment(zero_vector(GF(2),11)).augment(C[:,8:23])
EC = EC_cols.stack(ones_matrix(GF(2), 1, 24))
EG = codes.from_parity_check_matrix(EC)
EG.length(), EG.dimension(), EG.minimum_distance()
```

```
(24, 12, 8)
```

The verbose option will give back a permutation that shows the equivalence of the codes.

```
SEG = codes.GolayCode(GF(2), extended=True)
EG.is_permutation_equivalent(SEG, algorithm="verbose")
```

```
(True, (9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24))
```

3. *Note:* This problem is on holiday (as of Sage 6.7), while some buggy Sage code for the minimum distance of a Hamming code gets sorted out. The `r = 2` case produces an error message and for `r > 5` the computation of the minimum distance has become intolerably slow. So it is a bit harder to make a reasonable conjecture from just 3 cases.

The dual of an (n, k) block code is formed as all the set of all binary vectors which are orthogonal to every vector of the original code. Exercise 8.5.25 describes this construction and asks about some of its properties.

You can construct the dual of a code in Sage with the `.dual_code()` method. Construct the binary Hamming codes, and their duals, with the parameter `r` ranging from `2` to `5`, inclusive. Build a table with six columns (perhaps

employing the `html.table()` function) that lists r, the length of the codes, the dimensions of the original and the dual, and the minimum distances of the orginal and the dual.

Conjecture formulas for the dimension and minimum distance of the dual of the Hamming code as expressions in the parameter r.

Solution. The computations for $r = 7, 8, 9, 10$ take a long time, so we do not test them.

```
for r in range(2, 6): # was range(2, 8)
    C = codes.HammingCode(GF(2), r)
    D = C.dual_code()
    (r, C.length(),
    C.dimension(), C.minimum_distance(),
    D.dimension(), D.minimum_distance())
```

```
(2, 3, 1, 3, 2, 2)
(3, 7, 4, 3, 3, 4)
(4, 15, 11, 3, 4, 8)
(5, 31, 26, 3, 5, 16)
```

4. A code with minimum distance d is called **perfect** if every possible vector is within Hamming distance $(d-1)/2$ of some codeword. If we expand our notion of geometry to account for the Hamming distance as the metric, then we can speak of a sphere of radius r around a vector (or codeword. For a code of length n, such a sphere will contain

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$$

vectors within in it. For a perfect code, the spheres of radius d centered at the codewords of the code will exactly partition the entire set of all possible vectors. (This is the connection that means that coding theory meshes with sphere packing problems.)

A consequence of a code of dimension k being perfect is that

$$2^k \left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{\frac{d-1}{2}} \right) = 2^n$$

Conversely, if a code has minimum distance d and the condition above is true, then the code is perfect.

Write a Python function, named `is_perfect()` which accepts a linear code as input and returns `True` or `False`. Demonstrate your function by checking that the (binary) Golay code is perfect, and then use a loop to verify that the (binary) Hamming codes are perfect for all lengths below 32.

Solution.

```
def is_perfect(C):
    n = C.length()
    k = C.dimension()
    d = C.minimum_distance()
    spheres = [binomial(n, r) for r in range(0, (d-1)/2+1)]
    return 2^n == 2^k*sum(spheres)
```

```
is_perfect(codes.GolayCode(GF(2), extended=False))
```

```
True
```

```
for r in range(2, 6): # was range(3, 10), lengths to 1000
    C = codes.HammingCode(GF(2), r)
    C.length(), is_perfect(C)
```

```
(3, True)
(7, True)
(15, True)
(31, True)
```

Chapter 9

Isomorphisms

9.3 Exercises

1. Prove that $\mathbb{Z} \cong n\mathbb{Z}$ for $n \neq 0$.

Hint. Every infinite cyclic group is isomorphic to $\mathbb{Z}$ by Theorem 9.7.

Solution. Every infinite cyclic group is isomorphic to $\mathbb{Z}$ by Theorem 9.7. We can also prove this statement directly. Define $\phi : \mathbb{Z} \to n\mathbb{Z}$ by $\phi : r \mapsto rn$. Then ϕ perserves the group operation since

$$\phi(r+s) = n(r+s) = nr + ns = \phi(r) + \phi(s).$$

If $rn \in n\mathbb{Z}$, then $\phi(r) = rn$ demonstrating the ϕ is onto. Since $\ker \phi = \{0\}$, the map is one-to-one.

2. Prove that $\mathbb{C}^*$ is isomorphic to the subgroup of $GL_2(\mathbb{R})$ consisting of matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Hint. Define $\phi : \mathbb{C}^* \to GL_2(\mathbb{R})$ by

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Solution. Define $\phi : \mathbb{C}^* \to GL_2(\mathbb{R})$ by

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Since the determinant of this matrix is $a^2 + b^2$, we know that ϕ does indeed send elements in $\mathbb{C}^*$ to elements in $GL_2(\mathbb{R})$. Clearly, ϕ is onto, and it must also be one-to-one since two matrices are equal exactly when their corresponding entries are equal. Finally,

$$\begin{aligned} \phi(a+bi)\phi(c+di) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \\ &= \phi[(ac-bd) + (ad+bc)i] \\ &= \phi[(a+bi)(c+di)]. \end{aligned}$$

3. Prove or disprove: $U(8) \cong \mathbb{Z}_4$.

Hint. False.

Solution. False. The elements in $U(8)$ all have order two.

4. Prove that $U(8)$ is isomorphic to the group of matrices

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

Solution. Use the isomorphism

$$\begin{aligned} 1 &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 3 &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ 5 &\mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ 7 &\mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

5. Show that $U(5)$ is isomorphic to $U(10)$, but $U(12)$ is not.

Solution. $U(5)$ and $U(10)$ are both cyclic groups of order 4; however, $U(12)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

6. Show that the nth roots of unity are isomorphic to $\mathbb{Z}_n$.

Hint. Define a map from $\mathbb{Z}_n$ into the nth roots of unity by $k \mapsto \text{cis}(2k\pi/n)$.

Solution. Define a map ϕ from $\mathbb{Z}_n$ into the nth roots of unity by $\phi : k \mapsto \text{cis}(2k\pi/n)$. Then

$$\begin{aligned} \phi(j+k) &= \text{cis}\left(\frac{2(j+k)\pi}{n}\right) \\ &= \text{cis}\left(\frac{2j\pi}{n} + \frac{2k\pi}{n}\right) \\ &= \text{cis}\left(\frac{2j\pi}{n}\right) \text{cis}\left(\frac{2k\pi}{n}\right) \\ &= \phi(j)\phi(k). \end{aligned}$$

If

$$\text{cis}\left(\frac{2j\pi}{n}\right) = \phi(j) = \phi(k) = \text{cis}\left(\frac{2k\pi}{n}\right),$$

then $j = k$ and the map is one-to-one. The map is onto since $|\mathbb{Z}_n| = n$.

7. Show that any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Solution. Let g be a generator for a cyclic group G of order n and define $\phi : \mathbb{Z}_n \to G$ by $\phi(k) \mapsto g^k$. Then for $k_1, k_2 \in \mathbb{Z}_n$, we have

$$\phi(k_1 + k_2) = g^{k_1+k_2} = g^{k_1} g^{k_2} = \phi(k_1)\phi(k_2).$$

Furthermore, if $k_1 \neq k_2$, then $\phi(k_1) = g_{k_1} \neq g^{k_2} = \phi(k_2)$, and so ϕ is one-to-one. Since $|G| = |\mathbb{Z}_n| = n$, the map ϕ must also be onto. Therefore, $G \cong \mathbb{Z}_n$.

8. Prove that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$.

Hint. Assume that $\mathbb{Q}$ is cyclic and try to find a generator.

Solution. Suppose that $\mathbb{Q}$ is cyclic and assume that p/q is a generator for $\mathbb{Q}$, where $q \neq 0$ and p/q is in lowest terms. Then any element of $\mathbb{Q}$ can be written as np/q for some $n \in \mathbb{Z}$. However, if we chose $r \in \mathbb{N}$ such that $\gcd(r, q) = 1$, it is impossible to write $1/r$ as a multiple of p/q.

9. Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by

$$a * b = a + b + ab.$$

Prove that G is a group under this operation. Show that $(G, *)$ is isomorphic to the multiplicative group of nonzero real numbers.

Solution. We will show that the map $\phi : \mathbb{R}^* \to S$ defined by $\phi(a) = a - 1$ is an isomorphism. Since

$$\phi(ab) = ab - 1 = (a-1) + (b-1) + (a-1)(b-1) = (a-1) * (b-1) = \phi(a)\phi(b),$$

group operation is preserved. If

$$a - 1 = \phi(a) = \phi(b) = b - 1,$$

then $a = b$ and the map is one-to-one. If $a \in \mathbb{R} \setminus \{-1\}$, then $\phi(a + 1) = a$ and the map is onto.

10. Show that the matrices

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

form a group. Find an isomorphism of G with a more familiar group of order 6.

Solution. This group is isomorphic to S_3. One possible isomorphism is

$$(1) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (23) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad (12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$(123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad (13) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad (132) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

11. Find five non-isomorphic groups of order 8.

Hint. There are two nonabelian and three abelian groups that are not isomorphic.

Solution. D_4, Q_8, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

12. Prove S_4 is not isomorphic to D_{12}.

Solution. Although D_{12} has an element of order 12, S_4 does not.

13. Let $\omega = \operatorname{cis}(2\pi/n)$ be a primitive nth root of unity. Prove that the matrices

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

generate a multiplicative group isomorphic to D_n.

Solution. Certainly,

$$A^n = I,$$
$$B^2 = I,$$
$$BAB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix} = A^{-1},$$

where I is the 2×2 identity matrix. Since the generators and relations are the same, the two groups must be isomorphic.

14. Show that the set of all matrices of the form

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

is a group isomorphic to D_n, where all entries in the matrix are in $\mathbb{Z}_n$.

Solution. If we let

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

then $A^n = I$, $B^2 = I$, and

$$BAB = \begin{pmatrix} 1 & n-1 \\ 0 & 1 \end{pmatrix} = A^{-1},$$

where I is the 2×2 identity matrix. Since the generators and relations are the same, the two groups must be isomorphic.

15. List all of the elements of $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Solution. $(0,0)$, $(1,0)$, $(2,0)$, $(3,0)$, $(0,1)$, $(1,1)$, $(2,1)$, $(3,1)$.

16. Find the order of each of the following elements.

(a) $(3,4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $(6,15,4)$ in $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$

(c) $(5,10,15)$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$

(d) $(8,8,8)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

Hint. (a) 12; (c) 5.

Solution. (a) 12; (b) 30; (c) 5; (d) 30.

17. Prove that D_4 cannot be the internal direct product of two of its proper subgroups.

Solution. If D_4 is the internal direct product of two of its proper subgroups, say H and K, then one of the subgroups must have order 2 and the other must have order 4. However, no subgroup of order 2 commutes with a subgroup of order 4.

18. Prove that the subgroup of $\mathbb{Q}^*$ consisting of elements of the form $2^m 3^n$ for $m, n \in \mathbb{Z}$ is an internal direct product isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

Solution. Define a map $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*$ by $\phi : (m,n) \mapsto 2^m 3^n$. Then

$$\phi(m,n)\phi(r,s) = 2^m 3^n 2^r 3^s = 2^{m+r} 3^{n+s} = \phi(m+r, n+s) = \phi[(m,n) + (r,s)].$$

If $\phi(m,n) = \phi(r,s)$, then $2^m 3^n = 2^r 3^s$ or $2^{m-r} 3^{n-s} = 1$. Thus, $(m,n) = (r,s)$ adn the map is one-to-one. Clearly, the map is onto. Thus, ϕ is an isomorphism, and we have an internal direct product.

19. Prove that $S_3 \times \mathbb{Z}_2$ is isomorphic to D_6. Can you make a conjecture about D_{2n}? Prove your conjecture.

Hint. Draw the picture.

Solution. Since $S_3 \times \mathbb{Z}_2$ is nonabelian, it must be isomorphic to either A_4 or D_6. However, $S_3 \times \mathbb{Z}_2$ has a subgroup of order 6 and A_4 does not. Thus, $S_3 \times \mathbb{Z}_2 \cong D_6$.

20. Prove or disprove: Every abelian group of order divisible by 3 contains a subgroup of order 3.

Hint. True.

Solution. True.

21. Prove or disprove: Every nonabelian group of order divisible by 6 contains a subgroup of order 6.

Solution. False. A_6 contains no subgroup of order 6.

22. Let G be a group of order 20. If G has subgroups H and K of orders 4 and 5 respectively such that $hk = kh$ for all $h \in H$ and $k \in K$, prove that G is the internal direct product of H and K.

Solution. If $g \in H \cap K$, then $g^5 = g^4 = e$; hence, $g = e$. By a counting argument, $HK = G$.

23. Prove or disprove the following assertion. Let G, H, and K be groups. If $G \times K \cong H \times K$, then $G \cong H$.

Solution. False. Let $G = \mathbb{Z} \times \mathbb{Z} \times \cdots$, $H = \mathbb{Z}$, and $K = \mathbb{Z} \times \mathbb{Z}$.

24. Prove or disprove: There is a noncyclic abelian group of order 51.

Solution. By Theorem 9.21, every abelian group of order 51 is isomorphic to $\mathbb{Z}_{51}$ since $51 = 3 \cdot 17$.

25. Prove or disprove: There is a noncyclic abelian group of order 52.

Hint. True.

Solution. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{13}$ is not cyclic.

26. Let $\phi : G \to H$ be a group isomorphism. Show that $\phi(x) = e_H$ if and only if $x = e_G$, where e_G and e_H are the identities of G and H, respectively.

Solution. Since $\phi(e_G) = \phi(e_G^2) = \phi(e_G)\phi(e_G)$, it must be the case that $\phi(e_G) = e_H$. If $x = e$, then $\phi(x) = \phi(e_G) = e_H$. Conversely, if $\phi(x) = e_H = \phi(e_G)$, then $x = e_G$, since ϕ is one-to-one.

27. Let $G \cong H$. Show that if G is cyclic, then so is H.

Hint. Let a be a generator for G. If $\phi : G \to H$ is an isomorphism, show that $\phi(a)$ is a generator for H.

Solution. Let $h \in H$. If $\phi : G \to H$ is an isomorphism, then there exists an element $g \in G$ such that $\phi(g) = h$. If a is a generator for G, then $g = a^n$ for some integer n. Hence,

$$h = \phi(g) = \phi(a^n) = [\phi(a)]^n.$$

Thus, $\phi(a)$ is a generator for H.

28. Prove that any group G of order p, p prime, must be isomorphic to $\mathbb{Z}_p$.

Solution. Since the order of G is prime, it cannot contain any nontrivial proper subgroups and must therefore be cyclic. By Theorem 9.8, G must be isomorphic to $\mathbb{Z}_p$.

29. Show that S_n is isomorphic to a subgroup of A_{n+2}.

Solution. We can define an isomorphism $\phi : S_n \to A_{n+2}$ by

$$\phi(\sigma) = \begin{cases} \sigma & \text{if is even} \\ \sigma(n+1, n+2) & \text{if is odd.} \end{cases}$$

30. Prove that D_n is isomorphic to a subgroup of S_n.

Solution. If we number the vertices of a regular n-gon, then rigid motion of a regular n-gon is a permutation of the n vertices. therefore, D_n must be isomorphic to a subgroup of S_n.

31. Let $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be isomorphisms. Show that ϕ^{-1} and $\psi \circ \phi$ are both isomorphisms. Using these results, show that the isomorphism of groups determines an equivalence relation on the class of all groups.

Solution. That ϕ^{-1} is an isomorphism follows directly from the fact that ϕ is a bijection. If ϕ and ψ are bijections, then $\psi \circ \phi$ is also a bijection. If $a, b \in G_1$, then

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b).$$

32. Prove $U(5) \cong \mathbb{Z}_4$. Can you generalize this result for $U(p)$, where p is prime?

Solution. Noting that $U(5) = \{1, 2, 3, 4\}$ and any element other than the identity generates the entire group, it follows that $U(5) \cong \mathbb{Z}_4$. In general, $U(p) \cong \mathbb{Z}_{p-1}$, which we will prove in Chapter 22.

33. Write out the permutations associated with each element of S_3 in the proof of Cayley's Theorem.

Solution. $S_3 = \{\mathrm{id}, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ (see Table 3.7). The permutations $\lambda_g : G \to G$ are given by

$$\lambda_{id} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \end{pmatrix}$$

$$\lambda_{\rho_1} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \rho_1 & \rho_2 & id & \mu_3 & \mu_1 & \mu_2 \end{pmatrix}$$

$$\lambda_{\rho_2} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \rho_2 & id & \rho_1 & \mu_2 & \mu_3 & \mu_1 \end{pmatrix}$$

$$\lambda_{\mu_1} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \mu_1 & \mu_2 & \mu_3 & id & \rho_1 & \rho_2 \end{pmatrix}$$

$$\lambda_{\mu_2} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \mu_2 & \mu_3 & \mu_1 & \rho_2 & id & \rho_1 \end{pmatrix}$$

$$\lambda_{\mu_3} = \begin{pmatrix} id & \rho_1 & \rho_2 & \mu_1 & \mu_2 & \mu_3 \\ \mu_3 & \mu_1 & \mu_2 & \rho_1 & \rho_2 & id \end{pmatrix}.$$

34. An **automorphism** of a group G is an isomorphism with itself. Prove that complex conjugation is an automorphism of the additive group of complex numbers; that is, show that the map $\phi(a+bi) = a-bi$ is an isomorphism from $\mathbb{C}$ to $\mathbb{C}$.

Solution. If we define $\phi : \mathbb{C} \to \mathbb{C}$ by $\phi(a + bi) = a - bi$, then it is easy to show that ϕ is one-to-one and onto. If $z = a + bi$ and $w = c + di$, then

$$\phi(z+w) = \phi((a+c)+(b+d)i) = (a+c)-(b+d)i = (a-bi)+(c-di) = \phi(z)+\phi(w).$$

35. Prove that $a + ib \mapsto a - ib$ is an automorphism of $\mathbb{C}^*$.

Solution. Define $\phi : \mathbb{C}^* \to \mathbb{C}^*$ by $\phi(a+bi) = a-bi$. If $z = a+bi$ and $w = c+di$, then

$$\phi(zw) = \phi((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i = (a-bi)(c-di) = \phi(z)\phi(w).$$

It is straightforward to show that ϕ is one-to-one and onto.

36. Prove that $A \mapsto B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$ for all B in $GL_2(\mathbb{R})$.

Solution. Let $\phi_B : SL_2(\mathbb{R}) \to GL_2(\mathbb{R})$ be defined by $\phi_B(A) \mapsto B^{-1}AB$. If $A \in SL_2(\mathbb{R})$, then

$$\det(\phi_B(A)) = \det(B^{-1}AB) = (\det B^{-1})(\det A)(\det B) = \det A = 1.$$

Therefore, ϕ_B is a map from $SL_2(\mathbb{R})$ to itself. If $A_1, A_2 \in SL_2(\mathbb{R})$, then

$$\phi_B(A_1A_2) = B^{-1}A_1A_2B = (B^{-1}A_1B)(B^{-1}A_2B) = \phi_B(A_1)\phi_B(A_2).$$

If $\phi_B(A_1) = \phi_B(A_2)$, then $B^{-1}A_1B = B^{-1}A_2B$ or $A_1 = A_2$; therefore, ϕ_B is one-to-one. Also, ϕ_B is onto since $\phi_B(BAB^{-1}) = A$.

37. We will denote the set of all automorphisms of G by $\mathrm{Aut}(G)$. Prove that $\mathrm{Aut}(G)$ is a subgroup of S_G, the group of permutations of G.

Solution. This follows immediately from Exercise 9.3.31.

38. Find $\mathrm{Aut}(\mathbb{Z}_6)$.

Hint. Any automorphism of $\mathbb{Z}_6$ must send 1 to another generator of $\mathbb{Z}_6$.

Solution. Any automorphism of $\mathbb{Z}_6$ must send 1 to another generator of $\mathbb{Z}_6$. Since the generators of $\mathbb{Z}_6$ are 1 and 5, the only possible automorphisms are determined by $1 \mapsto 1$ and $1 \mapsto 5$. Thus, $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

39. Find $\mathrm{Aut}(\mathbb{Z})$.

Solution. The automorphisms of a cyclic group must send a generator to a generator. The two possible automorphisms are $\mathrm{id} : \mathbb{Z} \to \mathbb{Z}$ defined by $\mathrm{id}(1) = 1$ and $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(1) = -1$. Therefore, $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

40. Find two nonisomorphic groups G and H such that $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Solution. $\mathrm{Aut}(\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

41. Let G be a group and $g \in G$. Define a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G. Such an automorphism is called an **inner automorphism**. The set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Solution. If $x, y \in G$, then $i_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$. To show that i_g is onto, let $x \in G$. Then $i_g(g^{-1}xg) = x$. If $i_g(x) = i_g(y)$, then $gxg^{-1} = gyg^{-1}$ or $x = y$. Consequently, the map is also one-to-one.

42. Prove that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

Solution. This follows immediately from Exercise 9.3.41.

43. What are the inner automorphisms of the quaternion group Q_8? Is $\mathrm{Inn}(G) = \mathrm{Aut}(G)$ in this case?

Solution. The distinct inner automorphisms of Q_8 are given by $\{i_1, i_I, i_J, i_K\}$. It follows that $\mathrm{Inn}(G) \neq \mathrm{Aut}(G)$, since the automorphism given by

$$\begin{aligned} 1 &\mapsto 1 \\ I &\mapsto J \\ J &\mapsto K \\ K &\mapsto I \end{aligned}$$

is not given by any i_g, $g \in Q_8$.

44. Let G be a group and $g \in G$. Define maps $\lambda_g : G \to G$ and $\rho_g : G \to G$ by $\lambda_g(x) = gx$ and $\rho_g(x) = xg^{-1}$. Show that $i_g = \rho_g \circ \lambda_g$ is an automorphism of G. The isomorphism $g \mapsto \rho_g$ is called the **right regular representation** of G.

Solution. Since $\rho_g \circ \lambda_g(x) = \rho_g(gx) = gxg^{-1} = i_g(x)$, this follows from Exercise 9.3.41.

45. Let G be the internal direct product of subgroups H and K. Show that the map $\phi : G \to H \times K$ defined by $\phi(g) = (h, k)$ for $g = hk$, where $h \in H$ and $k \in K$, is one-to-one and onto.

Hint. To show that ϕ is one-to-one, let $g_1 = h_1k_1$ and $g_2 = h_2k_2$ and consider $\phi(g_1) = \phi(g_2)$.

Solution. To show that ϕ is one-to-one, let $g_1 = h_1k_1$ and $g_2 = h_2k_2$. Then

$$\phi(h_1k_1) = \phi(g_1) = \phi(g_2) = \phi(h_2k_2).$$

Since $(h_1, k_1) = (h_2, k_2)$, it must be the case that $h_1 = h_2$ and $k_1 = k_2$. Thus, $g_1 = g_2$. If $(h, k) \in H \times K$, then $\phi(hk) = (h, k)$, and ϕ is onto.

46. Let G and H be isomorphic groups. If G has a subgroup of order n, prove that H must also have a subgroup of order n.

Solution. Let $\phi : G \to H$ be an isomorphism of groups. If K is a subgroup of G of order n, then $|\phi(K)| = n$ since ϕ is a bijection. We only need to show that $\phi(K)$is a subgroup of H. If $\phi(a), \phi(b) \in \phi(K)$, then $\phi(a)\phi(b) = \phi(ab)$ is also in $\phi(K)$. If e_G and e_H are the identities of G and H, respectively, then

$$e_H\phi(e_G) = \phi(e_G) = \phi(e_Ge_G) = \phi(e_G)\phi(e_G),$$

and $e_H = \phi(e_G)$ by cancellation. Finally, $[\phi(g)]^{-1} = \phi(g^{-1})$, since

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e_G) = e_H.$$

47. If $G \cong \overline{G}$ and $H \cong \overline{H}$, show that $G \times H \cong \overline{G} \times \overline{H}$.

Solution. If $\phi_1 : G \to \overline{G}$ and $\phi_2 : H \to \overline{H}$, the required isomorphism can be defined by $\phi(g, h) = (\phi_1(g), \phi_2(h))$.

48. Prove that $G \times H$ is isomorphic to $H \times G$.

Solution. Define an isomorphism $\phi : G \times H \to H \times G$ by $\phi(g, h) = (h, g)$.

49. Let $n_1, \ldots, n_k$ be positive integers. Show that

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Solution. Use Theorem 9.10 and mathematical induction.

50. Prove that $A \times B$ is abelian if and only if A and B are abelian.

Solution. If A and B are abelian, then for $(a_1, b_1), (a_2, b_2) \in A \times B$, we have $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2)(a_1, b_1)$. Conversely, if $A \times B$ is abelian, then A must be abelian, since $(a_1a_2, 1) = (a_1, 1)(a_2, 1) = (a_2, 1)(a_1, 1) = (a_2a_1, 1)$. Similarly, B must also be abelian.

51. If G is the internal direct product of $H_1, H_2, \ldots, H_n$, prove that G is isomorphic to $\prod_i H_i$.

Solution. Use Theorem 9.13 and mathematical induction.

52. Let H_1 and H_2 be subgroups of G_1 and G_2, respectively. Prove that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.

Solution. The identity $(1,1)$ is in $H_1 \times H_2$. If $(a_1, b_1), (a_2, b_2) \in H_1 \times H_2$, then $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$ is in $H_1 \times H_2$, since $a_1 a_2 \in H_1$ and $b_1 b_2 \in H_2$. Finally, $(a, b)^{-1} = (a^{-1}, b^{-1})$ is in $H_1 \times H_2$.

53. Let $m, n \in \mathbb{Z}$. Prove that $\langle m, n \rangle = \langle d \rangle$ if and only if $d = \gcd(m, n)$.

Solution. Show that $\langle m, n \rangle$ is a cyclic group of order $d = \gcd(m, n)$.

54. Let $m, n \in \mathbb{Z}$. Prove that $\langle m \rangle \cap \langle n \rangle = \langle l \rangle$ if and only if $l = \text{lcm}(m, n)$.

Solution. Show that $\langle m \rangle \cap \langle n \rangle$ is a cyclic group of order $l = \text{lcm}(m, n)$.

55. **Groups of order $2p$.** In this series of exercises we will classify all groups of order $2p$, where p is an odd prime.

(a) Assume G is a group of order $2p$, where p is an odd prime. If $a \in G$, show that a must have order 1, 2, p, or $2p$.

(b) Suppose that G has an element of order $2p$. Prove that G is isomorphic to $\mathbb{Z}_{2p}$. Hence, G is cyclic.

(c) Suppose that G does not contain an element of order $2p$. Show that G must contain an element of order p. *Hint*: Assume that G does not contain an element of order p.

(d) Suppose that G does not contain an element of order $2p$. Show that G must contain an element of order 2.

(e) Let P be a subgroup of G with order p and $y \in G$ have order 2. Show that $yP = Py$.

(f) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z. If y is an element of order 2, then $yz = z^k y$ for some $2 \leq k < p$.

(g) Suppose that G does not contain an element of order $2p$. Prove that G is not abelian.

(h) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z and y is an element of order 2. Show that we can list the elements of G as $\{z^i y^j \mid 0 \leq i < p, 0 \leq j < 2\}$.

(i) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z and y is an element of order 2. Prove that the product $(z^i y^j)(z^r y^s)$ can be expressed as a uniquely as $z^m y^n$ for some non negative integers m, n. Thus, conclude that there is only one possibility for a non-abelian group of order $2p$, it must therefore be the one we have seen already, the dihedral group.

Solution.

9.5 Sage Exercises

1. This exercise is about putting Cayley's Theorem into practice. First, read and study the theorem. Realize that this result by itself is primarily of theoretical interest, but with some more theory we could get into some subtler aspects of this (a subject known as "representation theory").

You should create these representations mostly with pencil-and-paper work, using Sage as a fancy calculator and assistant. You do not need to include all

these computations in your worksheet. Build the requested group representations and then include enough verifications in Sage to prove that that your representation correctly represents the group.

Begin by building a permutation representation of the quaternions, Q. There are eight elements in Q $(\pm 1, \pm I, \pm J, \pm K)$, so you will be constructing a subgroup of S_8. For each $g \in Q$ form the function T_g, defined as $T_g(x) = xg$. Notice that this definition is the "reverse" of that given in the text. This is because Sage composes permutations left-to-right, while your text composes right-to-left. To create the permutations T_g, the two-line version of writing permutations could be very useful as an intermediate step. You will probably want to "code" each element of Q with an integer in $\{1, 2, \ldots, 8\}$.

One such representation is included in Sage as `QuaternionGroup()` — your answer should look very similar, but perhaps not identical. Do not submit your answer for a representation of the quaternions, but I strongly suggest working this particular group representation until you are sure you have it right — the problems below might be very difficult otherwise. You can use Sage's `.is_isomorphic()` method to check if your representations are correct. However, do not use this as a substitute for the part of each question that asks you to investigate properties of your representation towards this end.

(a) Build the permutation representation of $\mathbb{Z}_2 \times \mathbb{Z}_4$ described in Cayley's Theorem. (Remember that this group is additive, while the theorem uses multiplicative notation.) Include the representation of *each* of the 8 elements in your submitted work. Then construct the permutation group as a subgroup of a full symmetric group that is generated by exactly two of the eight elements you have already constructed. Hint: which two elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ might you use to generate all of $\mathbb{Z}_2 \times \mathbb{Z}_4$? Use commands in Sage to investigate various properties of your permutation group, other than just `.list()`, to provide evidence that your subgroup is correct — include these in your submitted worksheet.

(b) Build a permutation representation of $U(24)$, the group of units mod 24. Again, list a representation of *each* element in your submitted work. Then construct the group as a subgroup of a full symmetric group created with three generators. To determine these three generators, you will likely need to understand $U(24)$ as an internal direct product. Use commands in Sage to investigate various properties of your group, other than just `.list()`, to provide evidence that your subgroup is correct — include these in your submitted worksheet.

Solution. The quaternions can be realized in Sage as a subgroup of a quaternion algebra. We show here how to create the permutation representation, though the directions suggest doing the bulk of the work by hand. The `.index()` method of a list is an easy way to map the group elements to integers (counting from zero), which may be specified as the domain of the permutations in a permutation group. We use lists of images to construct the permutations.

```
G.<I,J,K> = QuaternionAlgebra(-1,-1)
elts = [G(1), I, J, K, G(-1), -I, -J, -K]
S = SymmetricGroup(srange(len(elts)))
perms = [S([elts.index(x*g) for x in elts]) for g in elts]
H = S.subgroup(perms)
H.is_isomorphic(QuaternionGroup())
```

```
True
```

Now $\mathbb{Z}_2 \times \mathbb{Z}_4$.

```
G = AbelianGroup([2,4])
elts = G.list()
S = SymmetricGroup(srange(len(elts)))
perms = [S([elts.index(g*h) for h in elts]) for g in elts]
H = S.subgroup(perms)
```

Abelian.

```
H.is_abelian()
```

```
True
```

8 elements, with the expected orders.

```
[x.order() for x in H]
```

```
[1, 2, 4, 2, 4, 2, 4, 4]
```

More than one generator required.

```
H.is_cyclic()
```

```
False
```

Two generators is enough.

```
H.gens_small()
```

```
[(0,6)(1,7)(2,4)(3,5), (0,5,2,7)(1,6,3,4)]
```

You can try to check isomorphism, but the method for an `AbelianGroup` also expects an `AbelianGroup` in the argument, so should at least throw an error when given a permutation group. We document this bug here, in hopes it will be fixed soon, and we will notice.

```
G.is_isomorphic(H)
```

```
False
```

An unrelated example which makes the fault obvious.

```
K = AbelianGroup([17])
L = CyclicPermutationGroup(17)
K.is_isomorphic(L)
```

```
False
```

Reversing the order of the groups will not give a answer, but at least the result is not incorrect.

```
H.is_isomorphic(G)
```

```
Traceback (most recent call last):
...
TypeError: right must be a permutation group
```

2. Consider the symmetries of a 10-gon, D_{10} in your text, `DihedralGroup(10)` in Sage. Presume that the vertices of the 10-gon have been labeled 1 through 10 in order. Identify the permutation that is a 180 degree rotation and use it to generate a subgroup R of order 2. Then identify the permutation that is a 72 degree rotation, and any one of the ten permutations that are a reflection

of the 10-gon about a line. Use these latter two permutations to generate a subgroup S of order 10. Use Sage to verify that the full dihedral group is the internal direct product of the subgroups R and S by checking the conditions in the definition of an internal direct product.

We have a theorem which says that if a group is an internal direct product, then it is isomorphic to some external direct product. Understand that this does not mean that you can use the converse in this problem. In other words, establishing an isomorphism of G with an external direct product *does not prove* that G is an internal direct product.

Solution.

```
D = DihedralGroup(10)
# 2nd and 5th powers of base rotation
rotate = D("(1,2,3,4,5,6,7,8,9,10)")
oneeighty = rotate^5
seventwenty = rotate^2
# reflect about 2-7 axis
reflect = D("(1,3)(4,10)(5,9)(6,8)")
R = D.subgroup([oneeighty])
S = D.subgroup([seventwenty, reflect])
```

Intersection is trivial. As a bonus, Sage knows the intersection is also a subgroup.

```
R.intersection(S)
```

```
Permutation Group with generators [()]
```

Pairs commute.

```
all([r*s == s*r for r in R for s in S])
```

```
True
```

All 20 elements of the group arise as products.

```
len([r*s for r in R for s in S])
```

```
20
```

Now that we know D_{10} is the internal direct product of R and S, we can verify the conclusion of Theorem 9.27.

```
D.is_isomorphic(direct_product_permgroups([R,S]))
```

```
True
```

The 180-degree rotation is the sole non-identity element of the center, which explains why the pairs all commute. The subgroup S is isomorphic to the dihedral group D_5, which can be seen for this particular choice of a reflection by inscribing a pentagon at the odd-numbered vertices.

```
S.is_isomorphic(DihedralGroup(5))
```

```
True
```

Chapter 10

Normal Subgroups and Factor Groups

10.3 Exercises

1. For each of the following groups G, determine whether H is a normal subgroup of G. If H is a normal subgroup, write out a Cayley table for the factor group G/H.

(a) $G = S_4$ and $H = A_4$

(b) $G = A_5$ and $H = \{(1), (123), (132)\}$

(c) $G = S_4$ and $H = D_4$

(d) $G = Q_8$ and $H = \{1, -1, I, -I\}$

(e) $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$

Hint. (a)

	A_4	$(12)A_4$
A_4	A_4	$(12)A_4$
$(12)A_4$	$(12)A_4$	A_4

(c) D_4 is not normal in S_4.

Solution.

(a)

	A_4	$(12)A_4$
A_4	A_4	$(12)A_4$
$(12)A_4$	$(12)A_4$	A_4

(b) H is not a normal subgroup.

(c) D_4 is not normal in S_4.

(d)

	H	jH
H	H	jH
jH	jH	H

(e)

	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$0+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

2. Find all the subgroups of D_4. Which subgroups are normal? What are all the factor groups of D_4 up to isomorphism?

Solution. The group $D_4 = \langle r, s\rangle$, where $r^4 = 1$, $s^2 = 1$, and $srs = r^{-1}$, has the following subgroups,

$$\begin{aligned}
\langle 1\rangle &= \{1\}\\
\langle s\rangle &= \{1, s\}\\
\langle r^2\rangle &= \{1, r^2\}\\
\langle sr\rangle &= \{1, sr\}\\
\langle sr^2\rangle &= \{1, sr^2\}\\
\langle sr^3\rangle &= \{1, sr^3\}\\
\langle r\rangle &= \{1, r, r^2, r^3\}\\
\langle s, r^2\rangle &= \{1, s, r^2, sr^2\}\\
\langle sr, r^2\rangle &= \{1, sr, r^2, sr^3\}\\
D_4 &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}
\end{aligned}$$

The subgroups $\langle r\rangle$, $\langle s, r^2\rangle$, and $\langle sr, r^2\rangle$ are normal since each of these subgroups has index 2. The quotient groups $D_4/\langle r\rangle$, $D_4\langle s, r^2\rangle$, and $D_4\langle sr, r^2\rangle$ are isomorphic to $\mathbb{Z}_2$. The only subgroup of order 2 that is $\langle r^2\rangle$. Since the order of each element in $D_4/\langle r^2\rangle$ is 2, this quotient group must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Find all the subgroups of the quaternion group, Q_8. Which subgroups are normal? What are all the factor groups of Q_8 up to isomorphism?

Solution. The proper subgroups of Q_8 are $\{1\}$, $\{\pm 1\}$, $\{\pm 1, \pm I\}$, $\{\pm 1, \pm J\}$, and $\{\pm 1, \pm K\}$. Every subgroup is a normal subgroup. The nontrivial factor groups of Q_8 are isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Let T be the group of nonsingular upper triangular 2×2 matrices with entries in $\mathbb{R}$; that is, matrices of the form

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

where a, b, $c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

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

where $x \in \mathbb{R}$.

(a) Show that U is a subgroup of T.

(b) Prove that U is abelian.

(c) Prove that U is normal in T.

(d) Show that T/U is abelian.

(e) Is T normal in $GL_2(\mathbb{R})$?

Solution.

(a) If

$$X = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad Y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix},$$

then

$$Y^{-1} = \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix}.$$

So

$$XY^{-1} = \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix},$$

and U is a subgroup of T.

(b)

$$XY = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = YX$$

(c) If

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

is in T, then

$$A^{-1} = \begin{pmatrix} 1/a & -ba/c \\ 0 & 1/c \end{pmatrix}.$$

So

$$A^{-1}XA = \begin{pmatrix} 1 & cx/a \\ 0 & 1 \end{pmatrix}$$

is in U, and U is normal in T.

(d) Follows by a direct computation.

(e) No.

5. Show that the intersection of two normal subgroups is a normal subgroup.

Solution. If N_1 and N_2 are normal in G and $x \in N_1 \cap N_2$, then $x \in N_1$ and $x \in N_2$. Since these subgroups are both normal, $gxg^{-1} \in N_1$ and $gxg^{-1} \in N_2$ for all $g \in G$. Thus, $gxg^{-1} \in N_1 \cap N_2$ for all $g \in G$.

6. If G is abelian, prove that G/H must also be abelian.

Solution. If $a+H, b+H \in G/H$, then $(a+H)(b+H) = ab+H = ba+H = (b+H)(a+H)$.

7. Prove or disprove: If H is a normal subgroup of G such that H and G/H are abelian, then G is abelian.

Solution. False. Let $G = S_3$ and $H = \{(1), (123), (132)\}$.

8. If G is cyclic, prove that G/H must also be cyclic.

Hint. If $a \in G$ is a generator for G, then aH is a generator for G/H.

Solution. If $a \in G$ is a generator for G, then aH is a generator for G/H.

9. Prove or disprove: If H and G/H are cyclic, then G is cyclic.

Solution. False. Let $G = S_3$ and $H = \{(1), (123), (132)\}$.

10. Let H be a subgroup of index 2 of a group G. Prove that H must be a normal subgroup of G. Conclude that S_n is not simple for $n \geq 3$.

Solution. If $[G : H] = 2$, then H has two distinct left cosets in G, say H and aH, where $a \notin H$. Since the two right cosets H and Ha also partition G, $aH = Ha$. Consequently, H is normal in G. Since $[S_n : A_n] = 2$, S_n cannot be simple.

11. If a group G has exactly one subgroup H of order k, prove that H is normal in G.

Hint. For any $g \in G$, show that the map $i_g : G \to G$ defined by $i_g : x \mapsto gxg^{-1}$ is an isomorphism of G with itself. Then consider $i_g(H)$.

Solution. For any $g \in G$, the map $i_g : G \to G$ defined by $i_g : x \mapsto gxg^{-1}$is an isomorphism of G with itself since

$$i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y).$$

for $x, y \in G$. By Theorem 9.6, $i_g(H) = gHg^{-1}$ is a subgroup of order k for all $g \in G$. Thus, $H = gHg^{-1}$ for all $g \in G$ and H is normal in G.

12. Define the **centralizer** of an element g in a group G to be the set

$$C(g) = \{x \in G : xg = gx\}.$$

Show that $C(g)$ is a subgroup of G. If g generates a normal subgroup of G, prove that $C(g)$ is normal in G.

Hint. Suppose that $\langle g \rangle$ is normal in G and let y be an arbitrary element of G. If $x \in C(g)$, we must show that yxy^{-1} is also in $C(g)$. Show that $(yxy^{-1})g = g(yxy^{-1})$.

Solution. Since $eg = ge$ for all $g \in G$, the identity is in $C(g)$. If $x, y \in C(g)$, then $xyg = xgy = gxy$. Thus, $xy \in C(g)$. If $xg = gx$, then $x^{-1}g = gx^{-1}$. Consequently, $x^{-1} \in C(g)$. Therefore, $C(g)$ is a subgroup of G. Suppose that $\langle g \rangle$ is normal in G and let y be an arbitrary element of G. If $x \in C(g)$, we must show that yxy^{-1} is also in $C(g)$. This follows from the fact that

$$(yxy^{-1})g = (yxy^{-1})gyy^{-1} = yx(y^{-1}gy)y^{-1} = y(y^{-1}gy)xy^{-1} = g(yxy^{-1}).$$

13. Recall that the **center** of a group G is the set

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}.$$

(a) Calculate the center of S_3.

(b) Calculate the center of $GL_2(\mathbb{R})$.

(c) Show that the center of any group G is a normal subgroup of G.

(d) If $G/Z(G)$ is cyclic, show that G is abelian.

Solution.

(a) (1)

(b) $Z(GL_2(\mathbb{R})) = \alpha I$, where $\alpha \in \mathbb{R}$ and I is the 2×2 identity matrix.

(c) By Exercise 3.4.48 in Chapter 3, $Z(G)$ is a subgroup of G. If $g \in G$ and $h \in Z(G)$, then $gh = hg$, or $h = ghg^{-1}$. Therefore, $ghg^{-1} \in Z(G)$ for all $g \in G$ and all $h \in Z(G)$.

(d) If $G/Z(G)$ is cyclic, there exists an $a \in G$ such that every element in $G/Z(G)$ is a power of $aZ(G)$. If $g, h \in G$, then $g = a^m z$ and $h = a^n z'$ for some $z, z' \in Z(G)$. Thus, $gh = a^m z a^n z' a^m a^n zz' = a^n a^m z' z = a^n z' a^m z = hg$.

14. Let G be a group and let $G' = \langle aba^{-1}b^{-1} \rangle$; that is, G' is the subgroup of all finite products of elements in G of the form $aba^{-1}b^{-1}$. The subgroup G' is called the **commutator subgroup** of G.

(a) Show that G' is a normal subgroup of G.

(b) Let N be a normal subgroup of G. Prove that G/N is abelian if and only if N contains the commutator subgroup of G.

Hint. (a) Let $g \in G$ and $h \in G'$. If $h = aba^{-1}b^{-1}$, then

$$\begin{aligned} ghg^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

We also need to show that if $h = h_1 \cdots h_n$ with $h_i = a_i b_i a_i^{-1} b_i^{-1}$, then ghg^{-1} is a product of elements of the same type. However, $ghg^{-1} = gh_1 \cdots h_n g^{-1} = (gh_1 g^{-1})(gh_2 g^{-1}) \cdots (gh_n g^{-1})$.

Solution.

(a) Let $g \in G$ and $h \in G'$. If $h = aba^{-1}b^{-1}$, then

$$\begin{aligned} ghg^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

We also need to show that if $h = h_1 \cdots h_n$ with $h_i = a_i b_i a_i^{-1} b_i^{-1}$, then ghg^{-1} is a product of elements of the same type. However, $ghg^{-1} = gh_1 \cdots h_n g^{-1} = (gh_1 g^{-1})(gh_2 g^{-1}) \cdots (gh_n g^{-1})$.

(b) If G/N is abelian and $g, h \in G$, then $ghN = gNhN = hNgN = hgN$. Hence, $gh = hgn$ for some $n \in N$. Consequently, $ghg^{-1}h^{-1} = n \in N$. Conversely, if $G' \subset N$ and $gN, hN \in G/N$, then $gNhN = ghN$ and $hNgN = hgN$. But $g^{-1}h^{-1}gh \in N$, so $hg(g^{-1}h^{-1}gh) = gh \in hgN$. Hence, $ghN = hgN$.

10.5 Sage Exercises

1. Build every subgroup of the alternating group on 5 symbols, A_5, and check that each is not a normal subgroup (except for the two trivial cases). This command might take a couple seconds to run. Compare this with the time needed to run the `.is_simple()` method and realize that there is a significant amount of theory and cleverness brought to bear in speeding up commands like this. (It is possible that your Sage installation lacks GAP's "Table of Marks" library and you will be unable to compute the list of subgroups.)

Solution. The requisite GAP library was missing from Sage 6.3 and the `.subgroups()` command below would fail. The problem was fixed for Sage 6.4, but seems to be missing from Sage 6.7.

```
A = AlternatingGroup(5)
sg = A.subgroups()
[H.order() for H in sg if H.is_normal(A)]
```

```
[1, 60]
```

2. Consider the quotient group of the group of symmetries of an 8-gon, formed with the cyclic subgroup of order 4 generated by a quarter-turn. Use the `coset_product` function to determine the Cayley table for this quotient group. Use the number of each coset, as produced by the `.cosets()` method as names for the elements of the quotient group. You will need to build the table "by hand" as there is no easy way to have Sage's Cayley table command do this one for you. You can build a table in the Sage Notebook pop-up editor (shift-click on a blue line) or you might read the documentation of the `html.table()` method.

Solution.

```
def coset_product(i, j, C):
    p = C[i][0]*C[j][0]
    c = [k for k in srange(len(C)) if p in C[k]]
    return c[0]
```

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
S.is_normal(G)
```

```
True
```

The quotient group has order 4 and is not cyclic.

```
C = G.cosets(S)
[[coset_product(i, j, C) for j in srange(4)] for i in
    srange(4)]
```

```
[[0, 1, 2, 3],
 [1, 0, 3, 2],
 [2, 3, 0, 1],
 [3, 2, 1, 0]]
```

3. Consider the cyclic subgroup of order 4 in the symmetries of an 8-gon. Verify that the subgroup is normal by first building the raw left and right cosets (without using the `.cosets()` method) and then checking their equality in Sage, all with a single command that employs sorting with the `sorted()` command.

Solution.

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
all([sorted([g*s for s in S]) == sorted([s*g for s in S])
    for g in G])
```

```
True
```

4. Again, use the same cyclic subgroup of order 4 in the group of symmetries of an 8-gon. Check that the subgroup is normal by using part (2) of

Theorem 10.3. Construct a one-line command that does the complete check and returns `True`. Maybe sort the elements of the subgroup `S` first, then slowly build up the necessary lists, commands, and conditions in steps. Notice that this check does not require ever building the cosets.

Solution.

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
all([g*s*g^-1 in S for s in S for g in G])
```

```
True
```

5. Repeat the demonstration from the previous subsection that for the symmetries of a tetrahedron, a cyclic subgroup of order 3 results in an undefined coset multiplication. Above, the default setting for the `.cosets()` method builds right cosets — but in this problem, work instead with left cosets. You need to choose two cosets to multiply, and then demonstrate two choices for representatives that lead to different results for the product of the cosets.

Solution. A product of the third and fourth cosets is not defined: the product of the first and second elements is in the fourth coset, while the product of the second and third elements is in the first coset. Of course, there are other such demonstrations.

```
G = AlternatingGroup(4)
face_turn = G("(1,2,3)")
S = G.subgroup([face_turn])
C = G.cosets(S, side='left')
C[2][0]*C[3][1] in C[3], C[2][1]*C[3][2] in C[0]
```

```
(True, True)
```

6. Construct some dihedral groups of order $2n$ (i.e. symmetries of an n-gon, D_n in the text, `DihedralGroup(n)` in Sage). Maybe all of them for $3 \leq n \leq 100$. For each dihedral group, construct a list of the orders of each of the normal subgroups (so use `.normal_subgroups()`). You may need to wait ten or twenty seconds for this to finish - be patient. Observe enough examples to hypothesize a pattern to your observations, check your hypothesis against each of your examples and then state your hypothesis clearly.

Can you predict how many normal subgroups there are in the dihedral group D_{470448} without using Sage to build all the normal subgroups? Can you *describe* all of the normal subgroups of a dihedral group in a way that would let us predict all of the normal subgroups of D_{470448} without using Sage?

Solution.

```
for n in [27, 28, 53, 54]:
    G = DihedralGroup(n)
    nsg = G.normal_subgroups()
    n, [H.order() for H in nsg]
```

```
(27, [1, 3, 9, 27, 54])
(28, [1, 2, 4, 7, 14, 28, 28, 28, 56])
(53, [1, 53, 106])
(54, [1, 2, 3, 6, 9, 18, 27, 54, 54, 54, 108])
```

There is one normal subgroup for each divisor of n, with the exception that if n is even, then there are three normal subgroups of order n. And, of course the whole group, of order $2n$, is normal.

The majority of these normal subgroups are the subgroups of the cyclic group of just rotations of the n-gon. Thus, exactly one for each divisor of n. Their normality can be explained with part (3) of Theorem 10.3. A reflection, followed by a rotation, followed by the inverse of a reflection, will reflect the n-gon twice, so the product is therefore not a reflection, and hence is a rotation. Since the conjugation of a subgroup will create a subgroup of the same order, and there is only one subgroup of this order within the cyclic group of rotations, we get the necessary equality.

How about the two "extra" subgroups of order n. As index 2 subgroups, their normality is easy to determine. Inscribe an $\frac{n}{2}$-gon and take the rotations which are symmetries of this figure. Combine these with all of the reflections which fix a pair of opposite vertices of the n-gon. This forms one index 2 subgroup. For the second group, take the same rotations, but now combine with the reflections which do not fix any vertices.

```
factor(470448)
```

```
2^4 * 3^5 * 11^2
```

So there are $5 \cdot 6 \cdot 3 = 90$ divisors, plus the whole group and the two extra for a total of 93 normal subgroups.

Chapter 11

Homomorphisms

11.3 Exercises

1. Prove that $\det(AB) = \det(A)\det(B)$ for $A, B \in GL_2(\mathbb{R})$. This shows that the determinant is a homomorphism from $GL_2(\mathbb{R})$ to $\mathbb{R}^*$.

Solution. This is a straighforward computation. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

then

$$AB = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}.$$

Hence,

$$\begin{aligned} \det(A)\det(B) &= (ad - bc)(xw - yz) \\ &= (ax + bz)(cy + dw) - (ay + bw)(cx + dz) \\ &= \det(AB). \end{aligned}$$

2. Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

(a) $\phi : \mathbb{R}^* \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : \mathbb{R} \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

where $\mathbb{M}_2(\mathbb{R})$ is the additive group of 2×2 matrices with entries in $\mathbb{R}$.

Hint. (a) is a homomorphism with kernel $\{1\}$; (c) is not a homomorphism.

Solution.

(a) A homomorphism with kernel $\{1\}$.

(b) A homomorphism with kernel $\{0\}$.

(c) Not a homomorphism.

(d) A homomorphism with kernel $SL_2(\mathbb{R})$.

(e) A homomorphism with a kernel consisting of all the lower triangular matrices.

3. Let A be an $m \times n$ matrix. Show that matrix multiplication, $x \mapsto Ax$, defines a homomorphism $\phi : \mathbb{R}^n \to \mathbb{R}^m$.

Solution.

$$\begin{aligned}
A(x+y) &= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \left[\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \right] \\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \\
&= \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ a_{21}x_1 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} + \begin{pmatrix} a_{11}y_1 + \cdots + a_{1n}y_n \\ a_{21}y_1 + \cdots + a_{2n}y_n \\ \vdots \\ a_{m1}y_1 + \cdots + a_{mn}y_n \end{pmatrix} \\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\
&= Ax + Ay
\end{aligned}$$

4. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be given by $\phi(n) = 7n$. Prove that ϕ is a group homomorphism. Find the kernel and the image of ϕ.

Hint. Since $\phi(m+n) = 7(m+n) = 7m + 7n = \phi(m) + \phi(n)$, ϕ is a homomorphism.

Solution. Since $\phi(m+n) = 7(m+n) = 7m + 7n = \phi(m) + \phi(n)$, ϕ is a homomorphism. The kernel of ϕ is $\{0\}$ and the image of ϕ is $7\mathbb{Z}$.

5. Describe all of the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

Hint. For any homomorphism $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, the kernel of ϕ must be a subgroup of $\mathbb{Z}_{24}$ and the image of ϕ must be a subgroup of $\mathbb{Z}_{18}$. Now use the fact that a generator must map to a generator.

Solution. For any homomorphism $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, the kernel of ϕ must be a subgroup of $\mathbb{Z}_{24}$ and the image of ϕ must be a subgroup of $\mathbb{Z}_{18}$. Now use the fact that a generator must map to a generator.

6. Describe all of the homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$.

Solution. The image of any homomorphism must be a subgroup of $\mathbb{Z}_{12} \cong \mathbb{Z}/12\mathbb{Z}$; thus, the only homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}_{12}$ are:

$$\begin{aligned} n &\mapsto 12n + \mathbb{Z}/12\mathbb{Z}, \\ n &\mapsto 6n + \mathbb{Z}/12\mathbb{Z}, \\ n &\mapsto 4n + \mathbb{Z}/12\mathbb{Z}, \\ n &\mapsto 3n + \mathbb{Z}/12\mathbb{Z}, \\ n &\mapsto 2n + \mathbb{Z}/12\mathbb{Z}, \\ n &\mapsto n + \mathbb{Z}/12\mathbb{Z}. \end{aligned}$$

7. In the group $\mathbb{Z}_{24}$, let $H = \langle 4 \rangle$ and $N = \langle 6 \rangle$.

(a) List the elements in HN (we usually write $H + N$ for these additive groups) and $H \cap N$.

(b) List the cosets in HN/N, showing the elements in each coset.

(c) List the cosets in $H/(H \cap N)$, showing the elements in each coset.

(d) Give the correspondence between HN/N and $H/(H \cap N)$ described in the proof of the Second Isomorphism Theorem.

Solution.

(a) $H + N = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$. $H \cap N = \{0, 12\}$.

(b)

$$\begin{aligned} N &= \{0, 6, 12, 18\} \\ 2 + N &= \{2, 8, 14, 20\} \\ 4 + N &= \{4, 10, 16, 22\} \end{aligned}$$

(c)

$$\begin{aligned} H \cap N &= \{0, 12\} \\ 4 + H \cap N &= \{4, 16\} \\ 8 + H \cap N &= \{8, 20\} \end{aligned}$$

(d)

$$\begin{aligned} H \cap N &\mapsto N \\ 4 + H \cap N &\mapsto 4 + N \\ 8 + H \cap N &\mapsto 2 + N \end{aligned}$$

8. If G is an abelian group and $n \in \mathbb{N}$, show that $\phi : G \to G$ defined by $g \mapsto g^n$ is a group homomorphism.

Solution. If $\phi(g) = g^n$, then $\phi(gh) = (gh)^n$, which is equal to $g^n h^n = \phi(g)\phi(h)$, since G is abelian.

9. If $\phi : G \to H$ is a group homomorphism and G is abelian, prove that $\phi(G)$ is also abelian.

Hint. Let $a, b \in G$. Then $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

Solution. Let $a, b \in G$. Then $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

10. If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.

Solution. If $h \in \phi(G)$, then $h = \phi(g^n) = [\phi(g)]^n$; hence, $\phi(g)$ is a generator for $\phi(G)$.

11. Show that a homomorphism defined on a cyclic group is completely determined by its action on the generator of the group.

Solution. If G is cyclic with generator a and $b \in G$, then we can write b as a power of a, say $a^n = b$. Any group homomorphism $\phi : G \to H$ is determined by its action on the generator, since $\phi(b) = \phi(a^n) = [\phi(a)]^n$.

12. If a group G has exactly one subgroup H of order k, prove that H is normal in G.

Solution. Let H be a subgroup of order k. For any $g \in G$, we claim that the map $i_g : H \to G$ defined by $i_g(h) = ghg^{-1}$ is an injective group homomorphism. Since

$$i_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = i_g(h_1)i_g(h_2),$$

we have a group homomorphism. If $gh_1g^{-1} = i_g(h_1) = i_g(h_2) = gh_2g^{-1}$, we have $h_1 = h_2$ and the map is injective. By Proposition 11.4, $i_g(H) = gHg^{-1}$ is a subgroup of order k for all $g \in G$. Since there is only one such subgroup, $H = gHg^{-1}$. Compare this to the solution of Exercise 10.3.11

13. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

Solution. The two groups are not isomorphic. Every element in $\mathbb{Q}$ has either infinite order or has order one. However, $1/2 + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has order two.

14. Let G be a finite group and N a normal subgroup of G. If H is a subgroup of G/N, prove that $\phi^{-1}(H)$ is a subgroup in G of order $|H| \cdot |N|$, where $\phi : G \to G/N$ is the canonical homomorphism.

Solution. By the Correspondence Theorem, $H = K/N$ and $\phi^{-1}(H) = K$ for some subgroup K, where $N \subset K \subset G$. By Lagrange's Theorem, $|K| = [K : N] \cdot |N| = |H| \cdot |N|$.

15. Let G_1 and G_2 be groups, and let H_1 and H_2 be normal subgroups of G_1 and G_2 respectively. Let $\phi : G_1 \to G_2$ be a homomorphism. Show that ϕ induces a natural homomorphism $\overline{\phi} : (G_1/H_1) \to (G_2/H_2)$ if $\phi(H_1) \subset H_2$.

Solution. Define $\overline{\phi} : (G_1/H_1) \to (G_2/H_2)$ by $\overline{\phi}(gH_1) = \phi(g)H_2$. To show that this map is well-defined, let $gH_1 = g'H_1$. Then $g = g'h_1$ for some $h_1 \in H_1$ and

$$\overline{\phi}(gH_1) = \phi(g)H_2 = \phi(g'h_1)H_2 = \phi(g')\phi(h_1)H_2 = \phi(g')H_2 = \overline{\phi}(gH_1).$$

If $gH_1, g'H_1 \in G/H_1$, then

$$\overline{\phi}(gH_1)\overline{\phi}(g'H_1) = \phi(g)H_2\phi(g')H_2 = \phi(g)\phi(g')H_2 = \phi(gg')H_2 = \overline{\phi}[(gH_1)(g'H_1)],$$

and $\overline{\phi}$ is a homomorphism.

16. If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \times G/K$.

Solution. Let $\phi_1 : G \to G/H$ and $\phi_2 : G \to G/K$ be the natural maps. Define a group homomorphism

$$\phi : G \to G/H \times G/K$$

by $\phi(g) = (\phi_1(g), \phi_2(g))$. The kernel of this map consists of those elements common to both H and K, but $H \cap K = \{e\}$. Thus, ϕ is one-to-one. Therefore, G is isomorphic to a subgroup of $G/H \times G/K$.

17. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism. Let H_1 be a normal subgroup of G_1 and suppose that $\phi(H_1) = H_2$. Prove or disprove that $G_1/H_1 \cong G_2/H_2$.

Hint. Find a counterexample.

Solution. Let $G_1 = \mathbb{Z} \times \mathbb{Z}$ and $G_2 = \mathbb{Z}$ and define a surjective group homomorphism by $\phi(m, n) = m$. If we let $H_1 = \mathbb{Z} \times \{0\}$, then $\phi(H_1) = \mathbb{Z} = H_2$. Since $G_1/H_1 \cong \mathbb{Z}$ and G_2/H_2 is the trivial subgroup, the two quotient groups are not isomorphic.

18. Let $\phi : G \to H$ be a group homomorphism. Show that ϕ is one-to-one if and only if $\phi^{-1}(e) = \{e\}$.

Solution. If ϕ is one-to-one, let $g \in \ker \phi$. Then $\phi(g) = e = \phi(e)$. So $g = e$. Conversely, let $\ker \phi = \{e\}$. If $\phi(a) = \phi(b)$, then $\phi(a)[\phi(b)^{-1}] = \phi(ab^{-1}) = \phi(e) = e$. So $ab^{-1} = e$ or $a = b$.

19. Given a homomorphism $\phi : G \to H$ define a relation $\sim$ on G by $a \sim b$ if $\phi(a) = \phi(b)$ for $a, b \in G$. Show this relation is an equivalence relation and describe the equivalence classes.

Solution. It is straightforward to show that the relation is reflexive, symmetric, and transitive. The equivalence classes are the inverse images of each $h \in H$.

11.6 Sage Exercises

1. An automorphism is an isomorphism between a group and itself. The identity function $(x \mapsto x)$ is always an isomorphism, which we consider trivial. Use Sage to construct a nontrivial automorphism of the cyclic group of order 12. Check that the mapping is both onto and one-to-one by computing the image and kernel and performing the proper tests on these subgroups. Now construct all of the possible automorphisms of the cyclic group of order 12 without any duplicates.

Solution. Take the one generator of the domain and map it to the possible generators of the (necessary) image. Notice how Sage reports the mapping as an "endomorphism."

```
C12 = CyclicPermutationGroup(12)
x = C12.gen(0)
autos = [PermutationGroupMorphism(C12, C12, x^k) for k in
    [1, 5, 7, 11]]
autos[2]
```

```
Permutation group endomorphism of Cyclic group of order 12 as
    a permutation group
Defn: [(1,2,3,4,5,6,7,8,9,10,11,12)] ->
    [(1,8,3,10,5,12,7,2,9,4,11,6)]
```

```
[(phi.kernel().order(), phi.image(C12).order()) for phi in
    autos]
```

```
[(1, 12), (1, 12), (1, 12), (1, 12)]
```

2. The four homomorphisms created by the direct product construction are each an example of a more general construction of homomorphisms involving groups G, H and $G \times H$. By using the same groups as in the example in the previous subsection, see if you can discover and describe these constructions with exact definitions of the four homomorphisms in general.

Your tools for investigating a Sage group homomorphism are limited, you might take each generator of the domain and see what its image is. Here is an example of the type of computation you might do repeatedly. We'll investigate the second homomorphism. The domain is the dihedral group, and we will compute the image of the first generator.

```
G = CyclicPermutationGroup(3)
H = DihedralGroup(4)
results = G.direct_product(H)
phi = results[2]
H.gens()
```

```
[(1,2,3,4), (1,4)(2,3)]
```

```
a = H.gen(0); a
```

```
(1,2,3,4)
```

```
phi(a)
```

```
(4,5,6,7)
```

Solution. Sage returns a permutation group formed by advancing the symbols used in the second group, so there is no overlap in the two symbol sets. Then each element of the direct product can be seen to act independently on the two symbol sets. The first homomorphism embeds the first group into the direct product. The second homomorphism behaves similarly with respect to the second group. The third (respectively fourth) homomorphism projects the direct product onto the first (respectively second) group.

```
for i in srange(1,5):
    print(results[i])
```

```
Permutation group morphism:
  From: Cyclic group of order 3 as a permutation group
  To:   Permutation Group with generators [(4,5,6,7),
      (4,7)(5,6), (1,2,3)]
  Defn: Embedding( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 1 )
Permutation group morphism:
  From: Dihedral group of order 8 as a permutation group
  To:   Permutation Group with generators [(4,5,6,7),
      (4,7)(5,6), (1,2,3)]
  Defn: Embedding( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 2 )
Permutation group morphism:
  From: Permutation Group with generators [(4,5,6,7),
      (4,7)(5,6), (1,2,3)]
```

```
  To:   Cyclic group of order 3 as a permutation group
  Defn: Projection( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 1 )
Permutation group morphism:
  From: Permutation Group with generators [(4,5,6,7),
      (4,7)(5,6), (1,2,3)]
  To:   Dihedral group of order 8 as a permutation group
  Defn: Projection( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 2 )
```

3. Consider two permutation groups. The first is the subgroup of S_7 generated by $(1,2,3)$ and $(4,5,6,7)$. The second is a subgroup of S_{12} generated by $(1,2,3)(4,5,6)(7,8,9)(10,11,12)$ and $(1,10,7,4)(2,11,8,5)(3,12,9,6)$. Build these two groups and use the proper Sage command to see that they are isomorphic. Then construct a homomorphism between these two groups that is an isomorphism and include enough details to verify that the mapping is really an isomorphism.

Solution.

```
S7 = SymmetricGroup(7)
S12 = SymmetricGroup(12)
a1 = S7("(1,2,3)")
a2 = S7("(4,5,6,7)")
b1 = S12("(1,2,3)(4,5,6)(7,8,9)(10,11,12)")
b2 = S12("(1,10,7,4)(2,11,8,5)(3,12,9,6)")
A = S7.subgroup([a1, a2])
B = S12.subgroup([b1, b2])
A.is_isomorphic(B)
```

```
True
```

Sage has its own ideas about what order to use when listing the generators. So we will list the images of the isomorphism accordingly.

```
A.gens()
```

```
[(4,5,6,7), (1,2,3)]
```

```
phi = PermutationGroupMorphism(A, B, [b2, b1])
phi.kernel().order() == 1, phi.image(A).order() == B.order()
```

```
(True, True)
```

It would be nice to test equality of the image and the codomain as groups, but this is not behaving properly now, as the result below is clearly wrong. Once fixed, our automated testing should notice.

```
phi.image(A) == B
```

```
False
```

4. The second paragraph of this chapter informally describes a homomorphism from S_n to $\mathbb{Z}_2$, where the even permutations all map to one of the elements and the odd permutations all map to the other element. Replace S_n by S_6 and replace $\mathbb{Z}_2$ by the permutation version of the cyclic subgroup of order 2, and construct a nontrivial homomorphism between these two groups. Evaluate your homomorphism with enough even and odd permutations to be

convinced that it is correct. Then construct the kernel and verify that it is the group you expect.

Hints: First, decide which elements of the group of order 2 will be associated with even permutations and which will be associated with odd permutations. Then examine the generators of S_6 to help decide just how to build the homomorphism.

Solution. The identity permutation should map to the identity permutation, hence all even permutations should map to the identity permutation. And thus, odd elements should map to the "other" element of the codomain, which will be the generator of the group. Notice that Sage uses two odd permutations as generators of S_6.

```
S6 = SymmetricGroup(6)
Z2 = CyclicPermutationGroup(2)
gen = Z2.gen(0)
S6.gens(), gen
```

```
([(1,2,3,4,5,6), (1,2)], (1,2))
```

```
phi = PermutationGroupMorphism(S6, Z2, [gen, gen])
phi.kernel().order() == S6.order()/2
```

```
True
```

```
phi.kernel().is_isomorphic(AlternatingGroup(6))
```

```
True
```

This homomorphism is basically the "sign" of a permutation, as we can check.

```
all([sigma.sign() == (-2*phi(sigma).order()+3) for sigma in
    S6])
```

```
True
```

5. The dihedral group D_{20} has several normal subgroups, as seen below. Each of these is the kernel of a homomorphism with D_{20} as the domain. For each normal subgroup of D_{20} construct a homomorphism from D_{20} to D_{20} that has the normal subgroup as the kernel. Include in your work verifications that you are creating the desired kernels. There is a pattern to many of these, but the three of order 20 will be a challenge.

```
G = DihedralGroup(20)
[H.order() for H in G.normal_subgroups()]
```

```
[1, 2, 4, 5, 10, 20, 20, 20, 40]
```

Solution. The particulars of the following come from a solution by Thomas Gagne. The list of `images` is the key. At the two extremes are the the identity isomorphism and the trivial homomorphism. The element `r` is a generator for the cyclic subgroup of rotations and `s` is a reflection about an axis joining midpoints of opposite sides of the n-gon. (Recall the group presentation given in Theorem 5.23.)

```
D = DihedralGroup(20)
r, s = D.gen(0), D.gen(1)
images =[(r,s), (r^2,s), (r^4,s), (r^5,s), (r^10,s),
         (r^10,s^2),(r*s,r*s),(r^20,s),(r^20,s^2)]
```

```
maps = [PermutationGroupMorphism(D, D, im) for im in images]
kernels = [phi.kernel() for phi in maps]
normals = D.normal_subgroups()
[g[0] == g[1] for g in zip(normals, kernels)]
```

```
[True, True, True, True, True, True, True, True, True]
```

Chapter 12

Matrix Groups and Symmetry

12.3 Exercises

1. Prove the identity

$$\langle \mathbf{x}, \mathbf{y} \rangle = \frac{1}{2} \left[\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right].$$

Hint.

$$\begin{aligned} \frac{1}{2} \left[\|\mathbf{x}+\mathbf{y}\|^2 + \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] &= \frac{1}{2} \left[\langle x+y, x+y \rangle - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \frac{1}{2} \left[\|\mathbf{x}\|^2 + 2\langle x, y \rangle + \|\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \langle \mathbf{x}, \mathbf{y} \rangle. \end{aligned}$$

Solution.

$$\begin{aligned} \frac{1}{2} \left[\|\mathbf{x}+\mathbf{y}\|^2 + \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] &= \frac{1}{2} \left[\langle x+y, x+y \rangle - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \frac{1}{2} \left[\|\mathbf{x}\|^2 + 2\langle x, y \rangle + \|\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \langle \mathbf{x}, \mathbf{y} \rangle. \end{aligned}$$

2. Show that $O(n)$ is a group.

Solution. If $A, B \in O(n)$, then $AB \in O(n)$ since $(AB)^t = B^t A^t = B^{-1}A^{-1} = (AB)^{-1}$.

3. Prove that the following matrices are orthogonal. Are any of these matrices in $SO(n)$?

(a)

$$\begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

(b)

$$\begin{pmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ -2/\sqrt{5} & 1/\sqrt{5} \end{pmatrix}$$

(c)

$$\begin{pmatrix} 4/\sqrt{5} & 0 & 3/\sqrt{5} \\ -3/\sqrt{5} & 0 & 4/\sqrt{5} \\ 0 & -1 & 0 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1/3 & 2/3 & -2/3 \\ -2/3 & 2/3 & 1/3 \\ -2/3 & 1/3 & 2/3 \end{pmatrix}$$

Hint. (a) is in $SO(2)$; (c) is not in $O(3)$.

Solution.

(a) An element of $SO(2)$.

(b) An element of $SO(2)$.

(c) Not in $O(3)$.

(d) Not in $O(3)$.

4. Determine the symmetry group of each of the figures in Figure 12.25.

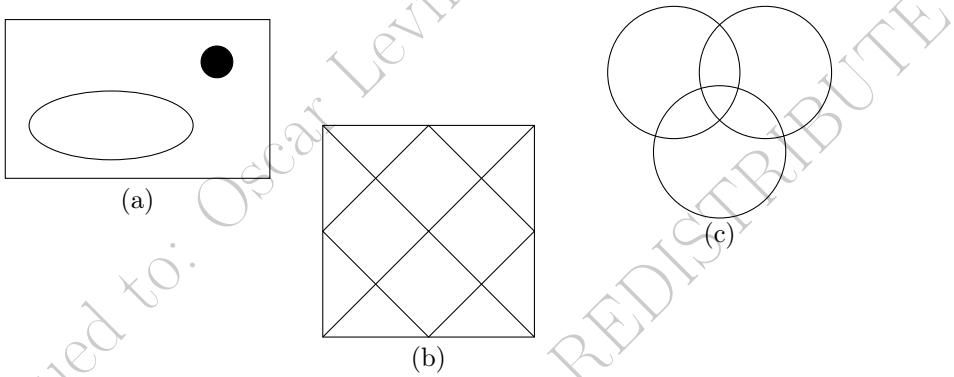


Figure 12.25

Solution. (a) The only symmetry is the identity. (b) D_4. (c) S_3.

5. Let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{w}$ be vectors in $\mathbb{R}^n$ and $\alpha \in \mathbb{R}$. Prove each of the following properties of inner products.

(a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

(b) $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.

(c) $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha\mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.

(d) $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ with equality exactly when $\mathbf{x} = 0$.

(e) If $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ for all $\mathbf{x}$ in $\mathbb{R}^n$, then $\mathbf{y} = 0$.

Hint. (a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

Solution.

(a) $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + \cdots + x_ny_n = y_1x_1 + \cdots + y_nx_n = \langle \mathbf{y}, \mathbf{x} \rangle$.

(b) $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = x_1(y_1 + w_1) + \cdots + x_n(y_n + w_n) = (x_1y_1 + \cdots + x_ny_n) + (x_1w_1 + \cdots + x_nw_n) = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.

(c) $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = (\alpha x_1)y_1 + \cdots + (\alpha x_n)y_n = \alpha(x_1y_1 + \cdots + x_ny_n) = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.

(d) $\langle \mathbf{x}, \mathbf{x} \rangle = x_1^2 + \cdots + x_n^2 \geq 0$. $x_1^2 + \cdots + x_n^2 = 0$ if and only if $x_1 = \cdots = x_n = 0$.

(e) Follows from (d).

6. Verify that

$$E(n) = \{(A, \mathbf{x}) : A \in O(n) \text{ and } \mathbf{x} \in \mathbb{R}^n\}$$

is a group.

Solution. To show that $E(n)$ is a group, verify that it is associative under the operation

$$(A, \mathbf{x})(B, \mathbf{y}) = (AB, A\mathbf{y} + \mathbf{x}).$$

Also show that $(I, \mathbf{0})$ is the identity and $(A, \mathbf{x})^{-1} = (A^{-1}, -A^{-1}\mathbf{x})$.

7. Prove that $\{(2, 1), (1, 1)\}$ and $\{(12, 5), (7, 3)\}$ are bases for the same lattice.

Hint. Use the unimodular matrix

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

Solution. Using the unimodular matrix

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix},$$

we have

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ 5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \end{pmatrix}.$$

8. Let G be a subgroup of $E(2)$ and suppose that T is the translation subgroup of G. Prove that the point group of G is isomorphic to G/T.

Solution. Use the First Isomorphism Theorem and the map $(A, \mathbf{x}) \mapsto A$.

9. Let $A \in SL_2(\mathbb{R})$ and suppose that the vectors $\mathbf{x}$ and $\mathbf{y}$ form two sides of a parallelogram in $\mathbb{R}^2$. Prove that the area of this parallelogram is the same as the area of the parallelogram with sides $A\mathbf{x}$ and $A\mathbf{y}$.

Solution. Show that the area of the parallelogram with sides $\mathbf{x}$ and $\mathbf{y}$ is the absolute value of the determinant of the matrix $(\mathbf{xy})$.

10. Prove that $SO(n)$ is a normal subgroup of $O(n)$.

Hint. Show that the kernel of the map $\det : O(n) \to \mathbb{R}^*$ is $SO(n)$.

Solution. Show that the kernel of the map $\det : O(n) \to \mathbb{R}^*$ is $SO(n)$.

11. Show that any isometry f in $\mathbb{R}^n$ is a one-to-one map.

Solution. If $f(\mathbf{x}) = f(\mathbf{y})$, then $f(\mathbf{x}) - f(\mathbf{y}) = \mathbf{0}$. So $\|f(\mathbf{x}) - f(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\| = 0$. Thus, $\mathbf{x} - \mathbf{y} = 0$ or $\mathbf{x} = \mathbf{y}$.

12. Prove or disprove: an element in $E(2)$ of the form $(A, \mathbf{x})$, where $\mathbf{x} \neq 0$, has infinite order.

Solution. False. Let

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

and $\mathbf{x} = (1, -1)$.

13. Prove or disprove: There exists an infinite abelian subgroup of $O(n)$.

Hint. True.

Solution. True.

14. Let $\mathbf{x} = (x_1, x_2)$ be a point on the unit circle in $\mathbb{R}^2$; that is, $x_1^2 + x_2^2 = 1$. If $A \in O(2)$, show that $A\mathbf{x}$ is also a point on the unit circle.

Solution. The point $\mathbf{x} = (x_1, x_2)$ is on the unit circle if and only if $\|\mathbf{x}\| = x_1^2 + x_2^2 = 1$. By Theorem 12.8, it follows that $\|A\mathbf{x}\| = \|\mathbf{x}\| = 1$.

15. Let G be a group with a subgroup H (not necessarily normal) and a normal subgroup N. Then G is a **semidirect product** of N by H if

- $H \cap N = \{\text{id}\}$;
- $HN = G$.

Show that each of the following is true.

(a) S_3 is the semidirect product of A_3 by $H = \{(1), (12)\}$.

(b) The quaternion group, Q_8, cannot be written as a semidirect product.

(c) $E(2)$ is the semidirect product of $O(2)$ by H, where H consists of all translations in $\mathbb{R}^2$.

Solution.

(a) $A_3 = \{(1), (123), (132)\}$. S_3 is a semidirect product of H and A_3, since A_3 is normal in S_3, $A_3 \cap H = \{(1)\}$, and $A_3 H = S_3$.

(b) The group Q_8 cannot be written as the union of two proper subgroups whose intersection is the identity.

(c) Let $N = O(2)$.

16. Determine which of the 17 wallpaper groups preserves the symmetry of the pattern in Figure 12.16.

Solution. pmg

17. Determine which of the 17 wallpaper groups preserves the symmetry of the pattern in Figure 12.26.

Hint. $p6m$

Solution. $p6m$

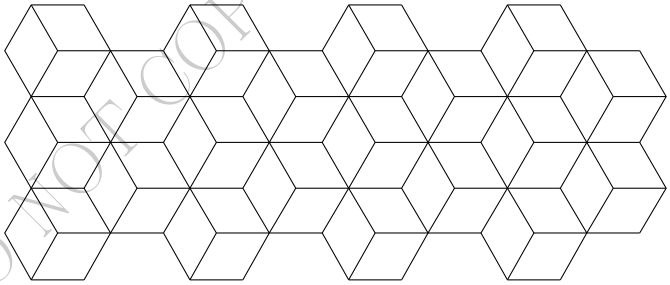


Figure 12.26

18. Find the rotation group of a dodecahedron.

Solution. A_5

19. For each of the 17 wallpaper groups, draw a wallpaper pattern having that group as a symmetry group.

Solution.

12.5 Sage Exercises

There are no Sage exercises for this chapter.

Chapter 13

The Structure of Groups

13.3 Exercises

1. Find all of the abelian groups of order less than or equal to 40 up to isomorphism.

Hint. There are three possible groups.

Solution. Since $40 = 2^3 \cdot 5$, the possible abelian groups of order 40 are $\mathbb{Z}_{40} \cong \mathbb{Z}_8 \times \mathbb{Z}_5$, $\mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Find all of the abelian groups of order 200 up to isomorphism.

Solution. Since $200 = 2^3 \cdot 5^2$, the possible abelian groups of order 200 are

$$\mathbb{Z}_{200} \cong \mathbb{Z}_8 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

3. Find all of the abelian groups of order 720 up to isomorphism.

Solution. Since $720 = 2^4 \cdot 3^2 \cdot 5$, the possible abelian groups of order 720 are

$$\mathbb{Z}_{720} \cong \mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

4. Find all of the composition series for each of the following groups.

(a) $\mathbb{Z}_{12}$

(b) $\mathbb{Z}_{48}$

(c) The quaternions, Q_8

(d) D_4

(e) $S_3 \times \mathbb{Z}_4$

(f) S_4

(g) S_n, $n \geq 5$

(h) $\mathbb{Q}$

Hint. (a) $\{0\} \subset \langle 6 \rangle \subset \langle 3 \rangle \subset \mathbb{Z}_{12}$; (e) $\{(1)\} \times \{0\} \subset \{(1), (123), (132)\} \times \{0\} \subset S_3 \times \{0\} \subset S_3 \times \langle 2 \rangle \subset S_3 \times \mathbb{Z}_4$.

Solution.

(a) $\{0\} \subset \langle 6 \rangle \subset \langle 3 \rangle \subset \mathbb{Z}_{12}$.

(b) $\{0\} \subset \langle 16 \rangle \subset \langle 8 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \mathbb{Z}_{12}$.

(c) $\{0\} \subset \{\pm 1\} \subset \{\pm 1, \pm I\} \subset Q_8$.

(d) $\{(1)\} \subset \{(1), (12)(34)\} \subset \{(1), (12)(34), (13)(24), (14)(23)\} \subset D_4$.

(e) $\{(1)\} \times \{0\} \subset \{(1), (123), (132)\} \times \{0\} \subset S_3 \times \{0\} \subset S_3 \times \langle 2 \rangle \subset S_3 \times \mathbb{Z}_4$.

(f) $(1) \subset \{(1), (12)(34), (13)(24), (14)(23)\} \subset A_4 \subset S_4$.

(g) $(1) \subset A_n \subset S_n$.

(h) There is no composition series for $\mathbb{Q}$.

5. Show that the infinite direct product $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ is not finitely generated.

Solution. If there were a finite number of generators, then G would be a finite group, since every element of G has order 2.

6. Let G be an abelian group of order m. If n divides m, prove that G has a subgroup of order n.

Solution. Apply the Fundamental Theorem of Finite Abelian Groups. Let G be an abelian group of order m. If n divides m, prove that G has a subgroup of order n.

7. A group G is a **torsion group** if every element of G has finite order. Prove that a finitely generated abelian torsion group must be finite.

Hint. Use the Fundamental Theorem of Finitely Generated Abelian Groups.

Solution. Use the Fundamental Theorem of Finitely Generated Abelian Groups.

8. Let G, H, and K be finitely generated abelian groups. Show that if $G \times H \cong G \times K$, then $H \cong K$. Give a counterexample to show that this cannot be true in general.

Solution. By the Fundamental Theorem of Finitely Generated Abelian Groups, we may assume that

$$\begin{aligned} G &= \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}^{\alpha} \\ H &= \mathbb{Z}_{q_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{q_m^{\beta_m}} \times \mathbb{Z}^{\beta} \\ K &= \mathbb{Z}_{r_1^{\gamma_1}} \times \cdots \times \mathbb{Z}_{r_n^{\gamma_n}} \times \mathbb{Z}^{\gamma}. \end{aligned}$$

Hence

$$\begin{aligned} G \times H &= \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}_{q_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{q_m^{\beta_m}} \times \mathbb{Z}^{\alpha+\beta} \\ G \times K &= \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}_{r_1^{\gamma_1}} \times \cdots \times \mathbb{Z}_{r_n^{\gamma_n}} \times \mathbb{Z}^{\alpha+\gamma}. \end{aligned}$$

Since these two direct products are the same up to the order of the primes p_i, q_j, and r_l, it must be the case that $\beta = \gamma$ and $m = n$. With a proper reordering of the factors, $q_1^{\beta_1} = r_1^{\gamma_1}, \ldots, q_m^{\beta_m} = r_m^{\beta_m}$. Consequently, $H \cong K$. To show that the exercise is not true in general, let $H = \mathbb{Z}$, $K = \mathbb{Z} \times \mathbb{Z}$ and $G = \mathbb{Z} \times \mathbb{Z} \times \cdots$.

9. Let G and H be solvable groups. Show that $G \times H$ is also solvable.

Solution. Since H and K are solvable, there exist composition series $\{H_i\}$ and $\{K_j\}$ for H and K, respectively, such that the factor groups of each composition series are abelian. The desired composition series for $H \times K$ is

$$H \times K \supset H_{m-1} \times K \supset H_{m-2} \times K \supset \cdots \{e\} \times K \supset \{e\} \times K_{n-1} \supset \{e\} \times K_{n-2} \supset \cdots \{e\} \times \{e\}.$$

Since

$$(H_{i+1} \times K)/(H_i \times K) \cong H_{i+1}/H_i \text{ and } (K_{j+1} \times \{e\})/(K_j \times \{e\}) \cong K_{j+1}/K_j$$

all of the factor groups are abelian.

10. If G has a composition (principal) series and if N is a proper normal subgroup of G, show there exists a composition (principal) series containing N.

Solution. Let

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$

be a composition series for G. Show that

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_{i+1} \supset N \supset H_i \cap N \supset \cdots \supset H_1 \cap N \supset H_0 \cap N = \{e\}$$

is a composition series for G, where N is a subset of H_{i+1} but not a subset of H_i.

11. Prove or disprove: Let N be a normal subgroup of G. If N and G/N have composition series, then G must also have a composition series.

Solution. True.

12. Let N be a normal subgroup of G. If N and G/N are solvable groups, show that G is also a solvable group.

Hint. If N and G/N are solvable, then they have solvable series

$$N = N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 = \{e\}$$
$$G/N = G_n/N \supset G_{n-1}/N \supset \cdots G_1/N \supset G_0/N = \{N\}.$$

Solution. If N and G/N are solvable, then they have solvable series

$$N = N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 = \{e\}$$
$$G/N = G_n/N \supset G_{n-1}/N \supset \cdots G_1/N \supset G_0/N = \{N\}.$$

The series

$$\begin{aligned} G &= G_n \supset G_{n-1} \supset \cdots \supset G_0 \\ &= N \\ &= N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 \\ &= \{e\} \end{aligned}$$

is a subnormal series. The are abelian since $G_{i+1}/G_i \cong (G_{i+1}/N)/(G_i/N)$.

13. Prove that G is a solvable group if and only if G has a series of subgroups

$$G = P_n \supset P_{n-1} \supset \cdots \supset P_1 \supset P_0 = \{e\}$$

where P_i is normal in P_{i+1} and the order of P_{i+1}/P_i is prime.

Solution. If the order of P_{i+1}/P_i is prime, then the factor group must be abelian. For the converse, use the Fundamental Theorem of Finite Abelian Groups.

14. Let G be a solvable group. Prove that any subgroup of G is also solvable.

Solution. Let G be a solvable group and H a subgroup of G. Since G is solvable, it has a composition series $\{G_i\}$. Consider the subnormal series $\{G_i \cap H\}$ of H. Using the Second Isomorphism Theorem,

$$(G_{i+1} \cap H)/(G_i \cap H) \cong G_i(G_{i+1} \cap H)/G_i.$$

The right-hand side is a subgroup of G_{i+1}/G_i; hence, it is abelian.

15. Let G be a solvable group and N a normal subgroup of G. Prove that G/N is solvable.

Solution. Let G have a subnormal series $\{H_i\}$, where H_{i+1}/H_i is abelian. If N is normal in G, then the natural homomorphism $\eta : G \to G/N$ takes normal subgroups of G to normal subgroups of G/N. Let $\overline{H}_i$ be the image of H_i under η. We need only show that $\overline{H}_{i+1}/\overline{H}_i$ is abelian. Let $\eta(x) = \overline{x}$ and $\eta(y) = \overline{y}$. Since H_{i+1}/H_i is abelian, there exists an $h \in H_i$ such that $xy = yxh$. Thus, $\eta(xy) = \eta(x)\eta(y) = \eta(y)\eta(x)\eta(h)$. But $\eta(h) \in \overline{H}_i$. Therefore,

$$\overline{x}\overline{H}_i\overline{y}\overline{H}_i = \overline{xy}\overline{H}_i = \eta(xy)\overline{H}_i = \eta(x)\eta(y)\overline{H}_i = \eta(y)\eta(x)\overline{H}_i = \overline{y}\overline{H}_i\overline{x}\overline{H}_i.$$

16. Prove that D_n is solvable for all integers n.

Hint. Use the fact that D_n has a cyclic subgroup of index 2.

Solution. Use the fact that D_n has a cyclic subgroup of index 2.

17. Suppose that G has a composition series. If N is a normal subgroup of G, show that N and G/N also have composition series.

Solution. The fact that N has a composition series is trivial. To show that G/N has a composition series, apply the Isomorphism Theorems and the Correspondence Theorem of Chapter 11.

18. Let G be a cyclic p-group with subgroups H and K. Prove that either H is contained in K or K is contained in H.

Solution. Suppose that H is not contained in K and look at a generator for K.

19. Suppose that G is a solvable group with order $n \geq 2$. Show that G contains a normal nontrivial abelian subgroup.

Solution. Use the definition of a solvable group and the Jordan-Hölder Theorem.

20. Recall that the **commutator subgroup** G' of a group G is defined as the subgroup of G generated by elements of the form $a^{-1}b^{-1}ab$ for $a, b \in G$. We can define a series of subgroups of G by $G^{(0)} = G$, $G^{(1)} = G'$, and $G^{(i+1)} = (G^{(i)})'$.

(a) Prove that $G^{(i+1)}$ is normal in $(G^{(i)})'$. The series of subgroups

$$G^{(0)} = G \supset G^{(1)} \supset G^{(2)} \supset \cdots$$

is called the **derived series** of G.

(b) Show that G is solvable if and only if $G^{(n)} = \{e\}$ for some integer n.

Solution.

(a) See Exercise 10.3.14 in Chapter 10.

(b) If $G^{(n)} = \{e\}$, then $\{e\} = G^{(n)} \subset \cdots \subset G^{(1)} \subset G$ is a subnormal series for G with abelian factor groups. Conversely, if G is solvable, there exists a subnormal series $\{H_i\}$ with abelian factor groups. Since H_i/H_{i+1} is abelian, $H_i \supset H'_{i+1}$. Now show by induction that $H_i \supset G^{(i)}$.

21. Suppose that G is a solvable group with order $n \geq 2$. Show that G contains a normal nontrivial abelian factor group.

Hint. G/G' is abelian.

Solution. G/G' is abelian.

22. **Zassenhaus Lemma.** Let H and K be subgroups of a group G. Suppose also that H^* and K^* are normal subgroups of H and K respectively. Then

(a) $H^*(H \cap K^*)$ is a normal subgroup of $H^*(H \cap K)$.

(b) $K^*(H^* \cap K)$ is a normal subgroup of $K^*(H \cap K)$.

(c) $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/(H^* \cap K)(H \cap K^*)$.

Solution. Let $D = (H^* \cap K)(H \cap K^*)$. Since K^* is normal in K, $SK^* = K^*S$ for every nonempty subset S of K. Thus, $K^*(H \cap K)$ is a subgroup of K, and K^* is a normal subgroup of $K^*(H \cap K)$. By the Second Isomorphism Theorem, $H \cap K^*$ is normal in $H \cap K$. Similarly, $H^* \cap K$ is normal in $H \cap K$. Consequently, D is a normal subgroup of $H \cap K$.

If $x \in K^*(H \cap K)$, then $x = bc$ for $b \in K^*$ and $c \in H \cap K$. Define $\phi : K^*(H \cap K) \to H \cap K/D$ by $\phi(x) = cD$. It is straightforward to show that ϕ is a well-defined onto homomorphism with kernel $K^*(H^* \cap K)$. By the First Isomorphism Theorem, $K^*(H^* \cap K)$ is normal in $K^*(H \cap K)$, and $K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/D$.

A similar argument gives a homomorphism $\psi : H^*(H \cap K) \to (H \cap K)/D$. Thus, $H^*(H \cap K)$ is normal in $H^*(H \cap K)$ and the quotient group is isomorphic to $(H \cap K)/D$. Therefore, the two quotient groups of the theorem are isomorphic.

23. **Schreier's Theorem.** Use the Zassenhaus Lemma to prove that two subnormal (normal) series of a group G have isomorphic refinements.

Solution. Let $\{H_i\}$ and $\{K_j\}$ be two normal series for G, with $1 \leq i \leq n$ and $1 \leq j \leq m$. In the first series, between each H_i and H_{i+1}, insert the groups $H_i(H_{i+1} \cap K_{j+1})$, where $1 \leq j \leq m$. This is a normal series with mn inclusions. Notice that the inclusions need not be strict. In the second series, insert $K_j(K_{j+1} \cap H_{i+1})$ between each K_j and K_{j+1} for $1 \leq j \leq n$. This is also a normal series. We now have normal series $\{H_i(H_{i+1} \cap K_{j+1})\}$ and $\{K_j(K_{j+1} \cap H_{i+1})\}$. These are common refinements. Apply the Zassenhaus lemma using the four subgroups H_i H_{i+1}, K_j, and K_{j+1}.

24. Use Schreier's Theorem to prove the Jordan-Hölder Theorem.

Solution. Let $\{H_i\}$ and $\{K_j\}$ be two composition series of a group G. By Schreier's theorem, they have isomorphic refinements. However, since all factor groups are simple, neither of the two series can have a further refinement. Consequently, $\{H_i\}$ and $\{K_j\}$ must be isomorphic.

13.6 Sage Exercises

There are no Sage exercises for this chapter.

Chapter 14

Group Actions

14.4 Exercises

1. Examples 14.1–14.5 in the first section each describe an action of a group G on a set X, which will give rise to the equivalence relation defined by G-equivalence. For each example, compute the equivalence classes of the equivalence relation, the G-**equivalence classes**.

Hint. Example 14.1: 0, $\mathbb{R}^2 \setminus \{0\}$. Example 14.2: $X = \{1, 2, 3, 4\}$.

Solution. Example 14.1: 0, $\mathbb{R}^2 \setminus \{0\}$. Example 14.1: $X = \{1, 2, 3, 4\}$. Example 14.2: The G-equivalence class depends on the subgroup H acting on G. If $H = G$, then there is a single equivalence class, namely G. Examples 14.3–14.5: The G-equivalence class depends on the subgroup H acting on G.

2. Compute all X_g and all G_x for each of the following permutation groups.

(a) $X = \{1, 2, 3\}$, $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

(b) $X = \{1, 2, 3, 4, 5, 6\}$, $G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$

Hint. (a) $X_{(1)} = \{1, 2, 3\}$, $X_{(12)} = \{3\}$, $X_{(13)} = \{2\}$, $X_{(23)} = \{1\}$, $X_{(123)} = X_{(132)} = \emptyset$. $G_1 = \{(1), (23)\}$, $G_2 = \{(1), (13)\}$, $G_3 = \{(1), (12)\}$.

Solution.

(a) $X_{(1)} = \{1, 2, 3\}$, $X_{(12)} = \{3\}$, $X_{(13)} = \{2\}$, $X_{(23)} = \{1\}$, $X_{(123)} = X_{(132)} = \emptyset$. $G_1 = \{(1), (23)\}$, $G_2 = \{(1), (13)\}$, $G_3 = \{(1), (12)\}$.

(b) $X_{(1)} = \{1, 2, 3, 4, 5, 6\}$, $X_{(12)} = \{3, 4, 5, 6\}$, $X_{(345)} = X_{(354)} = \{1, 2, 6\}$, $X_{(12)(345)} = X_{(12)(354)} = \{6\}$. $G_1 = G_2 = \{(1), (345), (354)\}$, $G_3 = G_4 = G_5 = \{(1), (12)\}$, $G_6 = G$.

3. Compute the G-equivalence classes of X for each of the G-sets in Exercise 14.4.2. For each $x \in X$ verify that $|G| = |\mathcal{O}_x| \cdot |G_x|$.

Hint. (a) $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$.

Solution.

(a) $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$.

(b) $\mathcal{O}_1 = \mathcal{O}_2 = \{1, 2\}$. $\mathcal{O}_3 = \mathcal{O}_4 = \mathcal{O}_5 = \{3, 4, 5\}$. $\mathcal{O}_6 = \{6\}$.

4. Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point on the plane other than the origin.

(a) Show that $\mathbb{R}^2$ is a G-set.

(b) Describe geometrically the orbit containing P.

(c) Find the group G_P.

Solution.

(a) G acts on a point $(x, y) \in \mathbb{R}^2$ by

$$\theta \cdot (x, y) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

Clearly $0 \cdot (x, y) = (x, y)$. Also,

$$\begin{aligned} (\alpha + \beta) \cdot (x, y) &= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \alpha \cdot (\beta \cdot (x, y)). \end{aligned}$$

(b) The orbit containing $P = (x, y)$ with $P \neq (0, 0)$ is a circle centered at the origin with radius $\sqrt{x^2 + y^2}$. The orbit of $(0, 0)$ is $(0, 0)$.

(c) If $P \neq (0, 0)$, then $G_P = 2\pi\mathbb{Z}$. $G_{(0,0)} = G$.

5. Let $G = A_4$ and suppose that G acts on itself by conjugation; that is, $(g, h) \mapsto ghg^{-1}$.

(a) Determine the conjugacy classes (orbits) of each element of G.

(b) Determine all of the isotropy subgroups for each element of G.

Solution.

(a) The conjugacy classes are

$$\begin{gathered} \{(1)\} \\ \{(12)(34), (13)(24), (14)(23)\} \\ \{(123), (132), (124), (142), (134), (143), (234), (243)\} \end{gathered}$$

(b) The isotropy subgroups are

$$\begin{aligned} G_{(1)} &= \{(1)\} \\ G_{(12)(34)} &= \{(1), (13)(24), (14)(23)\} \\ G_{(13)(24)} &= \{(1), (12)(34), (14)(23)\} \\ G_{(14)(23)} &= \{(1), (12)(34), (13)(24)\} \\ G_{(123)} = G_{(132)} &= \{(1), (123), (132)\} \\ G_{(124)} = G_{(142)} &= \{(1), (124), (142)\} \\ G_{(134)} = G_{(143)} &= \{(1), (134), (143)\} \\ G_{(234)} = G_{(243)} &= \{(1), (234), (243)\} \end{aligned}$$

6. Find the conjugacy classes and the class equation for each of the following groups.

(a) S_4 (b) D_5 (c) $\mathbb{Z}_9$ (d) Q_8

Hint. The conjugacy classes for S_4 are

$$\begin{gathered}\mathcal{O}_{(1)} = \{(1)\},\\ \mathcal{O}_{(12)} = \{(12),(13),(14),(23),(24),(34)\},\\ \mathcal{O}_{(12)(34)} = \{(12)(34),(13)(24),(14)(23)\},\\ \mathcal{O}_{(123)} = \{(123),(132),(124),(142),(134),(143),(234),(243)\},\\ \mathcal{O}_{(1234)} = \{(1234),(1243),(1324),(1342),(1423),(1432)\}.\end{gathered}$$

The class equation is $1+3+6+6+8=24$.

Solution.

(a) The conjugacy classes for S_4 are

$$\begin{gathered}\mathcal{O}_{(1)} = \{(1)\},\\ \mathcal{O}_{(12)} = \{(12),(13),(14),(23),(24),(34)\},\\ \mathcal{O}_{(12)(34)} = \{(12)(34),(13)(24),(14)(23)\},\\ \mathcal{O}_{(123)} = \{(123),(132),(124),(142),(134),(143),(234),(243)\},\\ \mathcal{O}_{(1234)} = \{(1234),(1243),(1324),(1342),(1423),(1432)\}.\end{gathered}$$

The class equation is $1+3+6+6+8=24$.

(b) The conjugacy classes for D_5 are

$$\begin{gathered}\mathcal{O}_{(1)} = \{(1)\},\\ \mathcal{O}_{(12345)} = \{(12345),(154323)\},\\ \mathcal{O}_{(13524)} = \{(13524),(14253)\},\\ \mathcal{O}_{(12)(35)} = \{(12)(35),(13)(45),(14)(23),(15)(24),(25)(34)\}.\end{gathered}$$

The class equation is $1+2+2+5=10$.

(c) The center of $\mathbb{Z}_9$ is itself, since $\mathbb{Z}_9$ is abelian; hence, the class equation is $9=9$.

(d) The conjugacy classes for Q_8 are

$$\begin{gathered}\mathcal{O}_1 = \{1\},\\ \mathcal{O}_{-1} = \{-1\},\\ \mathcal{O}_I = \mathcal{O}_{-I} = \{\pm I\},\\ \mathcal{O}_J = \mathcal{O}_{-J} = \{\pm J\},\\ \mathcal{O}_K = \mathcal{O}_{-K} = \{\pm K\}.\end{gathered}$$

The class equation is $2+2+2+2=8$.

7. Write the class equation for S_5 and for A_5.

Solution. The class equation for S_5 is $120 = 1+10+20+30+24+15+20$. The class equation for A_5 is $60 = 1+20+24+15$.

8. If a square remains fixed in the plane, how many different ways can the corners of the square be colored if three colors are used?

Hint. $(3^4+3^1+3^2+3^1+3^2+3^2+3^3+3^3)/8 = 21$.

Solution. $(3^4+3^1+3^2+3^1+3^2+3^2+3^3+3^3)/8 = 21$.

9. How many ways can the vertices of an equilateral triangle be colored using three different colors?

Solution. $(3^3 + 3 \cdot 3^2 + 2 \cdot 3)/6 = 10$.

10. Find the number of ways a six-sided die can be constructed if each side is marked differently with $1, \ldots, 6$ dots.

Solution. Let X be the set of $6! = 720$ possible different markings of the face using $1, \ldots, 6$ dots. If G is the rotation group of the cube then $|G| = 24$. For $g \in G$ with $g \neq e$, we have $|X_g| = 0$, since any rotation of the cube aside from the identity would transform one of the possible 720 markings of the die into a different one. Also, $|X_e| = 720$, since the identity leaves all of the markings fixed. Hence, the number of distinguishable dies is $720/24 = 30$.

11. Up to a rotation, how many ways can the faces of a cube be colored with three different colors?

Hint. The group of rigid motions of the cube can be described by the allowable permutations of the six faces and is isomorphic to S_4. There are the identity cycle, 6 permutations with the structure $(abcd)$ that correspond to the quarter turns, 3 permutations with the structure $(ab)(cd)$ that correspond to the half turns, 6 permutations with the structure $(ab)(cd)(ef)$ that correspond to rotating the cube about the centers of opposite edges, and 8 permutations with the structure $(abc)(def)$ that correspond to rotating the cube about opposite vertices.

Solution. The group of rigid motions of the cube can be described by the allowable permutations of the six faces and is isomorphic to S_4. There are the identity cycle, 6 permutations with the structure $(abcd)$ that correspond to the quarter turns, 3 permutations with the structure $(ab)(cd)$ that correspond to the half turns, 6 permutations with the structure $(ab)(cd)(ef)$ that correspond to rotating the cube about the centers of opposite edges, and 8 permutations with the structure $(abc)(def)$ that correspond to rotating the cube about opposite vertices. Thus, there are

$$\frac{1}{24}(1 \cdot 3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 6 \cdot 3^3 + 8 \cdot 3^2)/24 = 57.$$

12. Consider 12 straight wires of equal lengths with their ends soldered together to form the edges of a cube. Either silver or copper wire can be used for each edge. How many different ways can the cube be constructed?

Solution. $(2^{12} + 6 \cdot 2^7 + 8 \cdot 2^4 + 9 \cdot 2^3)/24 = 211$.

13. Suppose that we color each of the eight corners of a cube. Using three different colors, how many ways can the corners be colored up to a rotation of the cube?

Solution. $(9 \cdot 3^2 + 14 \cdot 3^4 + 3^{12})/24 = 22{,}194$.

14. Each of the faces of a regular tetrahedron can be painted either red or white. Up to a rotation, how many different ways can the tetrahedron be painted?

Solution. If we number the faces of a regular tetrahedron by 1, 2, 3, 4, then the symmetry group of the tetrahedron can be thought of as A_4:

$$\{(1), (12)(34), (13)(24), (14)(23),$$
$$(123), (132), (124), (142), (134), (143)(234), (243)\}$$

There are also 2^4 possible colorings of the tetrahedron; however, some of these colorings are equivalent. The identity fixes every face; thus, $|X_e| = 2^4 = 16$. Also,

$$X_{(12)(34)} = X_{(13)(24)} = X_{(14)(23)} = 2^2$$

and

$$X_{(123)} = X_{(132)} = X_{(124)} = X_{(142)}$$
$$= X_{(134)} = X_{(143)} = X_{(234)} = X_{(243)} = 2.$$

Hence, there are

$$\frac{1}{12}(2^4 + 3 \cdot 2^2 + 8 \cdot 2^2) = 5$$

possible colorings of the tetrahedron.

15. Suppose that the vertices of a regular hexagon are to be colored either red or white. How many ways can this be done up to a symmetry of the hexagon?

Hint. $(1 \cdot 2^6 + 3 \cdot 2^4 + 4 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2^1)/12 = 13$.

Solution. $(1 \cdot 2^6 + 3 \cdot 2^4 + 4 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2^1)/12 = 13$.

16. A molecule of benzene is made up of six carbon atoms and six hydrogen atoms, linked together in a hexagonal shape as in Figure 14.28.

(a) How many different compounds can be formed by replacing one or more of the hydrogen atoms with a chlorine atom?

(b) Find the number of different chemical compounds that can be formed by replacing three of the six hydrogen atoms in a benzene ring with a CH_3 radical.

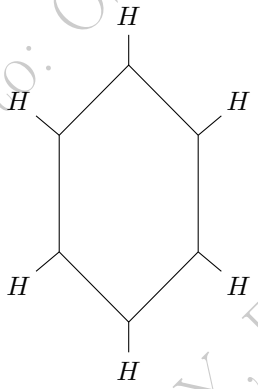


Figure 14.28: A benzene ring

Solution. (a) $(2^2 + 2^3 + 3 \cdot 2^4 + 2^5 + 2^6)/12 = 13$; (b) 3.

17. How many equivalence classes of switching functions are there if the input variables x_1, x_2, and x_3 can be permuted by any permutation in S_3? What if the input variables x_1, x_2, x_3, and x_4 can be permuted by any permutation in S_4?

Hint. $(1 \cdot 2^8 + 3 \cdot 2^6 + 2 \cdot 2^4)/6 = 80$.

Solution. $(1 \cdot 2^8 + 3 \cdot 2^6 + 2 \cdot 2^4)/6 = 80$.

18. How many equivalence classes of switching functions are there if the input variables x_1, x_2, x_3, and x_4 can be permuted by any permutation in the subgroup of S_4 generated by the permutation $(x_1x_2x_3x_4)$?

Solution. $(2^{16} + 6 \cdot 2^{12} + 6 \cdot 2^6 + 3 \cdot 2^{10} + 8 \cdot 2^4)/24 = 3904$.

19. A striped necktie has 12 bands of color. Each band can be colored by one of four possible colors. How many possible different-colored neckties are there?

Solution. $(4^{12} + 4^6)/2 = 8390656$.

20. A group acts **faithfully** on a G-set X if the identity is the only element of G that leaves every element of X fixed. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

Solution. If G acts faithfully on X and $g_1x = g_2x$, then $g_2^{-1}g_1x = x$. However, the only element in G that fixes every element in X is the identity. Therefore, $g_2^{-1}g_1 = e$ or $g_1 = g_2$. Conversely, if $gx = x = ex$, then g and e have the same action on x. Thus, $g = e$.

21. Let p be prime. Show that the number of different abelian groups of order p^n (up to isomorphism) is the same as the number of conjugacy classes in S_n.

Solution. Use mathematical induction.

22. Let $a \in G$. Show that for any $g \in G$, $gC(a)g^{-1} = C(gag^{-1})$.

Hint. Use the fact that $x \in gC(a)g^{-1}$ if and only if $g^{-1}xg \in C(a)$.

Solution. Since $x \in gC(a)g^{-1}$ if and only if $g^{-1}xg \in C(a)$, it follows that $x \in gC(a)g^{-1}$ if and only if $ag^{-1}xg = g^{-1}xga$. This last statement is equivalent to $gag^{-1}x = xgag^{-1}$ or $x \in C(gag^{-1})$.

23. Let $|G| = p^n$ be a nonabelian group for p prime. Prove that $|Z(G)| < p^{n-1}$.

Solution. If $|Z(G)| = p^n$, then $G = Z(G)$ and G is abelian. If $|Z(G)| = p^{n-1}$, then $G/Z(G)$ has order p and must be cyclic. By Exercise 10.3.13, we know that G is abelian.

24. Let G be a group with order p^n where p is prime and X a finite G-set. If $X_G = \{x \in X : gx = x \text{ for all } g \in G\}$ is the set of elements in X fixed by the group action, then prove that $|X| \equiv |X_G| \pmod{p}$.

Solution. Use the fact that

$$|X| = |X_G| + \sum_{i=k}^{n} |\mathcal{O}_{x_i}| = |X_G| + \sum_{i=k}^{n} [G : G_{x_i}].$$

25. If G is a group of order p^n, where p is prime and $n \geq 2$, show that G must have a proper subgroup of order p. If $n \geq 3$, is it true that G will have a proper subgroup of order p^2?

Solution.

14.7 Sage Exercises

1. Construct the Higman-Sims graph with the command `graphs.HigmanSimsGraph()`. Then construct the automorphism group and determine the order of the one interesting normal subgroup of this group. You can try plotting the graph, but the graphic is unlikely to be very informative.

Solution.

```
H = graphs.HigmanSimsGraph()
A = H.automorphism_group()
A.composition_series()[1].order()
```

```
44352000
```

2. This exercise asks you to verify the class equation outside of the usual situation where the group action is conjugation. Consider the example of the automorphism group of the path on 11 vertices. First construct the list of orbits. From each orbit, grab the first element of the orbit as a representative. Compute the size of the orbit as the index of the stabilizer of the representative in the group via Theorem 14.11. (Yes, you could just compute the size of the full orbit, but the idea of the exercise is to use more group-theoretic results.) Then sum these orbit-sizes, which should equal the size of the whole vertex set since the orbits form a partition.

Solution.

```
P = graphs.PathGraph(11)
A = P.automorphism_group()
orbs = [A.order()/A.stabilizer(x[0]).order() for x in
    A.orbits()]
orbs
```

```
[2, 2, 2, 2, 2, 1]
```

```
P.num_verts() == sum(orbs)
```

```
True
```

3. Construct a simple graph (no loops or multiple edges), with at least two vertices and at least one edge, whose automorphism group is trivial. You might start experimenting by drawing pictures on paper before constructing the graph. A command like the following will let you construct a graph from edges. The graph below looks like a triangle or 3-cycle.

```
G = Graph([(1,2), (2,3), (3,1)])
G.plot()
```

Solution. The example with the fewest vertices?

```
G = Graph([(1,2), (2,3), (3,1), (2,4), (3,5), (5,6)])
G.automorphism_group().order()
```

```
1
```

The smallest tree?

```
G = Graph([(1,2), (1,3), (3,4), (1,5), (5,6), (6,7)])
G.automorphism_group().order()
```

```
1
```

4. For the following two pairs of groups, compute the list of conjugacy class representatives for each group in the pair. For each part, compare and contrast the results for the two groups in the pair, with thoughtful and insightful comments.

(a) The full symmetric group on 5 symbols, S_5, and the alternating group on 5 symbols, A_5.

(b) The dihedral groups that are symmetries of a 7-gon and an 8-gon, D_7 and D_8.

Solution. Elements within a single conjugacy class will have identical cycle structure by Theorem ⟨⟨cycle structure⟩⟩. For the full symmetric group, each class will have *all* of the elements of a given cycle structure, since every permutation is available to conjugate with. However, for the alternating group, one set of elements with identical cycle structure (the five-cycles) splits into two conjugacy classes of equal sizes. This is partially explained by a "shortage" of elements to conjugate by. A more in-depth answer could explain how/why the split into the two sets happens. Why do some 5-cycles belong to one half, and not the other half?

```
G = SymmetricGroup(5)
G.conjugacy_classes_representatives()
```

```
[(), (1,2), (1,2)(3,4), (1,2,3), (1,2,3)(4,5), (1,2,3,4),
    (1,2,3,4,5)]
```

```
G = AlternatingGroup(5)
G.conjugacy_classes_representatives()
```

```
[(), (1,2)(3,4), (1,2,3), (1,2,3,4,5), (1,2,3,5,4)]
```

D_7 has non-trivial conjugacy classes of size two that are rotations paired with their inverses. One class of size 7 contains all of the reflections. For D_8 there is class of size 1 that contains the nontrivial element of the center, a half-turn rotation. Otherwise, rotations are paired with inverses. Also, the reflections split into two classes — those which fix a pair of vertices and those which do not.

```
D = DihedralGroup(7)
D.conjugacy_classes_representatives()
```

```
[(), (2,7)(3,6)(4,5), (1,2,3,4,5,6,7), (1,3,5,7,2,4,6),
    (1,4,7,3,6,2,5)]
```

```
D = DihedralGroup(8)
D.conjugacy_classes_representatives()
```

```
[(), (2,8)(3,7)(4,6), (1,2)(3,8)(4,7)(5,6), (1,2,3,4,5,6,7,8),
 (1,3,5,7)(2,4,6,8), (1,4,7,2,5,8,3,6), (1,5)(2,6)(3,7)(4,8)]
```

5. Use the command `graphs.CubeGraph(4)` to build the four-dimensional cube graph, Q_4. Using a plain `.plot()` command (without a spring layout) should create a nice plot. Construct the automorphism group of the graph, which will provide a group action on the vertex set.

(a) Construct the orbits of this action, and comment.

(b) Construct a stabilizer of a single vertex (which is a subgroup of the full automorphism group) and then consider the action of *this* group on the vertex set. Construct the orbits of this new action, and comment carefully and fully on your observations, especially in terms of the vertices of the graph.

Solution. The group is **transitive**, so we say the graph is **vertex-transitive**.

```
C = graphs.CubeGraph(4)
A = C.automorphism_group()
A.orbits()
```

```
[['0000', '0001', '0010', '0100',
  '0011', '1000', '0101', '1001',
  '0110', '1010', '0111', '1100',
  '1011', '1101', '1110', '1111']]
```

The graph is **distance-transitive**: it is vertex-transitive and the orbits of a stabilizer are distance sets.

```
S = A.stabilizer('0000')
S.orbits()
```

```
[['0000'],
 ['0001', '0010', '0100', '1000'],
 ['0011', '0101', '1001', '0110', '1010', '1100'],
 ['0111', '1011', '1101', '1110'],
 ['1111']]
```

6. Build the graph given by the commands below. The result should be a symmetric-looking graph with an automorphism group of order 16.

```
G = graphs.CycleGraph(8)
G.add_edges([(0,2),(1,3),(4,6),(5,7)])
G.plot()
```

Repeat the two parts of the previous exercise, but realize that in the second part there are now two different stabilizers to create, so build both and compare the differences in the stabilizers and their orbits. Creating a second plot with `G.plot(layout='planar')` might provide extra insight.

Solution.

```
A = G.automorphism_group()
A.order()
```

```
16
```

```
A.orbits()
```

```
[[0, 3, 4, 7],
 [1, 2, 5, 6]]
```

Notice that the orbits of the stabilizers below are partitions that have different sequences of part sizes.

```
S = A.stabilizer(0)
S.orbits()
```

```
[[0], [1, 2], [3], [4], [5, 6], [7]]
```

```
S = A.stabilizer(1)
S.orbits()
```

```
[[0, 3], [1], [2], [4, 7], [5, 6]]
```

Chapter 15

The Sylow Theorems

15.3 Exercises

1. What are the orders of all Sylow p-subgroups where G has order 18, 24, 54, 72, and 80?

Hint. If $|G| = 18 = 2 \cdot 3^2$, then the order of a Sylow 2-subgroup is 2, and the order of a Sylow 3-subgroup is 9.

Solution. If $|G| = 18 = 2 \cdot 3^2$, then the order of a Sylow 2-subgroup is 2, and the order of a Sylow 3-subgroup is 9. If $|G| = 54 = 2 \cdot 3^3$, then the order of a Sylow 2-subgroup is 2, and the order of a Sylow 3-subgroup is 27. If $|G| = 72 = 2^3 \cdot 3^2$, then the order of a Sylow 2-subgroup is 8, and the order of a Sylow 3-subgroup is 9. If $|G| = 80 = 2^4 \cdot 5$, then the order of a Sylow 2-subgroup is 16, and the order of a Sylow 5-subgroup is 5.

2. Find all the Sylow 3-subgroups of S_4 and show that they are all conjugate.

Hint. The four Sylow 3-subgroups of S_4 are $P_1 = \{(1), (123), (132)\}$, $P_2 = \{(1), (124), (142)\}$, $P_3 = \{(1), (134), (143)\}$, $P_4 = \{(1), (234), (243)\}$.

Solution. The four Sylow 3-subgroups of S_4 are $P_1 = \{(1), (123), (132)\}$, $P_2 = \{(1), (124), (142)\}$, $P_3 = \{(1), (134), (143)\}$, $P_4 = \{(1), (234), (243)\}$.

3. Show that every group of order 45 has a normal subgroup of order 9.

Solution. Since $|G| = 3^2 \cdot 5 = 45$, G has only a single Sylow 3-subgroup by the Third Sylow Theorem. This subgroup must be normal.

4. Let H be a Sylow p-subgroup of G. Prove that H is the only Sylow p-subgroup of G contained in $N(H)$.

Solution. Since $N(H) = \{g \in G : gHg^{-1} = H\}$, this follows directly from the Second Sylow Theorem.

5. Prove that no group of order 96 is simple.

Hint. Since $|G| = 96 = 2^5 \cdot 3$, G has either one or three Sylow 2-subgroups by the Third Sylow Theorem. If there is only one subgroup, we are done. If there are three Sylow 2-subgroups, let H and K be two of them. Therefore, $|H \cap K| \geq 16$; otherwise, HK would have $(32 \cdot 32)/8 = 128$ elements, which is impossible. Thus, $H \cap K$ is normal in both H and K since it has index 2 in both groups.

Solution. Since $|G| = 96 = 2^5 \cdot 3$, G has either one or three Sylow 2-subgroups by the Third Sylow Theorem. If there is only one subgroup, we are done. If there are three Sylow 2-subgroups, let H and K be two of them. Therefore, $|H \cap K| \geq 16$; otherwise, HK would have $(32 \cdot 32)/8 = 128$ elements, which is impossible. Thus, $H \cap K$ is normal in both H and K since it has index 2 in

both groups. Hence, $N(H \cap K)$ contains both H and K. Therefore, $|N(H \cap K)|$ must be a multiple of 32 greater than 1 and still divide 96, so $N(H \cap K) = G$.

6. Prove that no group of order 160 is simple.

Solution. Since $|G| = 160 = 2^5 \cdot 5$, G has either one or five Sylow 2-subgroups by the Third Sylow Theorem. If there is only one subgroup, we are done. If there are five Sylow 2-subgroups, let H and K be two of them and let $N = H \cap K$. Then $|N|$ must be a factor of 32 since the order of any Sylow 2-subgroup is 32. Since

$$160 = |G| \geq |HK| = \frac{|H||K|}{|N|} = \frac{1024}{|N|},$$

$|N|$ is either 8 or 16.

If $|N| = 16$, then N is normal in both H and K, since the index of N in both groups is 2. Thus, H and K are both in $N_G(N)$, the normalizer of N in G. Consequently,

$$160 = |G| \geq |N_G(N)| \geq |HK| = \frac{|H||K|}{|N|} = \frac{1024}{16} = 64 = 2^6.$$

Since $N_G(N)$ contains both H and K, subgroups of maximal order of the form 2^k, we know that $N_G(N) = G$.

If $|N| = 8$, then we can find subgroups H' and K' of order 16 such that $N \subset H' \subset H$ and $N \subset K' \subset K$. Since $[H' : N] = 2$, H' is in the normalizer of N. Similarly, K' is in the normalizer of N. Therefore.

$$160 = |G| \geq |N_G(N)| \geq |H'K'| = \frac{|H'||K'|}{|N|} = \frac{256}{8} = 32 = 2^5.$$

Since $N_G(N)$ is a factor of 160 and a multiple of 32, we know that $|N_G(N)| = 32$ or 160. If $|N_G(N)| = 160$, then $N_G(N) = G$ and we are done. If $|N_G(N)| = 32$, then $N_G(N)$ must be a Sylow 2-subgroup of G, say N'. Both H' and K' have index 2 in N' must therefore be normal subgroups of N'. Hence, $N' \subset N_G(H')$ and $H \subset N_G(H')$. Therefore,

$$160 \geq |N_G(H')| \geq |N'H| = \frac{|N||H|}{|N' \cap H|} = \frac{1024}{8} = 128.$$

Since $|N_G(H')|$ must be a factor of 160, if follows that $N_G(H') = G$ and H' is a normal subgroup of G.

7. If H is a normal subgroup of a finite group G and $|H| = p^k$ for some prime p, show that H is contained in every Sylow p-subgroup of G.

Solution. Since H is certainly contained in some Sylow p-subgroup of G. Since H is a normal subgroup and all Sylow p-subgroups are conjugate, it follows that H must be contained in every Sylow p-subgroup of G.

8. Let G be a group of order p^2q^2, where p and q are distinct primes such that $q \nmid p^2 - 1$ and $p \nmid q^2 - 1$. Prove that G must be abelian. Find a pair of primes for which this is true.

Hint. Show that G has a normal Sylow p-subgroup of order p^2 and a normal Sylow q-subgroup of order q^2.

Solution. For example, we can let $p = 5$ and $q = 7$. Suppose that G has a Sylow q-subgroup of order q^2. Since the number of such subgroups is congruent to 1 modulo q and divides p^2q^2, there must be either 1, p, or p^2 Sylow q-subgroups. Since $q \nmid p^2 - 1 = (p-1)(p+1)$, there can be only one Sylow

q-subgroup, say Q. Similarly, we can show that there is a single Sylow p-subgroup P. Therefore, both P and Q are normal in G. Every element in Q other than the identity has order q or q^2, so $P \cap Q = \{e\}$. Let $h \in P$ and $k \in Q$. Then

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in P \cap Q,$$

and $hk = kh$. By Theorem 9.27 $G \cong P \times Q$. By Corollary 14.16 both P and Q are abelian, so G must also be abelian.

9. Show that a group of order 33 has only one Sylow 3-subgroup.

Solution. By the Third Sylow Theorem, the number of Sylow 3-subgroups must be $1, 4, 7, 10, \ldots$. However, only 1 divides $|G| = 33$.

10. Let H be a subgroup of a group G. Prove or disprove that the normalizer of H is normal in G.

Hint. False.

Solution. False. Consider the group A_5, which is simple and has no normal subgroups.

11. Let G be a finite group divisible by a prime p. Prove that if there is only one Sylow p-subgroup in G, it must be a normal subgroup of G.

Solution. All Sylow p-subgroups are conjugate by the Second Sylow Theorem. Thus, $gPg^{-1} = P$ if P is the only Sylow p-subgroup in G.

12. Let G be a group of order p^r, p prime. Prove that G contains a normal subgroup of order p^{r-1}.

Solution. We will induct on r. If $|G| = p$, then there is nothing to prove. Suppose that $|G| = p^{r+1}$ and the result is true for all groups of order p^r and less. Let H be a subgroup of order p^r. There is an element $x \in Z(G)$ of order p (Theorem 14.15). Let $K = \langle x \rangle$. If K is not contained in H, then $K \subset N(H)$ since K is in the center of G. Hence, $N(H) \neq H$. The only possibility is that $N(H) = G$. If $K \subset H$, let $G' = G/K$ and $H' = H/K$. Then $H' \subset G'$, and we can apply the induction step since $|G'| = p^r$ and $|H'| = p^{r-1}$. That is, H' is normal in G'. If $y \in G' \setminus H'$, then $yH'y^{-1} \subset H'$. If $y = zK$, then $z \notin H$, but $zHz^{-1} \subset H$. Consequently, $z \in N(H) \setminus H$, or $N(H) = G$.

13. Suppose that G is a finite group of order $p^n k$, where $k < p$. Show that G must contain a normal subgroup.

Solution. Use induction on n.

14. Let H be a subgroup of a finite group G. Prove that $gN(H)g^{-1} = N(gHg^{-1})$ for any $g \in G$.

Solution. Follow the proof of Exercise 14.4.22 in Chapter 14.

15. Prove that a group of order 108 must have a normal subgroup.

Solution. Follow the proof in Exercise 15.3.5.

16. Classify all the groups of order 175 up to isomorphism.

Solution. If we can show that G is abelian, then we can apply the Fundamental Theorem of Finite Abelian Groups. If $|G| = 5^2 \cdot 7 = 175$, ten G has only one Sylow 5-subgroup by the Third Sylow Theorem. Similarly, the number of Sylow 7-subgroups is also 1. Let H be the unique Sylow 5-subgroup and K be the unique Sylow 7-subgroup. Both of these subgroups are abelian as well as normal. Furthermore, $H \cap K = \{e\}$. Consequently, $G \cong H \times K$ is also abelian. By the Fundamental Theorem of Finite Abelian Groups, G must be isomorphic to either $\mathbb{Z}_{175}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

17. Show that every group of order 255 is cyclic.

Hint. If G is abelian, then G is cyclic, since $|G| = 3 \cdot 5 \cdot 17$. Now look at Example 15.14.

Solution. If G is abelian, then G is cyclic, since $|G| = 3 \cdot 5 \cdot 17$. Now look at Example 15.14.

18. Let G have order $p_1^{e_1} \cdots p_n^{e_n}$ and suppose that G has n Sylow p-subgroups $P_1, \ldots, P_n$ where $|P_i| = p_i^{e_i}$. Prove that G is isomorphic to $P_1 \times \cdots \times P_n$.

Solution. Use mathematical induction on n.

19. Let P be a normal Sylow p-subgroup of G. Prove that every inner automorphism of G fixes P.

Solution. Every Sylow p-subgroup is conjugate to every other Sylow p-subgroup. Since P is normal, it must be conjugate to itself; hence, P must be fixed by any inner automorphism of G.

20. What is the smallest possible order of a group G such that G is non-abelian and $|G|$ is odd? Can you find such a group?

Solution. $|G| = 27$.

21. **The Frattini Lemma.** If H is a normal subgroup of a finite group G and P is a Sylow p-subgroup of H, for each $g \in G$ show that there is an h in H such that $gPg^{-1} = hPh^{-1}$. Also, show that if N is the normalizer of P, then $G = HN$.

Solution. If $g \in G$, then $g^{-1}Pg$ is a Sylow p-subgroup contained in H. So there exists a $h \in H$ such that $h^{-1}g^{-1}Pgh = (gh)^{-1}Pgh = P$, or $g^{-1}Pg = hPh^{-1} = (h^{-1})^{-1}P(h^{-1})$. Consequently, gh is in the normalizer N of P or $ghh^{-1} = HN$

22. Show that if the order of G is $p^n q$, where p and q are primes and $p > q$, then G contains a normal subgroup.

Solution. See Exercise 13.

23. Prove that the number of distinct conjugates of a subgroup H of a finite group G is $[G : N(H)]$.

Hint. Define a mapping between the right cosets of $N(H)$ in G and the conjugates of H in G by $N(H)g \mapsto g^{-1}Hg$. Prove that this map is a bijection.

Solution. Define a mapping between the right cosets of $N(H)$ in G and the conjugates of H in G by $N(H)g \mapsto g^{-1}Hg$. Prove that this map is a bijection.

24. Prove that a Sylow 2-subgroup of S_5 is isomorphic to D_4.

Solution. Since every Sylow 2-subgroup of S_4 has order 8 and $|D_4| = 8$, we know D_4 is also a Sylow 2-subgroup. Every other Sylow 2-subgroup of S_4 is conjugate to D_4. Any two subgroups of a group that are conjugate are isomorphic.

25. **Another Proof of the Sylow Theorems.**

(a) Suppose p is prime and p does not divide m. Show that

$$p \nmid \binom{p^k m}{p^k}.$$

(b) Let $\mathcal{S}$ denote the set of all p^k element subsets of G. Show that p does not divide $|\mathcal{S}|$.

(c) Define an action of G on $\mathcal{S}$ by left multiplication, $aT = \{at : t \in T\}$ for $a \in G$ and $T \in \mathcal{S}$. Prove that this is a group action.

(d) Prove $p \nmid |\mathcal{O}_T|$ for some $T \in \mathcal{S}$.

(e) Let $\{T_1, \ldots, T_u\}$ be an orbit such that $p \nmid u$ and $H = \{g \in G : gT_1 = T_1\}$. Prove that H is a subgroup of G and show that $|G| = u|H|$.

(f) Show that p^k divides $|H|$ and $p^k \leq |H|$.

(g) Show that $|H| = |\mathcal{O}_T| \leq p^k$; conclude that therefore $p^k = |H|$.

Solution.

(a) The expression

$$\binom{p^k m}{p^k} = \frac{p^k m(p^k m - 1) \cdots (p^k m - p^k + 1)}{p^k(p^k - 1) \cdots (p^k - p^k + 1)}$$

is a product of fractions of the type $(p^k m - j)/(p^k - j)$ except for the factor m, where $0 < j \leq p^k - 1$. If each of the factors is reduced to its lowest terms, then none will have a numerator divisible by p.

(b) Let $\mathcal{S}$ denote the set of all p^k element subsets of G. By part (a), $p \nmid |\mathcal{S}|$.

(c) The verification that aT is a group action of G on $\mathcal{S}$ is straightforward.

(d) Since $|\mathcal{S}|$ is the sum of the $|\mathcal{O}_T|$, it must be the case that $p \nmid |\mathcal{O}_T|$ for some $T \in \mathcal{S}$; otherwise, $p \nmid |\mathcal{S}|$.

(e) Let $\{T_1, \ldots, T_u\}$ be an orbit such that $p \nmid u$ and $H = \{g \in G : gT_1 = T_1\}$. Then H is the stabilizer subgroup of T_1. By Theorem 14.3, $|G| = u|H|$.

(f) Since p^k divides the order of G and does not divide u, it must be the case that $p^k \mid |H|$. Hence, $p^k \leq |H|$.

(g) Since H fixes T_1, H acts on T_1. Let $t \in T_1$. The stabilizer subgroup of t, H_t, is $\{e\}$. Thus, $|H| = |\mathcal{O}_t| \leq p^k$, and $p^k = |H|$.

26. Let G be a group. Prove that $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ is a normal subgroup of G and G/G' is abelian. Find an example to show that $\{aba^{-1}b^{-1} : a, b \in G\}$ is not necessarily a group.

Hint. Let $aG', bG' \in G/G'$. Then $(aG')(bG') = abG' = ab(b^{-1}a^{-1}ba)G' = (abb^{-1}a^{-1})baG' = baG'$.

Solution. Let $aG', bG' \in G/G'$. Then $(aG')(bG') = abG' = ab(b^{-1}a^{-1}ba)G' = (abb^{-1}a^{-1})baG' = baG'$.

15.6 Sage Exercises

1. This exercise verifies Theorem 15.13. The commutator subgroup is computed with the permutation group method `.commutator()`. For the dihedral group of order 40, D_{20} (`DihedralGroup(20)` in Sage), compute the commutator subgroup and form the quotient with the dihedral group. Then verify that this quotient is abelian. Can you identify the quotient group exactly (in other words, up to isomorphism)?

Solution.

```
D = DihedralGroup(20)
C = D.commutator()
Q = D.quotient(C)
Q.is_abelian(), Q.order(), Q.is_cyclic()
```

```
(True, 4, False)
```

```
Q.is_isomorphic(KleinFourGroup())
```

```
True
```

2. For each possible prime, find all of the distinct Sylow p-subgroups of the alternating group A_5. Confirm that your results are consistent with the Third Sylow Theorem for each prime. We know that A_5 is a simple group. Explain how this would explain or predict some aspects of your answers.

Count the number of distinct elements contained in the union of all the Sylow subgroups you just found. What is interesting about this count?

Solution. We reproduce our routine to create all the Sylow p-subgroups.

```
def all_sylow(G, p):
    '''Form the set of all distinct Sylow p-subgroups of G'''
    scriptP = []
    P = G.sylow_subgroup(p)
    for x in G:
        H = P.conjugate(x)
        if not(H in scriptP):
            scriptP.append(H)
    return scriptP
```

```
A = AlternatingGroup(5)
[len(all_sylow(A, p)) for p in [2,3,5]]
```

```
[5, 10, 6]
```

Building all these subgroups and using `Set()` to combine them and eliminate duplicates will not work as you expect, since the equality used in constructing the set is not what you would expect. The Sylow 2-subgroups have pairwise intersections that are trivial, and since the other Sylow p-subgroups are cyclic of prime order, the same can be said for any pairwise intersection. So the expression below counts the size of the union of all the Sylow p-subgroups.

```
1 + 5*3 + 10*2 + 6*4 == A.order()
```

```
True
```

3. For the dihedral group D_{36} (symmetries of a 36-gon) and each possible prime, determine the possibilities for the number of distinct Sylow p-subgroups as predicted by the Third Sylow Theorem (15.8). Now compute the actual number of distinct Sylow p-subgroups for each prime and comment on the result.

It can be proved that *any group* with order 72 is not a simple group, using techniques such as those used in the later examples in this chapter. Discuss this result in the context of your computations with Sage.

Solution. First, what Sylow's Third Theorem predicts generally, based only on the order of the group.

```
D = DihedralGroup(36)
D.order().factor()
```

```
2^3 * 3^2
```

```
n = D.order(); p = 2
[m for m in srange(n) if m.divides(n) and m.mod(p) == 1]
```

```
[1, 3, 9]
```

```
n = D.order(); p = 3
[m for m in srange(n) if m.divides(n) and m.mod(p) == 1]
```

```
[1, 4]
```

Now, the actual situation for this group, which is consistent with the predictions above. Being non-simple does not *guarantee* a normal Sylow p-subgroup, but it is *not unexpected* to discover a normal subgroup this way (*the* Sylow 3-subgroup).

```
[len(all_sylow(D, p)) for p in [2, 3]]
```

```
[9, 1]
```

4. This exercise verifies Lemma 15.6. Let G be the dihedral group of order 36, D_{18}. Let H be the one Sylow 3-subgroup. Let K be the subgroup of order 6 generated by the two permutations `a` and `b` given below. First, form a list of the distinct conjugates of K by the elements of H, and determine the number of subgroups in this list. Compare this with the index given in the statement of the lemma, employing a single (long) statement making use of the `.order()`, `.normalizer()` and `.intersection()` methods with `G`, H and K, *only*.

```
G = DihedralGroup(18)
a = G("(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18)")
b = G("(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13)")
```

Solution.

```
G = DihedralGroup(18)
H = G.sylow_subgroup(3)
a = G("(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18)")
b = G("(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13)")
K = G.subgroup([a, b])
H.order(), K.order()
```

```
(9, 6)
```

```
conj = []
for L in [K.conjugate(x) for x in H]:
    if not(L in conj):
        conj.append(L)
len(conj)
```

```
3
```

```
H.order()/G.normalizer(K).intersection(H).order()
```

```
3
```

5. Example 15.19 shows that every group of order 48 has a normal subgroup. The dicyclic groups are an infinite family of non-abelian groups with order $4n$, which includes the quaternions (the case of $n = 2$). So the permutation group `DiCyclicGroup(12)` has order 48. Use Sage to follow the logic of the proof

in Example 15.19 and construct a normal subgroup in this group. (In other words, do not just ask for a list of the normal subgroups from Sage, but instead trace through the implications in the example to arrive at a normal subgroup, and then check your answer.)

Solution.

```
G = DiCyclicGroup(12)
S = all_sylow(G, 2)
len(S)
```

```
3
```

```
L = S[0].intersection(S[1])
L.order()
```

```
8
```

```
L.is_normal(G)
```

```
True
```

6. The proofs of the Second and Third Sylow Theorems (15.7, 15.8) employ a group action on sets of Sylow p-subgroups, For the Second Theorem, the list is proposed as incomplete and is proved to be *all* of the Sylow p-subgroups. In this exercise we will see how these actions behave, and how they are different when we use different groups acting on the same set.

Construct the six Sylow 5-subgroups of the alternating group A_5. This will be the set of objects for both of our actions. Conjugating one of these Sylow 5-subgroups by an element of A_5 will produce another Sylow 5-subgroup, and so can be used to create a group action. For such an action, from each group element form a Sage permutation of the subgroups by numbering the six subgroups and using these integers as markers for the subgroups. You will find the Python list method `.index()` very helpful. Now use all of these permutations to generate a permutation group (a subgroup of S_6). Finally, use permutation group methods for orbits and stabilisers, etc. to explore the actions.

For the first action, use all of A_5 as the group. Show that the resulting action is transitive. In other words, there is exactly one single orbit.

For the second action, use just one of the Sylow 5-subgroups as the group. Write the class equation for this action in a format that suggests the "congruent to 1 mod p" part of the conclusion of the Third Theorem.

Solution. The groups and the set for the actions.

```
A = AlternatingGroup(5)
P = A.sylow_subgroup(5)
scriptP = all_sylow(A, 5)
len(scriptP)
```

```
6
```

The action of the entire group will be transitive, this is a translation of the conclusion of the Second Theorem.

```
S6 = SymmetricGroup(srange(6))
gens = []
for x in A:
    perm = [scriptP.index(H.conjugate(x)) for H in scriptP]
```

```
    gens.append(S6(perm))
V = S6.subgroup(gens)
V.orbits()
```

```
[[0, 1, 2, 3, 4, 5]]
```

We get a "finer" partition when the action uses a subgroup. We could choose *any* one of the six Sylow 5-subgroups – we use `P` from above.

```
S6 = SymmetricGroup(srange(6))
gens = []
for x in P:
    perm = [scriptP.index(H.conjugate(x)) for H in scriptP]
    gens.append(S6(perm))
V = S6.subgroup(gens)
V.orbits()
```

```
[[0], [1, 2, 3, 4, 5]]
```

Here the class equation would be expressed as

$$6 = 1 + 5^1$$

Send us more descriptive examples if you know them. More than two orbits, powers of the prime greater than 1 and if possible, different powers of the prime for the different non-singleton orbits (is this impossible?).

Chapter 16

Rings

16.6 Exercises

1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) $7\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

(e) $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

(g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$

(h) $\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

Hint. (a) $7\mathbb{Z}$ is a ring but not a field; (c) $\mathbb{Q}(\sqrt{2})$ is a field; (f) R is not a ring.

Solution.

(a) $7\mathbb{Z}$ is a ring but not a field.

(b) $\mathbb{Z}_{18}$ is a ring but not a field.

(c) $\mathbb{Q}(\sqrt{2})$ is a field.

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a field.

(e) $\mathbb{Z}[\sqrt{3}]$ is a ring but not a field.

(f) R is not a ring.

(g) $\mathbb{Z}[i]$ is a ring but not a field.

(h) $\mathbb{Q}(\sqrt[3]{3})$ is a field.

2. Let R be the ring of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a subring S of R with an identity.

Solution. The ring consisting of matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

has identity

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

3. List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$

Hint. (a) $\{1, 3, 7, 9\}$; (c) $\{1, 2, 3, 4, 5, 6\}$; (e)

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}.$$

Solution.

(a) $\{1, 3, 7, 9\}$.

(b) $\{1, 5, 7, 11\}$.

(c) $\{1, 2, 3, 4, 5, 6\}$.

(d) $SL_2(\mathbb{Z})$.

(e)

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}.$$

4. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

(c) $\mathbb{M}_2(\mathbb{R})$, the 2×2 matrices with entries in $\mathbb{R}$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{Q}$

Hint. (a) $\{0\}$, $\{0, 9\}$, $\{0, 6, 12\}$, $\{0, 3, 6, 9, 12, 15\}$, $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$; (c) there are no nontrivial ideals.

Solution.

(a) $\{0\}$, $\{0, 9\}$, $\{0, 6, 12\}$, $\{0, 3, 6, 9, 12, 15\}$, $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$.

(b) $\{0\}$, $\{0, 5, 10, 15, 20\}$.

(c) There are no nontrivial ideals.

(d) $\mathbb{M}(n\mathbb{Z})$.

(e) There are no nontrivial ideals.

5. For each of the following rings R with ideal I, give an addition table and a multiplication table for R/I.

(a) $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$

(b) $R = \mathbb{Z}_{12}$ and $I = \{0, 3, 6, 9\}$

Solution.

(a)

$+$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$1+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$
$2+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$
$3+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$
$4+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$
$5+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$

$\cdot$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$0+6\mathbb{Z}$
$1+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$2+6\mathbb{Z}$	$0+6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$	$0+6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$3+6\mathbb{Z}$	$0+6\mathbb{Z}$	$3+6\mathbb{Z}$	$0+6\mathbb{Z}$	$3+6\mathbb{Z}$	$0+6\mathbb{Z}$	$3+6\mathbb{Z}$
$4+6\mathbb{Z}$	$0+6\mathbb{Z}$	$4+6\mathbb{Z}$	$2+6\mathbb{Z}$	$0+6\mathbb{Z}$	$4+6\mathbb{Z}$	$2+6\mathbb{Z}$
$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$5+6\mathbb{Z}$	$4+6\mathbb{Z}$	$3+6\mathbb{Z}$	$2+6\mathbb{Z}$	$1+6\mathbb{Z}$

(b)

$+$	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$1+I$	$2+I$
$1+I$	$1+I$	$2+I$	$0+I$
$2+I$	$2+I$	$0+I$	$1+I$

and

$\cdot$	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$
$2+I$	$0+I$	$2+I$	$1+I$

6. Find all homomorphisms $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

Solution. Solution needed.

7. Prove that $\mathbb{R}$ is not isomorphic to $\mathbb{C}$.

Hint. Assume there is an isomorphism $\phi : \mathbb{C} \to \mathbb{R}$ with $\phi(i) = a$.

Solution. Assume there is an isomorphism $\phi : \mathbb{C} \to \mathbb{R}$ with $\phi(i) = a$.

8. Prove or disprove: The ring $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is isomorphic to the ring $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

Hint. False. Assume there is an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ such that $\phi(\sqrt{2}) = a$.

Solution. False. Assume there is an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ such that $\phi(\sqrt{2}) = a + b\sqrt{3}$. Since

$$2 = 1 + 1$$

$$\begin{aligned}
&= \phi(1) + \phi(1) \\
&= \phi(1+1) \\
&= \phi(2) \\
&= \phi(\sqrt{2}\sqrt{2}\,) \\
&= \phi(\sqrt{2}\,)\phi(\sqrt{2}\,) \\
&= (a + b\sqrt{3}\,)^2 \\
&= (a^2 + 3b^2) + 2ab\sqrt{3},
\end{aligned}$$

we know that $ab = 0$ and $a^2 + 3b^2 = 2$. Therefore, either $a = 0$ or $b = 0$. Therefore, either $a^2 = 2$ or $3b^2 = 2$. Since neither of these two equations have rational solutions, we cannot have an isomorphism $\phi : \mathbb{Q}(\sqrt{2}\,) \to \mathbb{Q}(\sqrt{3}\,)$.

9. What is the characteristic of the field formed by the set of matrices

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

with entries in $\mathbb{Z}_2$?

Solution. The characteristic is 2

10. Define a map $\phi : \mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Show that ϕ is an isomorphism of $\mathbb{C}$ with its image in $\mathbb{M}_2(\mathbb{R})$.

Solution. The proof of this exercise is straightforward using the definition of an isomorphism.

11. Prove that the Gaussian integers, $\mathbb{Z}[i]$, are an integral domain.

Solution. Let $z = a + bi$ and $w = c + di$ with $z \neq 0$. If

$$zw = (ac - bd) + (ad + bc)i = 0,$$

then

$$\begin{aligned}
ac - bd &= 0 \\
ad + bc &= 0.
\end{aligned}$$

Consequently,

$$0 = ad + bc = abd + b^2c = a^2c + b^2c = (a^2 + b^2)c;$$

hence, $c = 0$. Similarly,

$$0 = ad + bc = a^2d + abc = a^2d + b^2d = (a^2 + b^2)d,$$

and $d = 0$. Therefore, $w = c + di = 0$ is not a zero divisor.

12. Prove that $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ is an integral domain.

Solution. If $a + b\sqrt{3}\,i \neq 0$ and

$$(a + b\sqrt{3}\,i)(c + d\sqrt{3}\,i) = (ac - 3bd) + (ad + bc)\sqrt{3}\,i = 0,$$

then $ac - 3bd = 0$ and $ad + bc = 0$. Hence, $a(c^2 + 3d^2) = 0$ and $b(c^2 + 4d^2) = 0$. If $a \neq 0$, the first equation tells us that $c = d = 0$. If $b \neq 0$, the second equation says that $c = d = 0$. In either case $\mathbb{Z}[\sqrt{3}\,i]$ has no zero divisors.

13. Solve each of the following systems of congruences.

(a)

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 6 \pmod{11} \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 5 \pmod{15} \end{aligned}$$

(c)

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 7 \\ x &\equiv 7 \pmod 9 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

(d)

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 1 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

Hint. (a) $x \equiv 17 \pmod{55}$; (c) $x \equiv 214 \pmod{2772}$.

Solution.

(a) $x \equiv 17 \pmod{55}$.

(b) $x \equiv 80 \pmod{840}$.

(c) $x \equiv 214 \pmod{2772}$.

(d) $x \equiv 408 \pmod{5720}$.

14. Use the method of parallel computation outlined in the text to calculate $2234 + 4121$ by dividing the calculation into four separate additions modulo 95, 97, 98, and 99.

Solution. Solve the following system for x using Euclid's algorithm.

$$\begin{aligned} x &\equiv 2234 + 4121 \equiv 49 + 36 \equiv 85 \pmod{95} \\ x &\equiv 2234 + 4121 \equiv 3 + 47 \equiv 50 \pmod{97} \\ x &\equiv 2234 + 4121 \equiv 78 + 5 \equiv 83 \pmod{98} \\ x &\equiv 2234 + 4121 \equiv 56 + 62 \equiv 19 \pmod{99}. \end{aligned}$$

15. Explain why the method of parallel computation outlined in the text fails for $2134 \cdot 1531$ if we attempt to break the calculation down into two smaller calculations modulo 98 and 99.

Solution. The numbers are too large.

16. If R is a field, show that the only two ideals of R are $\{0\}$ and R itself.

Hint. If $I \neq \{0\}$, show that $1 \in I$.

Solution. If $I \neq \{0\}$, choose a nonzero element $a \in I$. It follows that $aa^{-1} = 1 \in I$. Hence, every element $r \in R$ must be in I, since $r = r1 \in I$.

17. Let a be any element in a ring R with identity. Show that $(-1)a = -a$.

Solution. Since $a + (-1)a = a(1 + (-1)) = 0$, we have $(-1)a = -a$.

18. Let $\phi : R \to S$ be a ring homomorphism. Prove each of the following statements.

(a) If R is a commutative ring, then $\phi(R)$ is a commutative ring.

(b) $\phi(0) = 0$.

(c) Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.

(d) If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.

Hint. (a) $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

Solution.

(a) $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

(b) $\phi(0) = \phi(a - a) = \phi(a) - \phi(a) = 0$.

(c) Since $\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R)$, $\phi(1_R) = 1_S$.

(d) From Part (a) we know that $\phi(R)$ is commutative. Since $1_S = \phi(1_R) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$, the inverse of $\phi(a)$ is $\phi(a^{-1})$.

19. Prove that the associative law for multiplication and the distributive laws hold in R/I.

Solution. For associativity,

$$\begin{aligned}(a+I)[(b+I)(c+I)] &= (a+I)(bc+I)\\ &= abc+I\\ &= (ab+I)(c+I)\\ &= [(a+I)(b+I)](c+I).\end{aligned}$$

To show left distribution,

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)[(b+c)+I]\\ &= a(b+c)+I\\ &= ab+ac+I\\ &= (ab+I)+(bc+I)\\ &= (a+I)(b+I)+(a+I)(c+I).\end{aligned}$$

Right distribution is proved the same way.

20. Prove the Second Isomorphism Theorem for rings: Let I be a subring of a ring R and J an ideal in R. Then $I \cap J$ is an ideal in I and

$$I/I \cap J \cong I + J/J.$$

Solution. The Second Isomorphism Theorem already holds for abelian groups. All that is needed to do here is to check that multiplication works.

21. Prove the Third Isomorphism Theorem for rings: Let R be a ring and I and J be ideals of R, where $J \subset I$. Then

$$R/I \cong \frac{R/J}{I/J}.$$

Solution. The Third Isomorphism Theorem already holds for abelian groups. All that is needed to do here is to check that multiplication works.

22. Prove the Correspondence Theorem: Let I be an ideal of a ring R. Then $S \to S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R correspond to ideals of R/I.

Solution. The Correspondence Theorem already holds for abelian groups. All that is needed to do here is to check that multiplication works.

23. Let R be a ring and S a subset of R. Show that S is a subring of R if and only if each of the following conditions is satisfied.

(a) $S \neq \emptyset$.

(b) $rs \in S$ for all $r, s \in S$.

(c) $r - s \in S$ for all $r, s \in S$.

Solution. Assume conditions (a)–(c) are satisfied. Conditions (a) and (c) imply that S is an abelian group. The associative and distributive law for multiplication follow from condition (b), and fact that S is an abelian group. The converse is clear.

24. Let R be a ring with a collection of subrings $\{R_\alpha\}$. Prove that $\bigcap R_\alpha$ is a subring of R. Give an example to show that the union of two subrings is not necessarily a subring.

Solution. Since 0 is in each R_α, $\bigcap R_\alpha$ is nonempty. If $a, b \in R_\alpha$ for each α, then $a - b, ab \in R_\alpha$ for each α. This is true since every R_α is a subring of R. Thus, $a - b, ab \in \bigcap R_\alpha$. Apply Exercise 16.6.23. $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a ring.

25. Let $\{I_\alpha\}_{\alpha \in A}$ be a collection of ideals in a ring R. Prove that $\bigcap_{\alpha \in A} I_\alpha$ is also an ideal in R. Give an example to show that if I_1 and I_2 are ideals in R, then $I_1 \cup I_2$ may not be an ideal.

Solution. Follow the proof in Exercise 16.6.24. The same counterexample works.

26. Let R be an integral domain. Show that if the only ideals in R are $\{0\}$ and R itself, R must be a field.

Hint. Let $a \in R$ with $a \neq 0$. Then the principal ideal generated by a is R. Thus, there exists a $b \in R$ such that $ab = 1$.

Solution. Let $a \in R$ with $a \neq 0$. Then the principal ideal generated by a is R. Thus, there exists a $b \in R$ such that $ab = 1$.

27. Let R be a commutative ring. An element a in R is **nilpotent** if $a^n = 0$ for some positive integer n. Show that the set of all nilpotent elements forms an ideal in R.

Solution. If $a^m = 0$ and $b^n = 0$, we can use the binomial theorem to show that $(a + b)^{mn} = 0$. For any $r \in R$, $(ra)^m = r^m a^m = r^m 0 = 0$.

28. A ring R is a **Boolean ring** if for every $a \in R$, $a^2 = a$. Show that every Boolean ring is a commutative ring.

Hint. Compute $(a + b)^2$ and $(-ab)^2$.

Solution. Compute $(a + b)^2$ and $(-ab)^2$.

29. Let R be a ring, where $a^3 = a$ for all $a \in R$. Prove that R must be a commutative ring.

Solution. If $b \in R$ and $b^2 = 0$, then $b = 0$. If $a^3 = a$, then $a^4 = a^2$. Thus, $(a^2b - a^2ba^2)^2 = 0$ or $a^2b = a^2ba^2$. Similarly, $ba^2 = a^2ba^2$. Consequently, $a^2b = ba^2$ for all a and b in R. From this we can show that $2ab = 2ba$. Next, show that $a + a^2 = a + 3a^2 + 3a + a^2$, and so $3(a + a^2)b = b3(a + a^2)$ or $3ab = 3ba$. Commutativity follows.

30. Let R be a ring with identity 1_R and S a subring of R with identity 1_S. Prove or disprove that $1_R = 1_S$.

Solution. See Exercise 18.

31. If we do not require the identity of a ring to be distinct from 0, we will not have a very interesting mathematical structure. Let R be a ring such that $1 = 0$. Prove that $R = \{0\}$.

Solution. For any element $a \in R$, we have $a = 1a = 0a = 0$.

32. Let S be a nonempty subset of a ring R. Prove that there is a subring R' of R that contains S.

Solution. Let $\{R_\alpha\}$ be the set of all subrings of R containing S. This collection is nonempty, since it contains S. Define $R' = \cap_\alpha R_\alpha$.

33. Let R be a ring. Define the **center** of R to be

$$Z(R) = \{a \in R : ar = ra \text{ for all } r \in R\}.$$

Prove that $Z(R)$ is a commutative subring of R.

Solution. The center of a ring is not empty since it contains 0. If $a, b \in Z(R)$, then $a - b$ and ab are in $Z(R)$, since $(a + b)r = ar - br = ra - rb = r(a - b)$ and $r(ab) = arb = (ab)r$. Since everything in the center of a ring commutes with all elements of the ring, it must be the case that $ab = ba$.

34. Let p be prime. Prove that

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z} \text{ and } \gcd(b, p) = 1\}$$

is a ring. The ring $\mathbb{Z}_{(p)}$ is called the **ring of integers localized at** p.

Hint. Let $a/b, c/d \in \mathbb{Z}_{(p)}$. Then $a/b + c/d = (ad + bc)/bd$ and $(a/b) \cdot (c/d) = (ac)/(bd)$ are both in $\mathbb{Z}_{(p)}$, since $\gcd(bd, p) = 1$.

Solution. Let $a/b, c/d \in \mathbb{Z}_{(p)}$. Then $a/b + c/d = (ad + bc)/bd$ and $(a/b) \cdot (c/d) = (ac)/(bd)$ are both in $\mathbb{Z}_{(p)}$, since $\gcd(bd, p) = 1$.

35. Prove or disprove: Every finite integral domain is isomorphic to $\mathbb{Z}_p$.

Solution. True.

36. Let R be a ring with identity.

(a) Let u be a unit in R. Define a map $i_u : R \to R$ by $r \mapsto uru^{-1}$. Prove that i_u is an automorphism of R. Such an automorphism of R is called an inner automorphism of R. Denote the set of all inner automorphisms of R by $\text{Inn}(R)$.

(b) Denote the set of all automorphisms of R by $\text{Aut}(R)$. Prove that $\text{Inn}(R)$ is a normal subgroup of $\text{Aut}(R)$.

(c) Let $U(R)$ be the group of units in R. Prove that the map

$$\phi : U(R) \to \text{Inn}(R)$$

defined by $u \mapsto i_u$ is a homomorphism. Determine the kernel of ϕ.

(d) Compute $\text{Aut}(\mathbb{Z})$, $\text{Inn}(\mathbb{Z})$, and $U(\mathbb{Z})$.

Solution.

(a) The map i_u is a ring homomorphism, since

$$i_u(r + s) = u(r + s)u^{-1} = uru^{-1} + usu^{-1} = i_u(r) + i_u(s),$$

and

$$i_u(rs) = u(rs)u^{-1} = uru^{-1}usu^{-1} = i_u(r)i_u(s).$$

To show that i_u is one-to-one, let $i_u(r) = i_u(s)$. Then $uru^{-1} = usu^{-1}$, or $r = s$. The fact that i_u is onto follows from $i_u(u^{-1}ru) = uu^{-1}ruu^{-1}$.

(b) If $\phi \in \mathrm{Aut}(R)$ and $i_u \in \mathrm{Inn}(R)$, then

$$\begin{aligned}(\phi i_u \phi^{-1})(r) &= (\phi i_u)(\phi^{-1}(r)) \\ &= (\phi)(u\phi^{-1}(r)u^{-1}) \\ &= \phi(u)\phi(\phi^{-1}(r))\phi(u^{-1}) \\ &= \phi(u)r[\phi(u)]^{-1} \\ &= i_{\phi(u)}(r).\end{aligned}$$

(c) If $\phi : U(R) \to \mathrm{Inn}(R)$ is defined by $u \mapsto i_u$, then

$$\begin{aligned}\phi(uv)(r) &= i_{uv}(r) \\ &= (uv)r(uv)^{-1} \\ &= u(vrv^{-1})u^{-1} \\ &= i_u(vrv^{-1}) \\ &= i_u i_v(r) \\ &= \phi(u)\phi(v)(r).\end{aligned}$$

The kernel of ϕ is the center of R.

(d) $U(\mathbb{Z}) = \{\pm 1\}$, $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}\}$, $\mathrm{Inn}(\mathbb{Z}) = \{\mathrm{id}\}$.

37. Let R and S be arbitrary rings. Show that their Cartesian product is a ring if we define addition and multiplication in $R \times S$ by

(a) $(r, s) + (r', s') = (r + r', s + s')$

(b) $(r, s)(r', s') = (rr', ss')$

Solution. From group theory $R \times S$ is an abelian group. It is straightforward to very the associative property for multiplication as well as the distributive property for $R \times S$.

38. An element x in a ring is called an **idempotent** if $x^2 = x$. Prove that the only idempotents in an integral domain are 0 and 1. Find a ring with a idempotent x not equal to 0 or 1.

Hint. Suppose that $x^2 = x$ and $x \neq 0$. Since R is an integral domain, $x = 1$. To find a nontrivial idempotent, look in $\mathbb{M}_2(\mathbb{R})$.

Solution. Suppose that $x^2 = x$ and $x \neq 0$. Since R is an integral domain, $x = 1$. To find a nontrivial idempotent, look in $\mathbb{M}_2(\mathbb{R})$.

39. Let $\gcd(a, n) = d$ and $\gcd(b, d) \neq 1$. Prove that $ax \equiv b \pmod{n}$ does not have a solution.

Solution. Look at the proof of (6) in Proposition 3.1.

40. **The Chinese Remainder Theorem for Rings.** Let R be a ring and I and J be ideals in R such that $I + J = R$.

(a) Show that for any r and s in R, the system of equations

$$\begin{aligned}x &\equiv r \pmod{I} \\ x &\equiv s \pmod{J}\end{aligned}$$

has a solution.

(b) In addition, prove that any two solutions of the system are congruent modulo $I \cap J$.

(c) Let I and J be ideals in a ring R such that $I + J = R$. Show that there exists a ring isomorphism

$$R/(I \cap J) \cong R/I \times R/J.$$

Solution. For (a) and (b) follow the proof of Lemma 15.18. To prove (c), Define a map $\phi : R \to R/I \times R/J$ by $r \mapsto (r + I, r + J)$. Show that is map is a surjective homomorphism with kernel $I \cap J$.

16.9 Sage Exercises

1. Define the two rings $\mathbb{Z}_{11}$ and $\mathbb{Z}_{12}$ with the commands `R = Integers(11)` and `S = Integers(12)`. For each ring, use the relevant command to determine: if the ring is finite, if it is commutative, if it is an integral domain and if it is a field. Then use single Sage commands to find the order of the ring, list the elements, and output the multiplicative identity (i.e. 1, if it exists).

2. Define `R` to be the ring of integers, $\mathbb{Z}$, by executing `R = ZZ` or `R = Integers()`. A command like `R.ideal(4)` will create the principal ideal $\langle 4 \rangle$. The same command can accept more than one generator, so for example, `R.ideal(3, 5)` will create the ideal $\{a \cdot 3 + b \cdot 5 \mid a, b \in \mathbb{Z}\}$. Create several ideals of $\mathbb{Z}$ with two generators and ask Sage to print each as you create it. Explain what you observe and then create code that will test your observation for thousands of different examples.

Solution.

```
R = Integers()
all([R.ideal([a,b]) == R.ideal([gcd(a,b)]) for a in range(1,
    200) for b in range(1, 200)])
```

```
True
```

3. Create a finite field F of order 81 with `F.<t>=FiniteField(3^4)`.

(a) List the elements of F.

(b) Obtain the generators of F with `F.gens()`.

(c) Obtain the first generator of F and save it as `u` with `u = F.0` (alternatively, `u = F.gen(0)`).

(d) Compute the first 80 powers of `u` and comment.

(e) The generator you have worked with above is a root of a polynomial over $\mathbb{Z}_3$. Obtain this polynomial with `F.modulus()` and use this observation to explain the entry in your list of powers that is the fourth power of the generator.

Solution.

```
F.<t> = FiniteField(81)
u = F.gen(0)
cyclic = [u^i for i in range(1, 81)]
F.list() == [F(0)] + cyclic
```

```
True
```

4. Build and analyze a quotient ring as follows:

(a) Use `P.<z>=Integers(7)[]` to construct a ring P of polynomials in z with coefficients from $\mathbb{Z}_7$.

(b) Use `K = P.ideal(z^2+z+3)` to build a principal ideal K generated by the polynomial $z^2 + z + 3$.

(c) Use `H = P.quotient(K)` to build H, the quotient ring of P by K.

(d) Use Sage to verify that H is a field.

(e) As in the previous exercise, obtain a generator and examine the proper collection of powers of that generator.

Solution.

```
P.<z> = Integers(7)[]
K = P.ideal(z^2+z+3)
H = P.quotient(K)
H.is_field()
```

```
True
```

Note that `.list()` is not implmenented for this quotient construction.

```
H.list()
```

```
Traceback (most recent call last):
...
NotImplementedError: object does not support iteration
```

```
u = H.gen(0)
cyclic = [u^i for i in range(1, 7^2)]
cyclic
```

```
[zbar, 6*zbar + 4, 5*zbar + 3, 5*zbar + 6,
zbar + 6, 5*zbar + 4, 6*zbar + 6, 3, 3*zbar,
4*zbar + 5, zbar + 2, zbar + 4, 3*zbar + 4,
zbar + 5, 4*zbar + 4, 2, 2*zbar, 5*zbar + 1,
3*zbar + 6, 3*zbar + 5, 2*zbar + 5, 3*zbar + 1,
5*zbar + 5, 6, 6*zbar, zbar + 3, 2*zbar + 4,
2*zbar + 1, 6*zbar + 1, 2*zbar + 3, zbar + 1,
4, 4*zbar, 3*zbar + 2, 6*zbar + 5, 6*zbar + 3,
4*zbar + 3, 6*zbar + 2, 3*zbar + 3, 5, 5*zbar,
2*zbar + 6, 4*zbar + 1, 4*zbar + 2, 5*zbar + 2,
4*zbar + 6, 2*zbar + 2, 1]
```

Chapter 17

Polynomials

17.4 Exercises

1. List all of the polynomials of degree 3 or less in $\mathbb{Z}_2[x]$.

Solution. There are 16 possible polynomials: $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, where a_i is equal to 0 or 1.

2. Compute each of the following.

(a) $(5x^2 + 3x - 4) + (4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(b) $(5x^2 + 3x - 4)(4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(c) $(7x^3 + 3x^2 - x) + (6x^2 - 8x + 4)$ in $\mathbb{Z}_9$

(d) $(3x^2 + 2x - 4) + (4x^2 + 2)$ in $\mathbb{Z}_5$

(e) $(3x^2 + 2x - 4)(4x^2 + 2)$ in $\mathbb{Z}_5$

(f) $(5x^2 + 3x - 2)^2$ in $\mathbb{Z}_{12}$

Hint. (a) $9x^2 + 2x + 5$; (b) $8x^4 + 7x^3 + 2x^2 + 7x$.

Solution.

(a) $9x^2 + 2x + 5$

(b) $8x^4 + 7x^3 + 2x^2 + 7x$

(c) $7x^3 + 4$

(d) $2x^2 + 2x + 3$

(e) $2x^4 + 3x^3 + 4x + 2$

(f) $x^4 + 6x^3 + x^2 + 4$

3. Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$ for each of the following pairs of polynomials.

(a) $a(x) = 5x^3 + 6x^2 - 3x + 4$ and $b(x) = x - 2$ in $\mathbb{Z}_7[x]$

(b) $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_7[x]$

(c) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$

(d) $a(x) = x^5 + x^3 - x^2 - x$ and $b(x) = x^3 + x$ in $\mathbb{Z}_2[x]$

Hint. (a) $5x^3+6x^2-3x+4 = (5x^2+2x+1)(x-2)+6$; (c) $4x^5-x^3+x^2+4 = (4x^2+4)(x^3+3)+4x^2+2$.

Solution.

(a) $5x^3 + 6x^2 - 3x + 4 = (5x^2 + 2x + 1)(x - 2) + 6$

(b) $6x^4 - 2x^3 + x^2 - 3x + 1 = (6x^2 + 6x)(x^2 + x - 2) + (2x + 1)$

(c) $4x^5 - x^3 + x^2 + 4 = (4x^2 + 4)(x^3 + 3) + 4x^2 + 2$

(d) $x^5 + x^3 - x^2 - x = (x^3 + x)(x^2) + (x^2 + x)$

4. Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \gcd(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $a(x)p(x) + b(x)q(x) = d(x)$.

(a) $p(x) = x^3 - 6x^2 + 14x - 15$ and $q(x) = x^3 - 8x^2 + 21x - 18$, where $p(x), q(x) \in \mathbb{Q}[x]$

(b) $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$, where $p(x), q(x) \in \mathbb{Z}_2[x]$

(c) $p(x) = x^3 + x^2 - 4x + 4$ and $q(x) = x^3 + 3x - 2$, where $p(x), q(x) \in \mathbb{Z}_5[x]$

(d) $p(x) = x^3 - 2x + 4$ and $q(x) = 4x^3 + x + 3$, where $p(x), q(x) \in \mathbb{Q}[x]$

Solution.

(a) $(-(2/15)x + 3/5)p(x) + ((2/15)x - 1/3)q(x) = x - 1$

(b) $(x^2 + x + 1)p(x) + x^2q(x) = 1$

(c) $(4x^2 + x)p(x) + (x^2 + 2)q(x) = 1$

(d) $((484/2887)x^2-(140/2887)x+925/2887)p(x)+(-(121/2887)x^2+(277/2887)x-271/2887)q(x) = 1$. You may find Sage useful here.

5. Find all of the zeros for each of the following polynomials.

(a) $5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}$

(b) $3x^3 - 4x^2 - x + 4$ in $\mathbb{Z}_5$

(c) $5x^4 + 2x^2 - 3$ in $\mathbb{Z}_7$

(d) $x^3 + x + 1$ in $\mathbb{Z}_2$

Hint. (a) No zeros in $\mathbb{Z}_{12}$; (c) 3, 4.

Solution.

(a) No zeros in $\mathbb{Z}_{12}$.

(b) No zeros in $\mathbb{Z}_5$.

(c) 3, 4

(d) No zeros in $\mathbb{Z}_2$

6. Find all of the units in $\mathbb{Z}[x]$.

Solution. The units are the constant polynomials 1 and -1.

7. Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\deg p(x) > 1$.

Hint. Look at $(2x + 1)$.

Solution. The polynomial $(2x + 1)$ is a unit since $(2x + 1)^2 = 1$.

8. Which of the following polynomials are irreducible over $\mathbb{Q}[x]$?

(a) $x^4 - 2x^3 + 2x^2 + x + 4$ (c) $3x^5 - 4x^3 - 6x^2 + 6$

(b) $x^4 - 5x^3 + 3x - 2$ (d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

Hint. (a) Reducible; (c) irreducible.

Solution.

(a) Reducible

(b) Irreducible

(c) Irreducible

(d) Irreducible

9. Find all of the irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$.

Solution. The irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$ are $x^2 + x + 1$, $x^3 + x + 1$, and $x^3 + x^2 + 1$.

10. Give two different factorizations of $x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

Hint. One factorization is $x^2 + x + 8 = (x + 2)(x + 9)$.

Solution. $x^2 + x + 8 = (x + 2)(x + 9) = (x + 7)(x + 4)$.

11. Prove or disprove: There exists a polynomial $p(x)$ in $\mathbb{Z}_6[x]$ of degree n with more than n distinct zeros.

Solution. True, the degree of the polynomial $p(x) = x^2 + 5x$ is 2, but $p(x)$ has zeros $x = 0, 1, 3, 4$.

12. If F is a field, show that $F[x_1, \ldots, x_n]$ is an integral domain.

Solution. Use mathematical induction.

13. Show that the division algorithm does not hold for $\mathbb{Z}[x]$. Why does it fail?

Hint. The integers $\mathbb{Z}$ do not form a field.

Solution. The division algorithm fails because $\mathbb{Z}$ is not a field. It is easy to find counterexamples. For example, if $f(x) = x^2 + 1$ and $g(x) = 2x - 1$, it is impossible to find polynomials $q(x), r(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)q(x) + r(x)$.

14. Prove or disprove: $x^p + a$ is irreducible for any $a \in \mathbb{Z}_p$, where p is prime.

Hint. False.

Solution. False. Consider $x^2 + 1 = (x + 1)(x + 1)$ in the polynomial ring $\mathbb{Z}_2[x]$.

15. Let $f(x)$ be irreducible in $F[x]$, where F is a field. If $f(x) \mid p(x)q(x)$, prove that either $f(x) \mid p(x)$ or $f(x) \mid q(x)$.

Solution. If $f(x)$ does not divide $p(x)$, then $r(x)f(x)+s(x)p(x) = 1$ for some polynomials $r(x)$ and $s(x)$. So

$$q(x) = q(x)[r(x)f(x) + s(x)p(x)] = f(x)[q(x)r(x)] + s(x)[p(x)q(x)].$$

Since $f(x)$ divides both terms on the right-hand side of the equation, $f(x)$ must also divide $q(x)$.

16. Suppose that R and S are isomorphic rings. Prove that $R[x] \cong S[x]$.

Hint. Let $\phi : R \to S$ be an isomorphism. Define $\overline{\phi} : R[x] \to S[x]$ by $\overline{\phi}(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$.

Solution. Let $\phi : R \to S$ be an isomorphism. Define $\overline{\phi} : R[x] \to S[x]$ by $\overline{\phi}(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$.

17. Let F be a field and $a \in F$. If $p(x) \in F[x]$, show that $p(a)$ is the remainder obtained when $p(x)$ is divided by $x - a$.

Solution. By the division algorithm, $p(a) = (a-a)q(a) + r = r$.

18. **The Rational Root Theorem.** Let

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$. Prove that if $p(r/s) = 0$, where $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

Solution. Multiplying both sides of

$$p\left(\frac{r}{s}\right) = a_n \left(\frac{r}{s}\right)^n a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0 \tag{17.1}$$

by s^n, we obtain

$$r(a_n r^{n-1} + a_{n-1}sr^{n-2} + \cdots + a_1 s^{n-1}) = -a_0 s^n.$$

Thus, r divides $a_0 s^n$ and must also divide a_0, since $\gcd(r, s) = 1$. Similarly, if we can rewrite equation (17.1) to obtain

$$s(a_{n-1}r^{n-1} + a_{n-2}sr^{n-2} + \cdots + a_0 s^{n-1}) = -a_n r^n,$$

and it follows that s divides a_n. The Rational Root Theorem can also be proven using Gauss's Lemma.

19. Let $\mathbb{Q}^*$ be the multiplicative group of positive rational numbers. Prove that $\mathbb{Q}^*$ is isomorphic to $(\mathbb{Z}[x], +)$.

Solution. List the primes in order, $p_1, p_2, \ldots$. Any element in $\mathbb{Q}^*$ can be written as $p_{i_1}^{e_{i_1}} p_{i_2}^{e_{i_2}} \cdots p_{i_k}^{e_{i_k}}$, where p_i is prime and e_i is in $\mathbb{Z}$. The proper group homomorphism is the one that sends $p_i^{e_i}$ to $e_i x^i$.

20. **Cyclotomic Polynomials.** The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the **cyclotomic polynomial.** Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

Hint. The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the **cyclotomic polynomial.** Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

Solution. Define $g(x)$ by $g(x) = \Phi_p(x+1)$ and show that $g(x)$ is irreducible over $\mathbb{Q}$.

21. If F is a field, show that there are infinitely many irreducible polynomials in $F[x]$.

Solution. If F is infinite, then there an infinite number of linear polynomials. If F is finite, follow the proof of the Fundamental Theorem of Arithmetic. That is, suppose that there are only a finite number of irreducible polynomials, say $p_1(x), \ldots, p_k(x)$. Show that $p(x) = p_1(x) \cdots p_k(x) + 1$ is irreducible.

22. Let R be a commutative ring with identity. Prove that multiplication is commutative in $R[x]$.

Solution. Let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$. Then

$$\begin{aligned} p(x)q(x) &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \\ &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_{i-j} b_j \right) x^i \\ &= q(x)p(x). \end{aligned}$$

23. Let R be a commutative ring with identity. Prove that multiplication is distributive in $R[x]$.

Solution. Let $p(x) = \sum_{i=0}^{m} a_i x^i$, $q(x) = \sum_{j=0}^{n} b_j x^j$, and $r(x) = \sum_{k=0}^{p} c_k x^k$. Then

$$\begin{aligned} p(x)(q(x) + r(x)) &= \sum_{i=0}^{m} a_i x^i \left(\sum_{j=0}^{n} b_j x^j + \sum_{k=0}^{p} c_k x^k \right) \\ &= \sum_{i=0}^{m} a_i x^i \left(\sum_{j=0}^{\max(n,p)} (b_j + c_j) x^i \right) \\ &= \sum_{i=0}^{m+\max(n,p)} \left(\sum_{j=0}^{i} a_j (b_{i-j} + c_{i-j}) \right) x^i \\ &= \sum_{i=0}^{m+\max(n,p)} \left(\sum_{j=0}^{i} a_j b_{i-j} + \sum_{j=0}^{i} a_j c_{i-j} \right) x^i \\ &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) + \sum_{i=0}^{m+p} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \\ &= p(x)q(x) + p(x)r(x). \end{aligned}$$

24. Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$, for any prime p. Conclude that

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Solution. To show that $x^p - x$ has p distinct zeros, we must show that every element of $\mathbb{Z}_p$ is a zero of $x^p - x$. Certainly, 0 is a zero of $x^p - x = x(x^{p-1} - 1)$. The order of the multiplicative group of nonzero elements of $\mathbb{Z}_p$ is $p-1$, so if α is a nonzero element of $\mathbb{Z}_p$, then $\alpha^{p-1} = 1$.

25. Let F be a field and $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be in $F[x]$. Define $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ to be the **derivative** of $f(x)$.

(a) Prove that

$$(f+g)'(x) = f'(x) + g'(x).$$

Conclude that we can define a homomorphism of abelian groups $D : F[x] \to F[x]$ by $D(f(x)) = f'(x)$.

(b) Calculate the kernel of D if $\operatorname{char} F = 0$.

(c) Calculate the kernel of D if $\operatorname{char} F = p$.

(d) Prove that

$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

(e) Suppose that we can factor a polynomial $f(x) \in F[x]$ into linear factors, say

$$f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n).$$

Prove that $f(x)$ has no repeated factors if and only if $f(x)$ and $f'(x)$ are relatively prime.

Solution.

(a) If $f(x) = \sum a_i x^i$ and $g(x) = \sum b_j x^j$, then $D(f(x)) = \sum i a_i x^{i-1}$ and $D(g(x)) = \sum j b_j x^{j-1}$, and

$$D(f(x)+g(x)) = D\left(\sum a_i x^i + \sum b_j x^j\right) = D\left(\sum (a_i + b_i) x^i\right) = \sum i(a_i+b_i)x^{i-1}.$$

(b) All constant polynomials.

(c) Polynomials in x^p.

(d) By part (a), it is enough to show that $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$ for $f(x) = x^m$ and $g(x) = x^n$.

(e) Suppose that we can factor a polynomial $f(x) \in F[x]$ into linear factors, say

$$f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n),$$

with $a_i \neq a_j$ for $i \neq j$. Then

$$\begin{aligned} f'(x) = a[&(x - a_2) \cdots (x - a_n) \\ &+ (x - a_1)(x - a_3) \cdots (x - a_n) \\ &+ \cdots + (x - a_1) \cdots (x - a_{n-1})]. \end{aligned}$$

Hence, $f(x)$ and $f'(x)$ can have no common factors. To prove the converse, we will show that the contrapositive of the statement is true. Suppose that $f(x) = (x - a)^k g(x)$, where $k > 1$. Differentiating, we have

$$f'(x) = k(x - a)^{k-1} g(x) + (x - a)^k g'(x).$$

Therefore, $f(x)$ and $f'(x)$ have a common factor.

26. Let F be a field. Show that $F[x]$ is never a field.

Hint. Find a nontrivial proper ideal in $F[x]$.

Solution. The ideal generated by x is a nontrivial proper ideal in $F[x]$. Since the only proper ideal in a field is the zero ideal, $F[x]$ cannot be a field.

27. Let R be an integral domain. Prove that $R[x_1, \ldots, x_n]$ is an integral domain.

Solution. Use Proposition 17.2 and mathematical induction. Finish the proof.

28. Let R be a commutative ring with identity. Show that $R[x]$ has a subring R' isomorphic to R.

Solution. Prove that the subring of constant polynomials of $R[x]$ is isomorphic to R.

29. Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is a commutative ring with identity. Prove that $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

Solution. Let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$ be polynomials in $R[x]$. We may assume that $m \geq n$. The highest power of x that can occur in $p(x) + q(x)$ is then m. Therefore, $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

17.7 Sage Exercises

1. Consider the polynomial $x^3 - 3x + 4$. Compute the most thorough factorization of this polynomial over each of the following fields: (a) the finite field $\mathbb{Z}_5$, (b) a finite field with 125 elements, (c) the rationals, (d) the real numbers and (e) the complex numbers. To do this, build the appropriate polynomial ring, and construct the polynomial as a member of this ring, and use the `.factor()` method.

Solution. The polynomial is irreducible over the finite field of size 5 and the rationals. Over the other three fields it factors. Notice that for the finite field of order 125 there are two different generators: one for the finite field and one for the polynomial ring. We consistently define and re-use `x` as the variable of the polynomial ring, and consistently redefine the polynomial.

```
R = Integers(5)
P.<x> = R[]
p = x^3 - 3*x + 4
p.factor()
```

```
x^3 + 2*x + 4
```

```
R.<a> = GF(5^3)
P.<x> = R[]
p = x^3 - 3*x + 4
p.factor()
```

```
(x + 3*a) * (x + a^2 + 2*a + 2) * (x + 4*a^2 + 3)
```

```
R = QQ
P.<x> = R[]
p = x^3 - 3*x + 4
p.factor()
```

```
x^3 - 3*x + 4
```

The rather complicated expressions confirm a factorization into a linear term and a quadratic term.

```
R = RR
P.<x> = R[]
p = x^3 - 3*x + 4
p.factor()[0][0].degree(), p.factor()[1][0].degree()
```

```
(1, 2)
```

And over the complexes, the quadratic term factors further.

```
R = CC
P.<x> = R[]
p = x^3 - 3*x + 4
fact = p.factor()
[p.factor()[i][0].degree() for i in range(3)]
```

```
[1, 1, 1]
```

2. "Conway polynomials" are irreducible polynomials over $\mathbb{Z}_p$ that Sage (and other software) uses to build maximal ideals in polynomial rings, and thus quotient rings that are fields. Roughly speaking, they are "canonical"

choices for each degree and each prime. The command `conway_polynomial(p, n)` will return a database entry that is an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Execute the command `conway_polynomial(5, 4)` to obtain an allegedly irreducible polynomial of degree 4 over $\mathbb{Z}_5$: $p = x^4 + 4x^2 + 4x + 2$. Construct the right polynomial ring (i.e., in the indeterminate x) and verify that `p` is really an element of your polynomial ring.

First determine that p has no linear factors. The only possibility left is that `p` factors as two quadratic polynomials over $\mathbb{Z}_5$. Use a list comprehension with *three* `for` statements to create *every* possible quadratic polynomial over $\mathbb{Z}_5$. Now use this list to create every possible product of two quadratic polynomials and check to see if `p` is in this list.

More on Conway polynomials is available at Frank Lübeck's site.

Solution. It is easy to end with `False` on this exercise, for the wrong reasons. So we are extra careful that our Conway polynomial is in the same polynomial ring as our quadratics and quartics.

```
p = conway_polynomial(5, 4)
Z5 = Integers(5)
R.<x> = Z5[]
p in R
```

```
True
```

No zeros, so no linear factors.

```
[p(u) for u in Z5]
```

```
[2, 1, 2, 1, 3]
```

```
quads = [a*x^2 + b*x + c for a in Z5 for b in Z5 for c in Z5]
quarts = [r*s for r in quads for s in quads]
p in quarts
```

```
False
```

3. Construct a finite field of order 729 as a quotient of a polynomial ring by a principal ideal generated with a Conway polynomial.

Solution.

```
p = conway_polynomial(3, 6)
R.<x> = Integers(3)[]
I = R.ideal([p])
F = R.quotient(I)
F.order(), F.is_field()
```

```
(729, True)
```

4. Define the polynomials $p = x^3 + 2x^2 + 2x + 4$ and $q = x^4 + 2x^2$ as polynomials with coefficients from the integers. Compute `gcd(p, q)` and verify that the result divides both `p` and `q` (just form a fraction in Sage and see that it simplifies cleanly, or use the `.quo_rem()` method).

Proposition 17.10 says there are polynomials $r(x)$ and $s(x)$ such that the greatest common divisor equals $r(x)p(x) + s(x)q(x)$, *if the coefficients come from a field*. Since here we have two polynomials over the integers, investigate the results returned by Sage for the extended gcd, `xgcd(p, q)`. In particular, show that the first result of the returned triple is a multiple of the gcd. Then verify the "linear combination" property of the result.

Solution.

```
R.<x> = ZZ[]
p = x^3 + 2*x^2 + 2*x + 4
q = x^4 + 2*x^2
g = gcd(p, q)
g
```

```
x^2 + 2
```

```
p.quo_rem(g), q.quo_rem(g)
```

```
((x + 2, 0), (x^2, 0))
```

```
r, s, t = xgcd(p, q)
r == s*p + t*q, r == 4*g
```

```
(True, True)
```

5. For a polynomial ring over a field, every ideal is principal. Begin with the ring of polynomials over the rationals. Experiment with constructing ideals using two generators and then see that Sage converts the ideal to a principal ideal with a single generator. (You can get this generator with the ideal method `.gen()`.) Can you explain how this single generator is computed?

Solution. Totally random polynomials are likely to be relatively prime, so we create a mix that will obviously contain some non-trivial common divisors. Perhaps there are better ways.

This is very similar to an earlier exercise about ideals of the integers.

```
R.<x> = QQ[]
rand = [R.random_element() for i in range(10)]
prod = [r*s for r in rand for s in rand]
all([R.ideal([p, q]) == R.ideal([gcd(p, q)]) for p in prod
    for q in prod])
```

```
True
```

Chapter 18

Integral Domains

18.3 Exercises

1. Let $z = a + b\sqrt{3}\,i$ be in $\mathbb{Z}[\sqrt{3}\,i]$. If $a^2 + 3b^2 = 1$, show that z must be a unit. Show that the only units of $\mathbb{Z}[\sqrt{3}\,i]$ are 1 and -1.

Hint. Note that $z^{-1} = 1/(a + b\sqrt{3}\,i) = (a - b\sqrt{3}\,i)/(a^2 + 3b^2)$ is in $\mathbb{Z}[\sqrt{3}\,i]$ if and only if $a^2 + 3b^2 = 1$. The only integer solutions to the equation are $a = \pm 1, b = 0$.

Solution. Note that $z^{-1} = 1/(a + b\sqrt{3}\,i) = (a - b\sqrt{3}\,i)/(a^2 + 3b^2)$ is in $\mathbb{Z}[\sqrt{3}\,i]$ if and only if $a^2 + 3b^2 = 1$. The only integer solutions to the equation are $a = \pm 1, b = 0$.

2. The Gaussian integers, $\mathbb{Z}[i]$, are a UFD. Factor each of the following elements in $\mathbb{Z}[i]$ into a product of irreducibles.

(a) 5

(b) $1 + 3i$

(c) $6 + 8i$

(d) 2

Hint. (a) $5 = -i(1 + 2i)(2 + i)$; (c) $6 + 8i = -i(1 + i)^2(2 + i)^2$.

Solution.

(a) $5 = -i(1 + 2i)(2 + i)$.

(b) $1 + 3i = (1 + i)(2 + i)$.

(c) $6 + 8i = -i(1 + i)^2(2 + i)^2$.

(d) $2 = -i(1 + i)^2$.

3. Let D be an integral domain.

(a) Prove that F_D is an abelian group under the operation of addition.

(b) Show that the operation of multiplication is well-defined in the field of fractions, F_D.

(c) Verify the associative and commutative properties for multiplication in F_D.

Solution.

(a) If $[a,b],[c,d] \in F_D$, then $[ad+bc,bd]$ is also in F_D. The additive identity is $[0,1]$. The additive inverse of $[a,b]$ is $[-a,b]$, since

$$[a,b]+[-a,b] = [ab-ab,b^2] = [0,b^2] = [0,1].$$

Associativity follows from

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

(b) To show that multiplication is well-defined, let $[a,b]=[a',b']$ and $[c,d]=[c',d']$. Then $ab'=a'b$ and $cd'=c'd$. Consequently, $ab'cd'=a'bc'd$ or $[ac,bd]=[a'c',b'd']$.

(c) For commutativity and associativity, observe that

$$[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b]$$

and

$$([a,b][c,d])[e,f] = [ac,bd][e,f] = [ace,bdf] = [a,b][ce,df] = [a,b]([c,d][d,f]).$$

4. Prove or disprove: Any subring of a field F containing 1 is an integral domain.

Hint. True.

Solution. Suppose that D is a subring of F containing 1. We need only show that cancellation holds. Suppose that $ab=ac$ for $a,b,c \in D$, where $a \neq 0$. Since $ab=ac$ makes sense in F, we can multiply both sides of this equation by a^{-1} to obtain $b=c$.

5. Prove or disprove: If D is an integral domain, then every prime element in D is also irreducible in D.

Solution. Let R be a subring of $\mathbb{F}$ and suppose that $ab=0$ for $a,b \in R$. Then $a,b \in \mathbb{F}$. So if $a \neq 0$, it must be the case that $b=0$. Therefore, R is a commutative ring containing $1 \neq 0$ and no zero divisors.

6. Let F be a field of characteristic zero. Prove that F contains a subfield isomorphic to $\mathbb{Q}$.

Solution. Define a ring homomorphism $\phi : \mathbb{Z} \to F$ and show that $\ker\phi = \{0\}$. By the First Isomorphism Theorem for Rings, $\phi(\mathbb{Z})/\ker\phi \cong \mathbb{Z}$. Use the fact that the smallest field containing $\mathbb{Z}$ is $\mathbb{Q}$.

7. Let F be a field.

(a) Prove that the field of fractions of $F[x]$, denoted by $F(x)$, is isomorphic to the set all rational expressions $p(x)/q(x)$, where $q(x)$ is not the zero polynomial.

(b) Let $p(x_1,\ldots,x_n)$ and $q(x_1,\ldots,x_n)$ be polynomials in $F[x_1,\ldots,x_n]$. Show that the set of all rational expressions $p(x_1,\ldots,x_n)/q(x_1,\ldots,x_n)$ is isomorphic to the field of fractions of $F[x_1,\ldots,x_n]$. We denote the field of fractions of $F[x_1,\ldots,x_n]$ by $F(x_1,\ldots,x_n)$.

Solution. For Part (a), apply Theorem 18.4. For Part (b), use mathematical induction.

8. Let p be prime and denote the field of fractions of $\mathbb{Z}_p[x]$ by $\mathbb{Z}_p(x)$. Prove that $\mathbb{Z}_p(x)$ is an infinite field of characteristic p.

Solution. Use the fact that there are an infinite number of polynomials in $\mathbb{Z}_p[x]$.

9. Prove that the field of fractions of the Gaussian integers, $\mathbb{Z}[i]$, is

$$\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}.$$

Hint. Let $z = a + bi$ and $w = c + di \neq 0$ be in $\mathbb{Z}[i]$. Prove that $z/w \in \mathbb{Q}(i)$.

Solution. Let $z = a+bi$ and $w = c+di \neq 0$ be in $\mathbb{Z}[i]$. Prove that $z/w \in \mathbb{Q}(i)$.

10. A field F is called a **prime field** if it has no proper subfields. If E is a subfield of F and E is a prime field, then E is a **prime subfield** of F.

(a) Prove that every field contains a unique prime subfield.

(b) If F is a field of characteristic 0, prove that the prime subfield of F is isomorphic to the field of rational numbers, $\mathbb{Q}$.

(c) If F is a field of characteristic p, prove that the prime subfield of F is isomorphic to $\mathbb{Z}_p$.

Solution.

(a) Let $\{F_\alpha\}$ be the collection of all subfields of F. Show that $E \cap_\alpha F_\alpha$ is a field.

(b) Look at Exercise 5.

(c) Using the fact that $\ker \phi = p\mathbb{Z}$, follow the proof of (b).

11. Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Prove that $\mathbb{Z}[\sqrt{2}\,]$ is an integral domain.

(b) Find all of the units in $\mathbb{Z}[\sqrt{2}\,]$.

(c) Determine the field of fractions of $\mathbb{Z}[\sqrt{2}\,]$.

(d) Prove that $\mathbb{Z}[\sqrt{2}i]$ is a Euclidean domain under the Euclidean valuation $\nu(a + b\sqrt{2}\,i) = a^2 + 2b^2$.

Solution.

(a) Let $(a + b\sqrt{2}\,)(c + d\sqrt{2}\,) = 0$. If $a + b\sqrt{2} \neq 0$, it is a straight forward computation to show that $c + d\sqrt{2} = 0$.

(b) ± 1, $\pm(\pm 1 \pm \sqrt{2}\,)^n$.

(c) $\mathbb{Q}(\sqrt{2}\,)$

(d) If $x = a + b\sqrt{2}\,i$ and $y = c + d\sqrt{2}\,i$, then

$$xy = (ac - 2bd) + (ad + bc)\sqrt{2}\,i;$$

consequently,

$$\nu(xy) = (ac - 2bd)^2 + 2(ad + bc)^2$$

$$\begin{aligned} &= (a^2 + 2b^2)(c^2 + 2d^2) \\ &= \nu(x)\nu(y) \\ &\geq \nu(x). \end{aligned}$$

If $x, y \in \mathbb{Z}[\sqrt{2}\,i]$ with $y \neq 0$, follow the proof in Example 8 to show that there exist $q, r \in \mathbb{Z}[\sqrt{2}\,i]$ such that $x = qy + r$, where either $r = 0$ or $\nu(r) < \nu(y)$.

12. Let D be a UFD. An element $d \in D$ is a **greatest common divisor of a and b in D** if $d \mid a$ and $d \mid b$ and d is divisible by any other element dividing both a and b.

(a) If D is a PID and a and b are both nonzero elements of D, prove there exists a unique greatest common divisor of a and b up to associates. That is, if d and d' are both greatest common divisors of a and b, then d and d' are associates. We write $\gcd(a, b)$ for the greatest common divisor of a and b.

(b) Let D be a PID and a and b be nonzero elements of D. Prove that there exist elements s and t in D such that $\gcd(a, b) = as + bt$.

Solution. Let I be the smallest ideal in D that contains both a and b. Since D is a PID, there exists an element $d \in D$ such that $I = \langle d \rangle$. The rest is straightforward.

13. Let D be an integral domain. Define a relation on D by $a \sim b$ if a and b are associates in D. Prove that $\sim$ is an equivalence relation on D.

Solution. The relation is reflexive, since $a = 1a$. Thus, $a \sim a$. To show that the relation is symmetric, let $a \sim b$. Then there exists a unit u in D such that $a = ub$. Since $b = u^{-1}a$, $b \sim a$. If $a \sim b$ and $b \sim c$, then there exist units $u, v \in D$ such that $a = ub$ and $b = vc$. Since $a = (uv)c$ and uv is a unit in D, $a \sim c$. Consequently, the relation is transitive.

14. Let D be a Euclidean domain with Euclidean valuation ν. If u is a unit in D, show that $\nu(u) = \nu(1)$.

Solution. Observe that $\nu(1) \leq \nu(1u) = \nu(u) \leq \nu(uu^{-1}) = \nu(1)$.

15. Let D be a Euclidean domain with Euclidean valuation ν. If a and b are associates in D, prove that $\nu(a) = \nu(b)$.

Hint. Let $a = ub$ with u a unit. Then $\nu(b) \leq \nu(ub) \leq \nu(a)$. Similarly, $\nu(a) \leq \nu(b)$.

Solution. Let $a = ub$ with u a unit. Then $\nu(b) \leq \nu(ub) \leq \nu(a)$. Similarly, $\nu(a) \leq \nu(b)$.

16. Show that $\mathbb{Z}[\sqrt{5}\,i]$ is not a unique factorization domain.

Hint. Show that 21 can be factored in two different ways.

Solution. Show that 21 can be factored in two different ways.

17. Prove or disprove: Every subdomain of a UFD is also a UFD.

Solution. False. Every field is a UFD including $\mathbb{C}$, but $\mathbb{Z}[\sqrt{3}\,i]$ is not a UFD.

18. An ideal of a commutative ring R is said to be **finitely generated** if there exist elements $a_1, \ldots, a_n$ in R such that every element $r \in R$ can be written as $a_1r_1 + \cdots + a_nr_n$ for some $r_1, \ldots, r_n$ in R. Prove that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

Solution. First suppose that R satisfies the ACC, and let I be any ideal in R. Choose a_1 in I and let I_1 be the ideal generated by a_1. If $I_1 \neq I$, then

choose $a_2 \in I \setminus I_1$ and let $I_2 = \langle a_1, a_2 \rangle$. If $I_2 \neq I$, continue in this manner to obtain a chain of ideals $I_1 \subset I_2 \subset \cdots$, where each I_k is contained in I. Since R satisfies the ACC, eventually $I = I_N = \langle a_1, \ldots, a_N \rangle$ for some N. Therefore, I is finitely generated.

Conversely, let I be finitely generated. If $I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals, then $I = \cup I_k$ is an ideal. Let $a_1, \ldots, a_n$ generate I. Each a_i is in some ideal I_{k_i} of R. If we let N be the largest k_i, then $I = I_N$.

19. Let D be an integral domain with a descending chain of ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$. Suppose that there exists an N such that $I_k = I_N$ for all $k \geq N$. A ring satisfying this condition is said to satisfy the **descending chain condition**, or **DCC**. Rings satisfying the DCC are called **Artinian rings**, after Emil Artin. Show that if D satisfies the descending chain condition, it must satisfy the ascending chain condition.

Solution. Needs solution.

20. Let R be a commutative ring with identity. We define a **multiplicative subset** of R to be a subset S such that $1 \in S$ and $ab \in S$ if $a, b \in S$.

(a) Define a relation $\sim$ on $R \times S$ by $(a, s) \sim (a', s')$ if there exists an $s^* \in S$ such that $s^*(s'a - sa') = 0$. Show that $\sim$ is an equivalence relation on $R \times S$.

(b) Let a/s denote the equivalence class of $(a, s) \in R \times S$ and let $S^{-1}R$ be the set of all equivalence classes with respect to $\sim$. Define the operations of addition and multiplication on $S^{-1}R$ by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st},$$

respectively. Prove that these operations are well-defined on $S^{-1}R$ and that $S^{-1}R$ is a ring with identity under these operations. The ring $S^{-1}R$ is called the **ring of quotients** of R with respect to S.

(c) Show that the map $\psi : R \to S^{-1}R$ defined by $\psi(a) = a/1$ is a ring homomorphism.

(d) If R has no zero divisors and $0 \notin S$, show that ψ is one-to-one.

(e) Prove that P is a prime ideal of R if and only if $S = R \setminus P$ is a multiplicative subset of R.

(f) If P is a prime ideal of R and $S = R \setminus P$, show that the ring of quotients $S^{-1}R$ has a unique maximal ideal. Any ring that has a unique maximal ideal is called a **local ring**.

Solution.

(a) We must show that $\sim$ is reflexive, symmetric, and transitive.

- Since $1(as - sa) = 0$, $(a, s) \sim (a, s)$ and the relation is reflexive.
- If $(a, s) \sim (a', s')$, there exists an $s^* \in S$ such that $s^*(s'a - sa') = 0$. Since

$$0 = s^*(s'a - sa') = -s^*(sa' - s'a) = s^*(sa' - s'a),$$

we know that $(a', s') \sim (a, s)$ and the relation is symmetric.

- To prove transitivity, assume that $(a,s) \sim (b,t)$ and $(b,t) \sim (c,u)$. Then there exist $v, w \in S$ such that $(at-bs)v = 0$ and $(bu-ct)w = 0$. Then $atv - bsv = 0$ and $buv - ctw = 0$. Consequently, $atuv - bsuv = 0$ and $bsuw - cstw = 0$. Adding these two equations, we obtain $atuv - cstw = (au - cs)tuv = 0$, which tells us that $(a,s) \sim (c,u)$ since $tuv \in S$.

(b) Follow the proof of Lemma 18.3. To show that the operations of addition and multiplication are well-defined, let $a/s = a'/s'$ and $b/t = b'/t'$. Then there exist $r^*, s^* \in S$ such that $r^*(s'a - sa') = 0$ and $s^*(t'b - tb') = 0$. If

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at+bs}{st} \\ \frac{a'}{s'} + \frac{b'}{t'} &= \frac{a't'+b's'}{s't'}, \end{aligned}$$

then

$$\begin{aligned} r*s*[(at+bs)s't' - st(a't'+b's')] &= r^*s^*[ats't' + bss't' - sta't' - stb's'] \\ &= s^*tt'[r^*(s'a - sa')] + r^*ss'[s^*(t'b - tb')] \\ &= 0 \end{aligned}$$

and these two fractions are equivalent. Similarly, if

$$\begin{aligned} \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \\ \frac{a'}{s'} \cdot \frac{b'}{t'} &= \frac{a'b'}{s't'}, \end{aligned}$$

then

$$\begin{aligned} r^*s^*[(ab)(s't') - (st)(a'b')] &= r^*s^*[abs't' - a'bst' + a'bst' - sta'b'] \\ &= r^*s^*[bt'(as' - a's) + a's(bt' - tb')] \\ &= s^*bt'[r^*(as' - a's)] + r^*a's[s^*(bt' - tb')] \\ &= 0 \end{aligned}$$

The additive and multiplicative identities are $0/1$ and $1/1$, respectively. To show that $(0,1)$ is the additive identity, observe that

$$\frac{a}{s} + \frac{0}{1} = \frac{a1 + s0}{st} = \frac{a}{s}.$$

It is easy to show that $[1,1]$ is the multiplicative identity. The additive inverse of a/s is $-a/s$, since

$$\frac{a}{s} + \frac{-a}{s} = \frac{as - as}{s^2} = \frac{0}{1}.$$

It is straightforward to show that addition and multiplication are associative. To show the distributive property holds, observe that

$$\begin{aligned} \frac{a}{s}\frac{b}{t} + \frac{a}{s}\frac{c}{u} &= \frac{ab}{st} + \frac{ac}{su} \\ &= \frac{abu + act}{stu} \\ &= \frac{a}{s}\left(\frac{bu+ct}{tu}\right) \\ &= \frac{a}{s}\left(\frac{b}{t} + \frac{c}{u}\right). \end{aligned}$$

(c) The map $\psi : R \to S^{-1}R$ defined by $\psi(a) = a/1$ is a ring homomorphism since

$$\psi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \psi(a) + \psi(b)$$
$$\psi(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = \psi(a)\psi(b).$$

(d) If $\psi(a) = \psi(b)$, then $a/1 = b/1$. Hence, there exists an $s \in S$ such that $s(a-b) = 0$. Since R has no zero divisors and $s \neq 0$, $a - b = 0$ or $a = b$.

(e) Certainly, $1 \in S$. Let $a, b \in S$ and assume that $ab \in P$. Since P is a prime ideal, either $a \in P$ or $b \in P$, which is a contradiction.

(f) We claim that $M = \{a/s : a \in P\}$ is the unique maximal ideal in $S^{-1}R$. Suppose that I is an ideal not contained in M and let $b/t \in I$. Then $b \in S$ and $t/b \in I$. Thus, I contains a unit and $I = S^{-1}R$.

18.5 Sage Exercises

There are no Sage exercises for this section.

Chapter 19

Lattices and Boolean Algebras

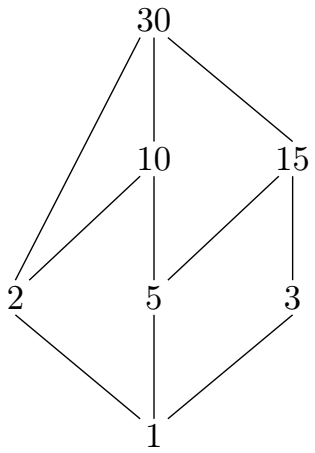
19.4 Exercises

1. Draw the lattice diagram for the power set of $X = \{a, b, c, d\}$ with the set inclusion relation, $\subset$.

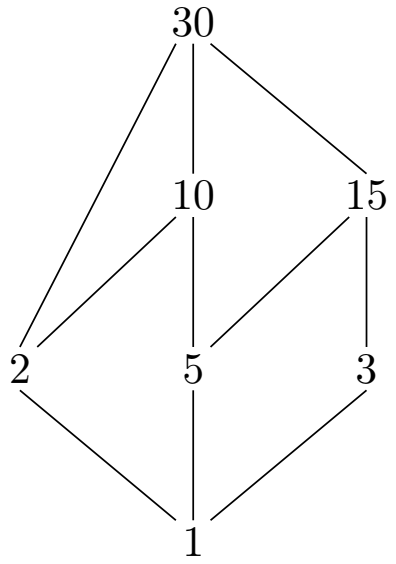
Solution. Solution needed.

2. Draw the diagram for the set of positive integers that are divisors of 30. Is this poset a Boolean algebra?

Hint.



Solution. Fix this. Missing 6.



3. Draw a diagram of the lattice of subgroups of $\mathbb{Z}_{12}$.

Solution. Solution needed.

4. Let B be the set of positive integers that are divisors of 36. Define an order on B by $a \preceq b$ if $a \mid b$. Prove that B is a Boolean algebra. Find a set X such that B is isomorphic to $\mathcal{P}(X)$.

Solution. Complete this solution. $a \vee b = \text{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$. The atoms in B are the prime numbers.

5. Prove or disprove: $\mathbb{Z}$ is a poset under the relation $a \preceq b$ if $a \mid b$.

Hint. False.

Solution. False. Complete this solution.

6. Draw the switching circuit for each of the following Boolean expressions.

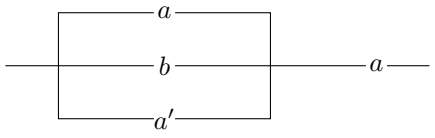
(a) $(a \vee b \vee a') \wedge a$

(b) $(a \vee b)' \wedge (a \vee b)$

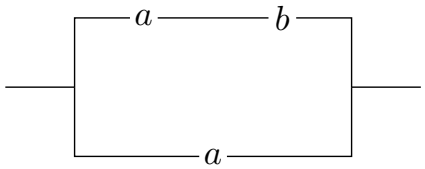
(c) $a \vee (a \wedge b)$

(d) $(c \vee a \vee b) \wedge c' \wedge (a \vee b)'$

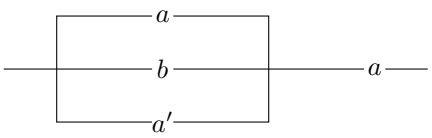
Hint. (a) $(a \vee b \vee a') \wedge a$



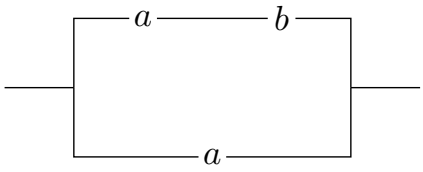
(c) $a \vee (a \wedge b)$



Solution. (a) $(a \vee b \vee a') \wedge a$



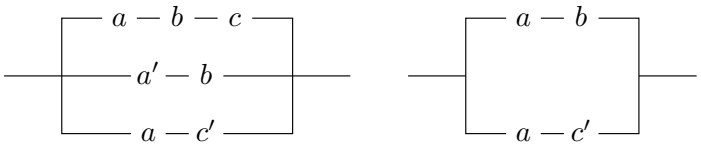
(c) $a \vee (a \wedge b)$



7. Draw a circuit that will be closed exactly when only one of three switches a, b, and c are closed.

Solution. Needs solution.

8. Prove or disprove that the two circuits shown are equivalent.



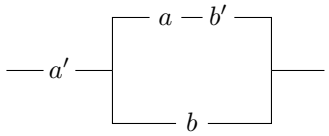
Hint. Not equivalent.

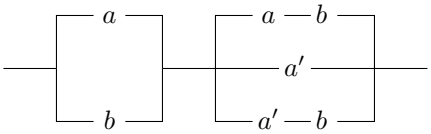
Solution. Not equivalent.

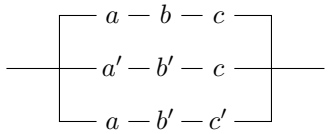
9. Let X be a finite set containing n elements. Prove that $\mathcal{P}(X) = 2^n$. Conclude that the order of any finite Boolean algebra must be 2^n for some $n \in \mathbb{N}$.

Solution. Induct on n. Finish solution.

10. For each of the following circuits, write a Boolean expression. If the circuit can be replaced by one with fewer switches, give the Boolean expression and draw a diagram for the new circuit.







Hint. (a) $a' \wedge [(a \wedge b') \vee b] = a \wedge (a \vee b)$.

Solution. (a) $a' \wedge [(a \wedge b') \vee b] = a \wedge (a \vee b)$; (b) $(a \vee b) \wedge ((a \wedge b) \vee a' \vee (a' \wedge b))$; (c) $(a \wedge b \wedge c) \vee (a' \wedge b' \wedge c) \vee (a \wedge b' \wedge c')$.

11. Prove or disprove: The set of all nonzero integers is a lattice, where $a \preceq b$ is defined by $a \mid b$.

Solution. True. The greatest lower bound of two integers a and g is their greatest common divisor. Their least upper bound is their least common multiple.

12. Let L be a nonempty set with two binary operations $\vee$ and $\wedge$ satisfying the commutative, associative, idempotent, and absorption laws. We can define a partial order on L, as in Theorem 19.14, by $a \preceq b$ if $a \vee b = b$. Prove that the greatest lower bound of a and b is $a \wedge b$.

Solution. Use the Principle of Duality.

13. Let G be a group and X be the set of subgroups of G ordered by set-theoretic inclusion. If H and K are subgroups of G, show that the least upper bound of H and K is the subgroup generated by $H \cup K$.

Solution. Use the fact that the subgroup generated by $H \cup K$ is the smallest subgroup containing both H and K.

14. Let R be a ring and suppose that X is the set of ideals of R. Show that X is a poset ordered by set-theoretic inclusion, $\subset$. Define the meet of two ideals I and J in X by $I \cap J$ and the join of I and J by $I + J$. Prove that the set of ideals of R is a lattice under these operations.

Hint. Let I, J be ideals in R. We need to show that $I + J = \{r + s : r \in I \text{ and } s \in J\}$ is the smallest ideal in R containing both I and J. If $r_1, r_2 \in I$ and $s_1, s_2 \in J$, then $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2) + (s_1 + s_2)$ is in $I + J$. For $a \in R$, $a(r_1 + s_1) = ar_1 + as_1 \in I + J$; hence, $I + J$ is an ideal in R.

Solution. Let I, J be ideals in R. We need to show that $I + J = \{r + s : r \in I \text{ and } s \in J\}$ is the smallest ideal in R containing both I and J. If $r_1, r_2 \in I$ and $s_1, s_2 \in J$, then $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2) + (s_1 + s_2)$ is in $I + J$. For $a \in R$, $a(r_1 + s_1) = ar_1 + as_1 \in I + J$; hence, $I + J$ is an ideal in R.

15. Let B be a Boolean algebra. Prove each of the following identities.

(a) $a \vee I = I$ and $a \wedge O = O$ for all $a \in B$.

(b) If $a \vee b = I$ and $a \wedge b = O$, then $b = a'$.

(c) $(a')' = a$ for all $a \in B$.

(d) $I' = O$ and $O' = I$.

(e) $(a \vee b)' = a' \wedge b'$ and $(a \wedge b)' = a' \vee b'$ (De Morgan's laws).

Solution.

(a) $a \vee I = a \vee (a \vee a') = (a \vee a) \vee a' = a \vee a' = I$ and $a \wedge O = a \wedge (a \wedge a') = (a \wedge a) \wedge a' = a \wedge a' = O$.

(b) Use Theorem 18.6 (2).

(c) Use Part (b).

(d) Use Part (b).

(e) Use Part (b).

16. By drawing the appropriate diagrams, complete the proof of Theorem 19.30 to show that the switching functions form a Boolean algebra.

Solution. The following diagram shows that $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Insert diagram

17. Let B be a Boolean algebra. Define binary operations $+$ and $\cdot$ on B by

$$a + b = (a \wedge b') \vee (a' \wedge b)$$
$$a \cdot b = a \wedge b.$$

Prove that B is a commutative ring under these operations satisfying $a^2 = a$ for all $a \in B$.

Solution. The additive and multiplicative identities are O and I, respectively. All of the ring axioms are straight forward to verify. Finally, $a^2 = a \cdot a = a \wedge a = a$ and $ab = a \wedge b = b \wedge a = ba$.

18. Let X be a poset such that for every a and b in X, either $a \preceq b$ or $b \preceq a$. Then X is said to be a **totally ordered set**.

(a) Is $a \mid b$ a total order on $\mathbb{N}$?

(b) Prove that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are totally ordered sets under the usual ordering $\leq$.

Hint. (a) No.

Solution. (a) No. (b) Apply the properties of the natural and real numbers.

19. Let X and Y be posets. A map $\phi : X \to Y$ is **order-preserving** if $a \preceq b$ implies that $\phi(a) \preceq \phi(b)$. Let L and M be lattices. A map $\psi : L \to M$ is a **lattice homomorphism** if $\psi(a \vee b) = \psi(a) \vee \psi(b)$ and $\psi(a \wedge b) = \psi(a) \wedge \psi(b)$. Show that every lattice homomorphism is order-preserving, but that it is not the case that every order-preserving homomorphism is a lattice homomorphism.

Solution. If $a \preceq b$, then $a \vee b = b$. So $\phi(a) \vee \phi(b) = \phi(a \vee b) = \phi(b)$ or $\phi(a) \preceq \phi(b)$. To show that it is not the case that every order-preserving homomorphism is a lattice homomorphism, consider the homomorphism $\phi : \mathbb{N} \to \mathbb{N}$ with orders defined by $a \preceq b$ if $a \mid b$ and the usual order of $\leq$.

20. Let B be a Boolean algebra. Prove that $a = b$ if and only if $(a \wedge b') \vee (a' \wedge b) = O$ for $a, b \in B$.

Hint. ($\Rightarrow$). $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = O \vee O = O$. ($\Leftarrow$). $(a \wedge b') \vee (a' \wedge b) = O \Rightarrow a \vee b = (a \vee a) \vee b = a \vee (a \vee b) = a \vee [I \wedge (a \vee b)] = a \vee [(a \vee a') \wedge (a \vee b)] = [a \vee (a \wedge b')] \vee [a \vee (a' \wedge b)] = a \vee [(a \wedge b') \vee (a' \wedge b)] = a \vee 0 = a$. A symmetric argument shows that $a \vee b = b$.

Solution. ($\Rightarrow$). $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = O \vee O = O$. ($\Leftarrow$). $(a \wedge b') \vee (a' \wedge b) = O \Rightarrow a \vee b = (a \vee a) \vee b = a \vee (a \vee b) = a \vee [I \wedge (a \vee b)] = a \vee [(a \vee a') \wedge (a \vee b)] = [a \vee (a \wedge b')] \vee [a \vee (a' \wedge b)] = a \vee [(a \wedge b') \vee (a' \wedge b)] = a \vee 0 = a$. A symmetric argument shows that $a \vee b = b$.

21. Let B be a Boolean algebra. Prove that $a = O$ if and only if $(a \wedge b') \vee (a' \wedge b) = b$ for all $b \in B$.

Solution. If $a = 0$, then

$$(a \wedge b') \vee (a' \wedge b) = (O \wedge b') \vee (I \wedge b) = O \vee b = b.$$

Conversely, if $(a \wedge b') \vee (a' \wedge b) = b$ for all $b \in B$, then

$$O = (a \wedge I) \vee (a' \wedge O) = a \vee O = a.$$

22. Let L and M be lattices. Define an order relation on $L \times M$ by $(a, b) \preceq (c, d)$ if $a \preceq c$ and $b \preceq d$. Show that $L \times M$ is a lattice under this partial order.

Solution. Define $(a, b) \vee (c, d)$ and $(a, b) \wedge (c, d)$ by $(a \vee c, b \vee d)$ and $(a \wedge c, b \wedge d)$, respectively.

19.7 Sage Exercises

1. Use `R = Posets.RandomPoset(30,0.05)` to construct a random poset. Use `R.plot()` to get an idea of what you have built.

(a) Illustrate the use of the poset methods: `.is_lequal()`, `.is_less_than()`, `.is_gequal()`, and `.is_greater_than()` to determine if two specific elements (of your choice) are related or incomparable.

(b) Use `.minimal_elements()` and `.maximal_elements()` to find the smallest and largest elements of your poset.

(c) Use `LatticePoset(R)` to see if the poset `R` is a lattice by attempting to convert it into a lattice.

(d) Find a linear extension of your poset. Confirm that any pair of elements that are comparable in the poset will be similarly comparable in the linear extension.

Solution. It is highly unlikely that the random poset will actually be a lattice.

For the linear extension, any pair of elements which compare according to $\preceq$ should appear in a similar order in the list returned by the `.linear_extension()` method.

```
R = Posets.RandomPoset(30,0.05)
L = R.linear_extension()
all([L.index(a) <= L.index(b) for a in L for b in L if
    R.is_lequal(a,b)])
```

```
True
```

2. Construct the poset on the positive divisors of $72 = 2^3 \cdot 3^2$ with divisiblity as the relation, and then convert to a lattice.

(a) Determine the one and zero element using `.top()` and `.bottom()`.

(b) Determine all the pairs of elements of the lattice that are complements of each other *without* using the `.complement()` method, but rather just use the `.meet()` and `.join()` methods. Extra credit if you can output each pair just once.

(c) Determine if the lattice is distributive using just the `.meet()` and `.join()` methods, and not the `.is_distributive()` method.

Solution.

```
divisors = (72).divisors()
divisibility = lambda a, b: a.divides(b)
P = Poset([divisors, divisibility])
L = LatticePoset(P)
L
```

```
Finite lattice containing 12 elements
```

```
L.bottom(), L.top()
```

```
(1, 72)
```

```
[(x, y) for x in divisors for y in divisors
    if (x <= y) and
       L.meet(x,y) == L.bottom() and
       L.join(x,y) == L.top()]
```

```
[(1, 72), (8, 9)]
```

```
all([L.join(a, L.meet(b,c)) == L.meet(L.join(a,b),
    L.join(a,c))
         for a in divisors for b in divisors for c in
             divisors])
```

```
True
```

3. Construct several specific diamond lattices with `Posets.DiamondPoset(n)` by varying the value of `n`. Once you feel you have enough empirical evidence, give answers, with justifications, to the following questions for *general* values of n, based on observations obtained from your experiments with Sage.

(a) Which elements have complements and which do not, and why?

(b) Read the documentation of the `.antichains()` method to learn what an antichain is. How many antichains are there?

(c) Is the lattice distributive?

Solution. Elements 0 and $n-1$ are complements of each other, and for any pair of the other $n-2$ elements, each is a complement of the other. Sage returns a Python dictionary from the `.complements()` method, which we convert to a list of pairs for testing the output. (There is no guarantee a dictionary outputs its key-value pairs in the same order every time.)

```
D = LatticePoset(Posets.DiamondPoset(7))
sorted(D.complements().items())
```

```
[(0, [6]),
 (1, [2, 3, 4, 5]),
 (2, [1, 3, 4, 5]),
 (3, [1, 2, 4, 5]),
 (4, [1, 2, 3, 5]),
 (5, [1, 2, 3, 4]),
 (6, [0])]
```

Any subset (including the empty set) of the $n-2$ "middle" elements will be an antichain, as will the singletons $\{0\}$ and $\{n-1\}$, for a total of $2^{n-2}+2$ antichains, and these are all the antichains since 0 and $n-1$ are individually comparable to any other element, so can only appear in the two singletons. The `.antichains()` method produces a Python generator, so we force it to produce *all* the antichains with the `list()` function.

```
n = 7
D = LatticePoset(Posets.DiamondPoset(n))
len(list(D.antichains())) == 2^(n-2) + 2
```

```
True
```

The lattice is distributive only for small values of n and iit should be easy to describe a counterexample once there are 3 elements in the middle level.

```
[m for m in range(3,40) if
    LatticePoset(Posets.DiamondPoset(m)).is_distributive()]
```

```
[3, 4]
```

4. Use `Posets.BooleanLattice(4)` to construct an instance of the prototypical Boolean algebra on 16 elements (i.e., all subsets of a 4-set).

Then use `Posets.IntegerCompositions(5)` to construct the poset whose 16 elements are the compositions of the integer 5. We have seen above that the integer composition lattice is distributive and complemented, making it a Boolean algebra. And by Theorem 19.23 we can conclude that these two Boolean algebras are isomorphic.

Use the `.plot()` method to see the similarity visually. Then use the method `.hasse_diagram()` on each poset to obtain a directed graph (which you can also plot, though the embedding into the plane may not be as informative). Employ the graph method `.is_isomorphic()` to see that the two Hasse diagrams really are the "same."

Solution.

```
B = LatticePoset(Posets.BooleanLattice(4))
C = LatticePoset(Posets.IntegerCompositions(5))
HB = B.hasse_diagram()
HC = C.hasse_diagram()
HB.is_isomorphic(HC)
```

```
True
```

5. (Advanced) For the previous question, construct an *explicit* isomorphism between the two Boolean algebras. This would be a bijective function (constructed with the `def` command) that converts compositions into sets (or if,

you choose, sets into compositions) and which respects the meet and join operations. You can test and illustrate your function by its interaction with specific elements evaluated in the meet and join operations, as described in the definition of an isomorphism of Boolean algebras.

Solution. Any finite Boolean algebra of size 2^n can be put into a correspondence with the set of binary strings of length n. For the power set of an n-set, we can think of the ones in such a string as indicating which elements are in a given subset. For an integer composition of $n+1$ we can imagine $n+1$ ones lined up in a row, with the n gaps between adjacent ones as being numbered. Then the ones in the binary string indicate placing separators in specific gaps and adding up all the ones between separators. Complicating matters, Sage labels the elements of the Boolean algebra with the decimal value of the binary string as if it were a base 2 repesentation of an integer. So for $n = 4$, the binary string 0101 would represent the set $\{1, 3\} \subset \{0, 1, 2, 3\}$, the integer $2 + 8 = 10$ (low-order bits to the left), and the integer composition $11|11|1 = 2, 2, 1$.

The function below converts an integer element of the `BooleanLattice` into a set (list, really) by stripping off powers of 2 and recording the location. Then the list is augmented so we can compute successive differences, which is the number of ones between separators in the description of integer compositions above. This function is the explicit isomorphism.

```
def iso(x):
    aset = []
    place = 0;
    while x > 0:
        if mod(x, 2) == 1:
            x = x - 1
            aset.append(place)
        x = x/2
        place += 1
    fenced = [-1] + aset + [4]
    return [fenced[i+1] - fenced[i] for i in
        range(len(fenced)-1)]
```

The output of this function is a list, which *looks* like an integer partition, but we will need to *coerce* these lists into the Boolean algebra of intger compositions. The next bit of code sets up the Boolean algebras, the **parent** of a typical integer composition, and tests the `iso()` function.

```
B = LatticePoset(Posets.BooleanLattice(4))
C = LatticePoset(Posets.IntegerCompositions(5))
CP = parent(C[0])
CP(iso(10))
```

```
[2, 2, 1]
```

We test that the meet operation is preserved under the isomorphism. This would be easier to read, if not for the necessity of `CP`, so ignore that part if it seems in the way.

```
all([C.meet(CP(iso(a)), CP(iso(b))) == CP(iso(B.meet(a, b)))
        for a in B for b in B])
```

```
True
```

Chapter 20

Vector Spaces

20.4 Exercises

1. If F is a field, show that $F[x]$ is a vector space over F, where the vectors in $F[x]$ are polynomials. Vector addition is polynomial addition, and scalar multiplication is defined by $\alpha p(x)$ for $\alpha \in F$.

Solution. $F[x]$ is an abelian group under addition, since it is a ring. The proof that

$$\begin{aligned}\alpha(\beta p(x)) &= (\alpha\beta)p(x)\\ (\alpha+\beta)p(x)) &= \alpha p(x) + \beta p(x)\\ \alpha(p(x)+q(x)) &= \alpha p(x) + \alpha q(x)\\ 1\cdot p(x)) &= p(x)\end{aligned}$$

is straightforward.

2. Prove that $\mathbb{Q}(\sqrt{2}\,)$ is a vector space.

Solution. Note that $\mathbb{Q}(\sqrt{2}\,)$ is a subgroup of the additive group of real numbers under addition, since

$$(a+b\sqrt{2}\,) - (c+d\sqrt{2}\,) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}\,).$$

In addition,

$$\begin{aligned}\alpha(\beta(a+b\sqrt{2}\,)) &= (\alpha\beta)(a+b\sqrt{2})\\ (\alpha+\beta)(a+b\sqrt{2}\,) &= \alpha(a+b\sqrt{2}) + \beta(a+b\sqrt{2})\\ \alpha[(a+b\sqrt{2}) + (c+d\sqrt{2}\,)] &= \alpha(a+b\sqrt{2}) + \alpha(c+d\sqrt{2})\\ 1\cdot(a+b\sqrt{2}\,) &= a+b\sqrt{2}.\end{aligned}$$

3. Let $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ be the field generated by elements of the form $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, where a,b,c,d are in $\mathbb{Q}$. Prove that $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ is a vector space of dimension 4 over $\mathbb{Q}$. Find a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$.

Hint. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\,\}$ over $\mathbb{Q}$.

Solution. $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ has basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\,\}$ over $\mathbb{Q}$.

4. Prove that the complex numbers are a vector space of dimension 2 over $\mathbb{R}$.

Solution. The complex numbers form an abelian group under addition, since they are a field. In addition,

$$\alpha(\beta(a+bi)) = (\alpha\beta)(a+bi)$$

$$(\alpha+\beta)(a+bi) = \alpha(a+bi)+\beta(a+bi)$$
$$\alpha[(a+bi)+(c+di)] = \alpha(a+bi)+\alpha(c+di)$$
$$1\cdot(a+bi) = a+bi.$$

A basis for $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$

5. Prove that the set P_n of all polynomials of degree less than n form a subspace of the vector space $F[x]$. Find a basis for P_n and compute the dimension of P_n.

Hint. The set $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for P_n.

Solution. The set $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for P_n.

6. Let F be a field and denote the set of n-tuples of F by F^n. Given vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in F^n and α in F, define vector addition by

$$u + v = (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

and scalar multiplication by

$$\alpha u = \alpha(u_1, \ldots, u_n) = (\alpha u_1, \ldots, \alpha u_n).$$

Prove that F^n is a vector space of dimension n under these operations.

Solution. Since F is an abelian group under addition, F^n must also be an abelian group under addition. It is a straightforward task to verify the remaining vector space axioms. A basis for F^n can be given by

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1).\}$$

7. Which of the following sets are subspaces of $\mathbb{R}^3$? If the set is indeed a subspace, find a basis for the subspace and compute its dimension.

(a) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2 + x_3 = 0\}$

(b) $\{(x_1, x_2, x_3) : 3x_1 + 4x_3 = 0, 2x_1 - x_2 + x_3 = 0\}$

(c) $\{(x_1, x_2, x_3) : x_1 - 2x_2 + 2x_3 = 2\}$

(d) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2^2 = 0\}$

Hint. (a) Subspace of dimension 2 with basis $\{(1, 0, -3), (0, 1, 2)\}$; (d) not a subspace

Solution.

(a) Subspace of dimension 2 with basis $\{(1, 0, -3), (0, 1, 2)\}$.

(b) Subspace of dimension 1 with basis $\{(-4, -5, 3)\}$.

(c) Not a subspace.

(d) Not a subspace.

8. Show that the set of all possible solutions $(x, y, z) \in \mathbb{R}^3$ of the equations

$$Ax + By + Cz = 0$$
$$Dx + Ey + Cz = 0$$

form a subspace of $\mathbb{R}^3$.

Solution. If (x_1, y_1, z_1) and (x_2, y_2, z_2) satisfy the equations of the equations

$$Ax + By + Cz = 0$$
$$Dx + Ey + Cz = 0,$$

then $(x_1 + x_2, y_1 + y_2, z_1 + z_2)$ and $(\alpha x_1, \alpha y_1, \alpha z_1)$ satisfy the same equations. Therefore, the set of solutions to this system is a subspace of $\mathbb{R}^3$.

9. Let W be the subset of continuous functions on $[0, 1]$ such that $f(0) = 0$. Prove that W is a subspace of $C[0, 1]$.

Solution. If $f, g \in C[0, 1]$, then $(f + g)(0) = f(0) + g(0) = 0$ and $(\alpha f)(0) = \alpha f(0) = 0$ are also in $C[0, 1]$; hence, W is a subspace of $C[0, 1]$.

10. Let V be a vector space over F. Prove that $-(\alpha v) = (-\alpha)v = \alpha(-v)$ for all $\alpha \in F$ and all $v \in V$.

Hint. Since $0 = \alpha 0 = \alpha(-v+v) = \alpha(-v)+\alpha v$, it follows that $-\alpha v = \alpha(-v)$.

Solution. Since $0 = \alpha 0 = \alpha(-v + v) = \alpha(-v) + \alpha v$, it follows that $-\alpha v = \alpha(-v)$.

11. Let V be a vector space of dimension n. Prove each of the following statements.

(a) If $S = \{v_1, \ldots, v_n\}$ is a set of linearly independent vectors for V, then S is a basis for V.

(b) If $S = \{v_1, \ldots, v_n\}$ spans V, then S is a basis for V.

(c) If $S = \{v_1, \ldots, v_k\}$ is a set of linearly independent vectors for V with $k < n$, then there exist vectors $v_{k+1}, \ldots, v_n$ such that

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

is a basis for V.

Solution.

(a) Let v be any vector in V. By By Proposition 20.11, $v, v_1, \ldots, v_n$ is a linearly dependent set. Consequently, there exist scalars $\alpha_0, \alpha_1, \ldots, \alpha_n$ that are not all zero and

$$\alpha_0 v + \alpha_1 v_1 + \cdots + \alpha_n v_n = 0.$$

In this case $\alpha_0 \neq 0$; otherwise, $v_1, \ldots, v_n$ would be linearly dependent. Therefore, we can write v as a linear combination of $v_1, \ldots, v_n$.

(b) If $v_1, \ldots, v_n$ are linearly dependent, then one of the v_is can be written as a linear combination of the remaining v_i's, say v_n. In this case we could eliminate v_n and $v_1, \ldots, v_{n-1}$ would still span V. Continuing we could eliminate vectors until we had a linearly independent set $v_1, \ldots, v_k$ that spans V with $k < n$. But this contradicts the fact that $\dim V = n$.

(c) If $v_1, \ldots, v_k$ are linearly independent with $k < n$, then there exists a vector v_{k+1} in V but not in the span of $v_1, \ldots, v_k$. In this case, $v_1, \ldots, v_{k+1}$ is a linearly independent set. If $k + 1 < n$ we can find a vector v_{k+2} such that $v_1, \ldots, v_{k+2}$ is a linearly independent set. Repeating this process, we will eventually arrive at a set of linearly independentvectors $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$.

12. Prove that any set of vectors containing $\mathbf{0}$ is linearly dependent.

Hint. Let $v_0 = 0, v_1, \ldots, v_n \in V$ and $\alpha_0 \neq 0, \alpha_1, \ldots, \alpha_n \in F$. Then $\alpha_0 v_0 + \cdots + \alpha_n v_n = 0$.

Solution. Let $v_0 = 0, v_1, \ldots, v_n \in V$ and $\alpha_0 \neq 0, \alpha_1, \ldots, \alpha_n \in F$. Then $\alpha_0 v_0 + \cdots + \alpha_n v_n = 0$.

13. Let V be a vector space. Show that $\{\mathbf{0}\}$ is a subspace of V of dimension zero.

Solution. Since $\mathbf{0} + \mathbf{0} = \mathbf{0}$ and $\alpha\mathbf{0} = \mathbf{0}$, we know that $\{\mathbf{0}\}$ is a subspace of V. The dimension of this subspace is 0 by definition.

14. If a vector space V is spanned by n vectors, show that any set of m vectors in V must be linearly dependent for $m > n$.

Solution. Let $v_1, \ldots, v_n$ span V, and $u_1, \ldots, u_m \in V$ with $m > n$. Then

$$\sum_{i=1}^{m} \alpha_i u_i = \sum_{i=1}^{m} \alpha_i \sum_{j=1}^{n} \beta_{ij} v_j = \sum_{j=1}^{n} \left(\alpha_i \sum_{i=1}^{m} \alpha_i \beta_{ij} \right) v_j$$

The homogeneous system $\sum_i \beta_{ij} x_i = 0$ has more unknowns than equations; hence, there exists a nontrivial solution, say

$$x_1 = \alpha_1', \ldots, x_m = \alpha_m'.$$

Therefore, $\alpha_1' u_1 + \cdots + \alpha_m' u_m = 0$, and $u_1, \ldots, u_m$ are linearly dependent.

15. **Linear Transformations.** Let V and W be vector spaces over a field F, of dimensions m and n, respectively. If $T : V \to W$ is a map satisfying

$$T(u + v) = T(u) + T(v)$$
$$T(\alpha v) = \alpha T(v)$$

for all $\alpha \in F$ and all $u, v \in V$, then T is called a **linear transformation** from V into W.

(a) Prove that the **kernel** of T, $\ker(T) = \{v \in V : T(v) = \mathbf{0}\}$, is a subspace of V. The kernel of T is sometimes called the **null space** of T.

(b) Prove that the **range** or **range space** of T, $R(V) = \{w \in W : T(v) = w \text{ for some } v \in V\}$, is a subspace of W.

(c) Show that $T : V \to W$ is injective if and only if $\ker(T) = \{\mathbf{0}\}$.

(d) Let $\{v_1, \ldots, v_k\}$ be a basis for the null space of T. We can extend this basis to be a basis $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_m\}$ of V. Why? Prove that $\{T(v_{k+1}), \ldots, T(v_m)\}$ is a basis for the range of T. Conclude that the range of T has dimension $m - k$.

(e) Let $\dim V = \dim W$. Show that a linear transformation $T : V \to W$ is injective if and only if it is surjective.

Hint. (a) Let $u, v \in \ker(T)$ and $\alpha \in F$. Then

$$T(u + v) = T(u) + T(v) = 0$$
$$T(\alpha v) = \alpha T(v) = \alpha 0 = 0.$$

Hence, $u + v, \alpha v \in \ker(T)$, and $\ker(T)$ is a subspace of V.

(c) The statement that $T(u) = T(v)$ is equivalent to $T(u - v) = T(u) - T(v) = 0$, which is true if and only if $u - v = 0$ or $u = v$.

Solution.

(a) Let $u, v \in \ker(T)$ and $\alpha \in F$. Then

$$T(u+v) = T(u) + T(v) = 0$$
$$T(\alpha v) = \alpha T(v) = \alpha 0 = 0.$$

Hence, $u+v, \alpha v \in \ker(T)$, and $\ker(T)$ is a subspace of V.

(b) If $w_1, w_2 \in R(T)$, then there exist $v_1, v_2 \in V$ such that $T(v_1) = w_1$ and $T(v_2) = w_2$. Since $w_1 + w_2 = T(v_1) + T(v_2) = T(v_1 + v_2)$, $w_1 + w_2 \in R(T)$. Similarly, we can show that if $w \in R(T)$, then $\alpha w \in R(T)$.

(c) The statement that $T(u) = T(v)$ is equivalent to $T(u-v) = T(u) - T(v) = 0$, which is true if and only if $u - v = 0$ or $u = v$.

(d) If $w \in R(T)$, then $w = T(v)$ for some $v \in V$. We can write v as a linear combination

$$v = \alpha_1 v_1 + \cdots + \alpha_k v_k + \alpha_{k+1} v_{k+1} + \cdots + \alpha_m v_m;$$

therefore,

$$\begin{aligned} w &= T(v) \\ &= \alpha_1 T(v_1) + \cdots + \alpha_k T(v_k) + \alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_m T(v_m) \\ &= \alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_m T(v_m), \end{aligned}$$

and $T(v_{k+1}), \ldots, T(v_m)$ span the range of T. To show that these vectors are linearly independent, let

$$\alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_m T(v_m) = T(\alpha_{k+1} v_{k+1} + \cdots + \alpha_m v_m) = 0.$$

Since $\alpha_{k+1} v_{k+1} + \cdots + \alpha_m v_m$ is in the kernel of T, there exist $\alpha_1, \ldots, \alpha_k$ such that

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \alpha_{k+1} v_{k+1} + \cdots + \alpha_m v_m,$$

or

$$\alpha_1 v_1 + \cdots + \alpha_k v_k - \alpha_{k+1} v_{k+1} - \cdots - \alpha_m v_m = 0.$$

Since $v_1, \ldots, v_m$ are linearly independent, all of the α_is are equal to 0. In particular, $T(v_{k+1}), \ldots, T(v_m)$ are linearly independent.

(e) This part follows directly from (c) and (d).

16. Let V and W be finite dimensional vector spaces of dimension n over a field F. Suppose that $T : V \to W$ is a vector space isomorphism. If $\{v_1, \ldots, v_n\}$ is a basis of V, show that $\{T(v_1), \ldots, T(v_n)\}$ is a basis of W. Conclude that any vector space over a field F of dimension n is isomorphic to F^n.

Solution. If $w \in W$, then $w = T(v)$ for some $v \in V$. We can write v as a linear combination $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$; therefore, $w = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n)$. Consequently, $T(v_1), \ldots, T(v_n)$ span the range of W. To show that these vectors are linearly independent, let

$$\alpha_1 T(v_1) + \cdots + \alpha_n T(v_n) = T(\alpha_1 v_1 + \cdots + \alpha_n v_n) = 0.$$

Then $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$, since it is in the kernel of T. Therefore, $\alpha_1 = \cdots = \alpha_n = 0$, and the $T(v_i)$s are linearly independent.

17. **Direct Sums.** Let U and V be subspaces of a vector space W. The sum of U and V, denoted $U + V$, is defined to be the set of all vectors of the form $u + v$, where $u \in U$ and $v \in V$.

(a) Prove that $U + V$ and $U \cap V$ are subspaces of W.

(b) If $U + V = W$ and $U \cap V = \mathbf{0}$, then W is said to be the **direct sum.** In this case, we write $W = U \oplus V$. Show that every element $w \in W$ can be written uniquely as $w = u + v$, where $u \in U$ and $v \in V$.

(c) Let U be a subspace of dimension k of a vector space W of dimension n. Prove that there exists a subspace V of dimension $n - k$ such that $W = U \oplus V$. Is the subspace V unique?

(d) If U and V are arbitrary subspaces of a vector space W, show that

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

Hint. (a) Let $u, u' \in U$ and $v, v' \in V$. Then

$$(u + v) + (u' + v') = (u + u') + (v + v') \in U + V$$
$$\alpha(u + v) = \alpha u + \alpha v \in U + V.$$

Solution.

(a) Let $u, u' \in U$ and $v, v' \in V$. Then

$$(u + v) + (u' + v') = (u + u') + (v + v') \in U + V$$
$$\alpha(u + v) = \alpha u + \alpha v \in U + V.$$

(b) Let $w = u + v$ and $w = u' + v'$, where $u, u' \in U$ and $v, v' \in V$. Then $u + v = u' + v'$, or $u - u' = v - v'$. Consequently, $u - u', v' - v \in U \cap V$. Thus, $u - u' = 0$ and $v' - v = 0$, or $u = u'$ and $v = v'$.

(c) If U is a subspace of dimension k, then it has some basis $v_1, \ldots, v_k$ that can be extended to a basis $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ of W. Let V be the span of $v_{k+1}, \ldots, v_n$. This subspace is not unique, and depends on the choice of the $v_{k+1}, \ldots, v_n$.

(d) Let $m = \dim U$ and $n = \dim V$. The set $U \cap V$ is a subspace of both U and V. If $w_1, \ldots, w_r$ is a basis of $U \cap V$, then we can extend this basis to bases $\{w_1, \ldots, w_r, u_1, \ldots, u_{m-r}\}$ and $\{w_1, \ldots, w_r, v_1, \ldots, v_{n-r}\}$ of U and V, respectively. We need only to show that $u_1, \ldots, u_{m-r}, v_1, \ldots, v_{n-r}$ is a basis for W. Since these vectors generate $U + V$, it suffices to show that these vectors are linearly independent. If

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 u_1 + \cdots + \beta_{m-r} u_{m-r} = w,$$

and

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 u_1 + \cdots + \beta_{m-r} u_{m-r} + \gamma_1 v_1 + \cdots + \gamma_{n-r} v_{n-r} = 0,$$

then $w = -\gamma_1 v_1 - \cdots - \gamma_{n-r} v_{n-r}$. Thus, $w \in U \cap V$. Consequently, there exist scalars $\delta_1, \ldots, \delta_r$ such that $w = \delta_1 w_1 + \cdots + \delta_r w_r$. Therefore,

$$\delta_1 w_1 + \cdots + \delta_r w_r + \gamma_1 v_1 + \cdots + \gamma_{n-r} v_{n-r} = 0,$$

and $\gamma_1 = \cdots = \gamma_{n-r} = 0$, since $w_1, \ldots, w_r, v_1, \ldots, v_{n-r}$ are linearly independent. Similarly, $\beta_1 = \cdots = \beta_{m-r} = 0$.

18. Dual Spaces. Let V and W be finite dimensional vector spaces over a field F.

(a) Show that the set of all linear transformations from V into W, denoted by $\text{Hom}(V, W)$, is a vector space over F, where we define vector addition as follows:

$$(S+T)(v) = S(v) + T(v)$$
$$(\alpha S)(v) = \alpha S(v),$$

where $S, T \in \text{Hom}(V, W)$, $\alpha \in F$, and $v \in V$.

(b) Let V be an F-vector space. Define the **dual space** of V to be $V^* = \text{Hom}(V, F)$. Elements in the dual space of V are called **linear functionals.** Let $v_1, \ldots, v_n$ be an ordered basis for V. If $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ is any vector in V, define a linear functional $\phi_i : V \to F$ by $\phi_i(v) = \alpha_i$. Show that the ϕ_i's form a basis for V^*. This basis is called the **dual basis** of $v_1, \ldots, v_n$ (or simply the dual basis if the context makes the meaning clear).

(c) Consider the basis $\{(3, 1), (2, -2)\}$ for $\mathbb{R}^2$. What is the dual basis for $(\mathbb{R}^2)^*$?

(d) Let V be a vector space of dimension n over a field F and let V^{**} be the dual space of V^*. Show that each element $v \in V$ gives rise to an element λ_v in V^{**} and that the map $v \mapsto \lambda_v$ is an isomorphism of V with V^{**}.

Solution.

(a) Let $v \in v$, $\alpha, \beta \in F$, and $R, S, T \in \text{Hom}(V, W)$. Then

i. $(S+T)(v) = S(v) + T(v) = T(v) + S(v) = (T+S)(v)$

ii. $[R + (S+T)](v) = R(v) + (S+T)(v) = R(v) + S(v) + T(v) = (R+S)(v) + T(v) = [(R+S) + T](v)$

iii. If 0 is the zero map, then $(T+0)(v) = T(v) + 0(v) = T(v) + 0 = T(v)$.

iv. $(T + (-1)T)(v) = T(v) - T(v) = 0(v)$

v. $(1T)(v) = 1T(v) = T(v)$

vi. $(\alpha(\beta T))(v) = \alpha(\beta T)(v) = (\alpha\beta)T(v) = ((\alpha\beta)T)(v)$

vii. $((\alpha+\beta)T)(v) = (\alpha+\beta)T(v) = \alpha T(v) + \beta T(v) = (\alpha T)(v) + (\beta T)(v)$

viii. $(\alpha(T+S))(v) = \alpha(T+S)(v) = \alpha(T(v) + S(v)) = \alpha T(v) + \alpha S(v) = (\alpha T)(v) + (\alpha S)(v) = (\alpha T + \alpha S)(v)$

(b) To show that the ϕ_i's span V^*, let $f \in V^*$. Then

$$\begin{aligned} f(v) &= f(\alpha_1 v_1 + \cdots + \alpha_n v_n) \\ &= \alpha_1 f(v_1) + \cdots + \alpha_n f(v_n) \\ &= \beta_1 \phi_1(v) + \cdots + \beta_n \phi_n(v), \end{aligned}$$

where $\beta_i = f(v_i)$. To show linear independence, assume that $\beta_1\phi_1 + \cdots + \beta_n\phi_n = 0$. We must show that $\beta_i = 0$, but $0 = \beta_1\phi_1(v_i) + \cdots + \beta_n\phi_n(v_i) = \beta_i$.

(c)

$$\phi_1(x, y) = \frac{1}{4}x + \frac{1}{4}y$$
$$\phi_1(x, y) = \frac{1}{8}x - \frac{3}{8}y$$

(d) Define a map $v \mapsto \phi_v$ from V to V^* by $\phi_v = \langle v, w\rangle = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$, where $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ and $w = \beta_1 w_1 + \cdots + \beta_n w_n$. Since $\dim V = \dim V^*$, it suffices to show that this map is one-to-one. Let $\phi_u = \phi_v$, then

$$\langle u, w\rangle = \phi_u(w) = \phi_v(w) = \langle v, w\rangle$$

for all $w \in V$. Hence,

$$0 = \langle u, w\rangle - \langle v, w\rangle = \langle u - v, w\rangle$$

and so $u - v = 0$ or $u = v$. Thus, the map is one-to-one.

(e) Observe that $\mu \in V^{**}$ is a linear map from V^* to F. Define $\lambda : V \to V^{**}$ by $\lambda_v(\phi) = \phi(v)$, where $\phi \in V^*$. To show that λ_v is in V^{**}, let $\alpha \in F$ and $\phi, \psi \in V^*$. Then

$$\lambda_v(\phi + \psi) = (\phi + \psi)(v) = \phi(v) + \psi(v) = \lambda_v\phi + \lambda_v\psi$$

and

$$\lambda_v(\alpha\phi) = \alpha\phi(v) = \alpha(\phi(v)) = \alpha\lambda_v\phi.$$

To show that λ is linear, let $u, v \in V$ and $\alpha \in F$, then

$$\lambda_{u+v}\phi = \phi(u + v) = \phi(u) + \phi(v) = \lambda_u\phi + \lambda_v\phi$$

and

$$\lambda_{\alpha v}\phi = \phi(\alpha v) = \alpha\phi(v) = \alpha\lambda_v\phi.$$

Since $\dim V < \infty$, it suffices to show that λ is one-to-one. Suppose that $\lambda_v = 0$, then we must show that $v = 0$. We have $\lambda_v(\phi) = 0$ for all $\phi \in V^*$. If $v \neq 0$, then it is an element in some ordered basis of V. Let $\phi \in V^*$ be the element in the dual basis corresponding to v, then $\lambda_v(\phi) = \phi(v) = 1$. But this is a contradiction.

20.6 Sage Exercises

1. Given two subspaces U and W of a vector space V, their sum $U + W$ can be defined as the *set* $U + W = \{u + w \mid u \in U,\ w \in W\}$, in other words, the set of all possible sums of an element from U and an element from W.

Notice this is not the direct sum of your text, nor the `direct_sum()` method in Sage. However, you can build this subspace in Sage as follows. Grab the bases of U and W individually, as lists of vectors. Join the two lists together by just using a plus sign between them. Now build the sum subspace by creating a subspace of V spanned by this set, by using the `.subspace()` method.

In the vector space (`QQ^10`) construct two subspaces that you expect to (a) have dimension 5 or 6 or so, and (b) have an intersection that is a vector space of dimension 2 or so. Compare their individual dimensions with the dimensions of the intersection of U and W ($U \cap W$, `.intersection()` in Sage) and the sum $U + W$.

Repeat the experiment with the two original vector spaces having dimension 8 or so, and with the intersection as small as possible. Form a general conjecture relating these four dimensions based on the results of your two (or more)experiments.

Solution. Sixteen random vectors, and four bases that should meet the requirements of the two suggested experiments.

```
V = QQ^10
R = [random_vector(QQ, 10) for i in range(16)]
B1 = R[0:5]
B2 = R[3:8]
B3 = R[0:8]
B4 = R[8:16]
```

```
V1 = V.subspace(B1)
V2 = V.subspace(B2)
I1 = V1.intersection(V2)
S1 = V.subspace(B1 + B2)
[X.dimension() for X in [V1, V2, I1, S1]]
```

```
[5, 5, 2, 8]
```

```
V3 = V.subspace(B3)
V4 = V.subspace(B4)
I2 = V3.intersection(V4)
S2 = V.subspace(B3 + B4)
[X.dimension() for X in [V3, V4, I2, S2]]
```

```
[8, 8, 6, 10]
```

In general,

$$\dim(V) + \dim(W) = \dim(U \cap W) + \dim(U + W).$$

2. We can construct a field in Sage that extends the rationals by adding in a fourth root of two, $\mathbb{Q}[\sqrt[4]{2}]$, with the command `F.<c> = QQ[2^(1/4)]`. This is a vector space of dimension 4 over the rationals, with a basis that is the first four powers of $c = \sqrt[4]{2}$ (starting with the zero power).

The command `F.vector_space()` will return three items in a triple (so be careful how you handle this output to extract what you need). The first part of the output is a vector space over the rationals that is isomorphic to `F`. The next is a vector space isomorphism (invertible linear transformation) from the provided vector space to the field, while the third is an isomorphism in the opposite direction. These two isomorphisms can then be used like functions. Notice that this is different behavior than for `.vector_space()` applied to finite fields. Create non-trivial examples that show that these vector space isomorphisms behave as an isomorphism should. (You will have at least four such examples in a complete solution.)

Solution. The field, the vector space, isomorphisms, four elements, and a scalar.

```
F.<c> = QQ[2^(1/4)]
V, fromV, toV = F.vector_space()
V
```

```
Vector space of dimension 4 over Rational Field
```

```
fromV
```

```
Isomorphism map:
  From: Vector space of dimension 4 over Rational Field
  To:   Number Field in a with defining polynomial x^4 - 2
```

```
toV
```

```
Isomorphism map:
  From: Number Field in a with defining polynomial x^4 - 2
  To:   Vector space of dimension 4 over Rational Field
```

```
f1 = 2 + 3*c -5*c^2 + 8*c^3
f2 = -1 + c + 2*c^2 - 7*c^3
v1 = V([3, 5, -6, 2])
v2 = V([1, 1, -5, 2])
alpha = QQ(8/3)
```

Two vector space operations, two isomorphisms, for four tests.

```
fromV(v1 + v2) == fromV(v1) + fromV(v2)
```

```
True
```

```
fromV(alpha * v1) == alpha * fromV(v1)
```

```
True
```

```
toV(f1 + f2) == toV(f1) + toV(f2)
```

```
True
```

```
toV(alpha * f1) == alpha * toV(f1)
```

```
True
```

3. Build a finite field F of order p^n in the usual way. Then construct the (multiplicative) group of all invertible (nonsingular) $m \times m$ matrices over this field with the command `G = GL(m, F)` ("the general linear group"). What is the order of this group? In other words, find a general expression for the order of this group.

Your answer should be a function of m, p and n. Provide a complete explanation of the logic behind your solution (i.e. something resembling a proof). Also provide tests in Sage that your answer is correct.

Hints: `G.order()` will help you test and verify your hypotheses. Small examples in Sage (listing all the elements of the group) might aid your intuition—which is why this is a Sage exercise. Small means 2×2 and 3×3 matrices and finite fields with $2, 3, 4, 5$ elements, at most. Results do not really depend on each of p and n, but rather just on p^n.

Realize this group is interesting because it contains representations of all the invertible (i.e. 1-1 and onto) linear transformations from the (finite) vector space F^m to itself.

Solution. As a product of allowable choices when building sequences of column vectors that remain linearly independent (by adding vectors outside the span of columns already chosen).

```
p = 5; n = 3; m = 2
F.<a> = FiniteField(p^n)
G = GL(m, F)
G.order()
```

```
242172000
```

```
prod([(p^n)^m - (p^n)^i for i in srange(m)]) == G.order()
```

```
True
```

Alternately, many powers of p^n can be factored from the above, yielding an expression that is simpler in some ways, but not as easy for a student to explain *prima facie*.

```
p = 3; n = 4; m = 3
F.<a> = FiniteField(p^n)
G = GL(m, F)
G.order()
```

```
14821874184499200 0
```

```
(p^n)^(((m-1)*m)/2)*prod([(p^n)^(m-i) - 1 for i in
    srange(m)]) == G.order()
```

```
True
```

$$\prod_{i=0}^{m-1} (p^n)^m - (p^n)^i = (p^n)^{0+1+2+\cdots+m-1} \prod_{i=0}^{m-1} (p^n)^{m-i} - (p^n)^{i-i}$$
$$= p^{n(m-1)m/2} \prod_{i=0}^{m-1} \left(p^{n(m-i)} - 1\right)$$

4. What happens if we try to do linear algebra over a *ring* that is not also a *field*? The object that resembles a vector space, but with this one distinction, is known as a **module**. You can build one easily with a construction like `ZZ^3`. Evaluate the following to create a module and a submodule.

```
M = ZZ^3
u = M([1, 0, 0])
v = M([2, 2, 0])
w = M([0, 0, 4])
N = M.submodule([u, v, w])
```

Examine the bases and dimensions (aka "rank") of the module and submodule, and check the equality of the module and submodule. How is this different than the situation for vector spaces? Can you create a third module, `P`, that is a proper subset of `M` and properly contains `N`?

Solution. Containment and equality of dimension/rank does not imply equality of sets.

```
M = ZZ^3
u = M([1, 0, 0])
v = M([2, 2, 0])
w = M([0, 0, 4])
N = M.submodule([u, v, w])
N.rank(), M.rank()
```

```
(3, 3)
```

```
M == N
```

```
False
```

A basis for N, along with the absence of $\frac{1}{2}$ from ZZ suggest the following spanning set to create an intermediate module P.

```
N.basis()
```

```
[
(1, 0, 0),
(0, 2, 0),
(0, 0, 4)
]
```

```
x = M([1, 0, 0])
y = M([0, 2, 0])
z = M([0, 0, 2])
P = M.submodule([x,y,z])
N == P, P == M, N.is_submodule(P), P.is_submodule(M)
```

```
(False, False, True, True)
```

5. A finite field, F, of order 5^3 is a vector space of dimension 3 over $\mathbb{Z}_5$. Suppose a is a generator of F. Let M be any 3×3 matrix with entries from $\mathbb{Z}_5$ (carefule here, the elements are from th field of scalars, not from the vector space). If we convert an element $x \in F$ to a vector (relative to the basis $\{1, a, a^2\}$), then we can multiply it by M (with M on the left) to create another vector, which we can translate to a linear combination of the basis elements, and hence another element of F. This function is a vector space homomorphism, better known as a linear transformation (implemented with a matrix representation relative to the basis $\{1, a, a^2\}$. Notice that each part below becomes less general and more specific.

(a) Create a non-invertible matrix R and give examples to show that the mapping described by R is a vector space homomorphism of F into F.

(b) Create an invertible matrix M. The mapping will now be an invertible homomorphism. Determine the inverse function and give examples to verify its properties.

(c) Since a is a generator of the field, the mapping $a \mapsto a^5$ can be extended to a vector space homomorphism (i.e. a linear transformation). Find a matrix M which effects this linear transformation, and from this, determine that the homomorphism is invertible.

(d) None of the previous three parts applies to properties of multiplication in the field. However, the mapping from the third part also preserves multiplication in the field, though a proof of this may not be obvious right now. So we are saying this mapping is a field automorphism, preserving both addition and multiplication. Give a nontrivial example of the multiplication-preserving properties of this mapping. (This is the **Frobenius map** which will be discussed further in Chapter 21.)

Solution. Fields, elements, scalars, and a vector of basis elements.

```
Z5 = Integers(5)
F.<a> = FiniteField(5^3)
f1 = 2 + 3*a + a^2
f2 = 1 + 4*a + 2*a^2
alpha = Z5(3)
basis = vector(F, [1, a, a^2])
```

```
R = matrix(F, 3, 3, [[1,2,3],[4,0,1], [0,2,4]])
R.is_invertible()
```

```
False
```

We use the `.inner_product()` method to form the necessary linear combinations, and test preservation of the two vector space operations.

```
A = (R*vector(f1 + f2)).inner_product(basis)
B = (R*vector(f1)).inner_product(basis) +
    (R*vector(f2)).inner_product(basis)
A == B
```

```
True
```

```
A = (R*vector(alpha*f1)).inner_product(basis)
B = alpha * (R*vector(f1)).inner_product(basis)
A == B
```

```
True
```

With an invertible matrix, the inverse linear transformation is represented by the inverse matrix representation. We check an example of one of the two round trips.

```
M = matrix(F, 3, 3, [[1,2,3],[4,0,1], [2, 3, 0]])
M.is_invertible()
```

```
True
```

```
g = (M*vector(f1)).inner_product(basis)
f1 == (M.inverse()*vector(g)).inner_product(basis)
```

```
True
```

The matrix representation of the linear transformation has columns that are outputs of the linear transformation on the basis, coordinatized relative to the basis.

```
T = column_matrix([vector(x^5) for x in [a^0, a^1, a^2]])
T
```

```
[1 4 3]
[0 4 2]
[0 2 0]
```

```
T.is_invertible()
```

```
True
```

We check one example of this mapping preserving multiplication in the field.

```
A = (T*vector(f1*f2)).inner_product(basis)
B = (T*vector(f1)).inner_product(basis) *
    (T*vector(f2)).inner_product(basis)
A == B
```

```
True
```

Chapter 21

Fields

21.4 Exercises

1. Show that each of the following numbers is algebraic over $\mathbb{Q}$ by finding the minimal polynomial of the number over $\mathbb{Q}$.

(a) $\sqrt{1/3+\sqrt{7}}$

(b) $\sqrt{3}+\sqrt[3]{5}$

(c) $\sqrt{3}+\sqrt{2}\,i$

(d) $\cos\theta + i\sin\theta$ for $\theta = 2\pi/n$ with $n \in \mathbb{N}$

(e) $\sqrt{\sqrt[3]{2}-i}$

Hint. (a) $x^4-(2/3)x^2-62/9$; (c) x^4-2x^2+25.

Solution.

(a) $x^4-(2/3)x^2-62/9$

(b) $x^6-9x^4-10x^3+27x^2-90x-2$

(c) x^4-2x^2+25

(d) x^n-1

(e) $x^{12}-3x^8-4x^6+3x^4+12x^2+5$

2. Find a basis for each of the following field extensions. What is the degree of each extension?

(a) $\mathbb{Q}(\sqrt{3},\sqrt{6}\,)$ over $\mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3}\,)$ over $\mathbb{Q}$

(c) $\mathbb{Q}(\sqrt{2},i)$ over $\mathbb{Q}$

(d) $\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7}\,)$ over $\mathbb{Q}$

(e) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}\,)$ over $\mathbb{Q}$

(f) $\mathbb{Q}(\sqrt{8}\,)$ over $\mathbb{Q}(\sqrt{2}\,)$

(g) $\mathbb{Q}(i,\sqrt{2}+i,\sqrt{3}+i)$ over $\mathbb{Q}$

(h) $\mathbb{Q}(\sqrt{2}+\sqrt{5}\,)$ over $\mathbb{Q}(\sqrt{5}\,)$

(i) $\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10}\,)$ over $\mathbb{Q}(\sqrt{3}+\sqrt{5}\,)$

Hint. (a) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$; (c) $\{1, i, \sqrt{2}, \sqrt{2}\,i\}$; (e) $\{1, 2^{1/6}, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}\}$.
Solution.

(a) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

(b) $\{1, 2^{1/3}, 2^{2/3}, 3^{1/3}, 3^{1/3}2^{1/3}, 3^{1/3}2^{2/3}, 3^{2/3}, 3^{2/3}2^{1/3}, 3^{2/3}2^{2/3}\}$

(c) $\{1, i, \sqrt{2}, \sqrt{2}\,i\}$

(d) $\{1, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{15}, \sqrt{21}, \sqrt{35}, \sqrt{105}\}$

(e) $\{1, 2^{1/6}, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}\}$

(f) $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$

(g) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, i, \sqrt{2}\,i, \sqrt{3}\,i, \sqrt{6}\,i\}$

(h) $\{1, \sqrt{2}\}$

(i) $\{1, \sqrt{2}\}$

3. Find the splitting field for each of the following polynomials.

(a) $x^4 - 10x^2 + 21$ over $\mathbb{Q}$

(b) $x^4 + 1$ over $\mathbb{Q}$

(c) $x^3 + 2x + 2$ over $\mathbb{Z}_3$

(d) $x^3 - 3$ over $\mathbb{Q}$

Hint. (a) $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.
Solution.

(a) $\mathbb{Q}(\sqrt{3}, \sqrt{7})$

(b) $\mathbb{Q}(i)$

(c) This polynomial is irreducible over $\mathbb{Z}_3$. Construct the field $\mathbb{Z}_2[x]/\langle x^3 + 2x + 2\rangle$ as in Example 21.2. This field has 27 elements.

(d) $\mathbb{Q}(\sqrt[3]{3}, i)$

4. Consider the field extension $\mathbb{Q}(\sqrt[4]{3}, i)$ over $\mathbb{Q}$.

(a) Find a basis for the field extension $\mathbb{Q}(\sqrt[4]{3}, i)$ over $\mathbb{Q}$. Conclude that $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}] = 8$.

(b) Find all subfields F of $\mathbb{Q}(\sqrt[4]{3}, i)$ such that $[F : \mathbb{Q}] = 2$.

(c) Find all subfields F of $\mathbb{Q}(\sqrt[4]{3}, i)$ such that $[F : \mathbb{Q}] = 4$.

Solution.

(a) If we $\alpha = \sqrt[4]{3}$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and we have a basis of

$$\{1, \alpha, \alpha^2, \alpha^3\}$$

for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Note that $\alpha^2 = \sqrt{3}$. Since $i \notin \mathbb{Q}(\alpha)$, it must be the case that $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. Thus, the set

$$\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

is a basis for $\mathbb{Q}(\sqrt[4]{3}, i)$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}] = 8$.

(b) The three fields of dimension 2 over $\mathbb{Q}$ are $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(i\sqrt{3})$.

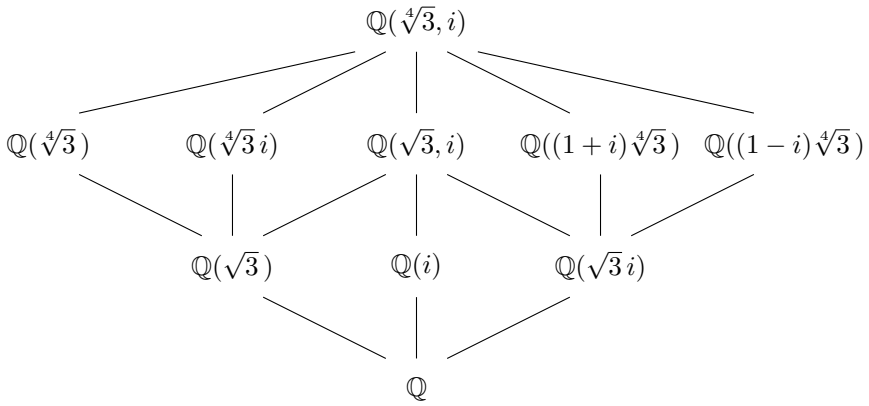
(c) To find all subfields F of $\mathbb{Q}(\sqrt[4]{3}, i)$ such that $[F : \mathbb{Q}] = 4$, we consider the fields containing $\mathbb{Q}(\sqrt{3}\,)$, $\mathbb{Q}(i)$, and $\mathbb{Q}(i\sqrt{3}\,)$.

- Over $\mathbb{Q}(\sqrt{3}\,)$, we can find three fields of dimension 2: $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha i)$, and $\mathbb{Q}(\sqrt{3}, i)$. These fields have dimension 4 over $\mathbb{Q}$.
- There only one field of dimension 4 over $\mathbb{Q}(i)$ is $\mathbb{Q}(\sqrt{3}i)$.
- Finally, we need to find all fields of dimension 2 over $\mathbb{Q}(i\sqrt{3}\,)$. Certainly, one such field is $\mathbb{Q}(\sqrt{3}, i)$. To find the remaining two fields, we will consider a new basis

$$\{1, \alpha + i\alpha, \alpha - i\alpha, \alpha^2, i, i\alpha^2, \alpha^3 + i\alpha^3, \alpha^3 - i\alpha^3\}.$$

The remaining two fields that we seek are $\mathbb{Q}(\alpha + i\alpha)$ and $\mathbb{Q}(\alpha - i\alpha)$. The field $\mathbb{Q}(\alpha + i\alpha)$ has basis $\{1, \alpha + i\alpha, i\sqrt{3}, \alpha^3 - i\alpha^3\}$. The field $\mathbb{Q}(\alpha - i\alpha)$ has basis $\{1, \alpha - i\alpha, i\sqrt{3}, \alpha^3 + i\alpha^3\}$. Both fields contain $\mathbb{Q}(i\sqrt{3})$ and are properly contained in $\mathbb{Q}(\sqrt[4]{3}, i)$.

All of the subfields of $\mathbb{Q}(\sqrt[4]{3}, i)$ over $\mathbb{Q}$ are described in the figure below.



5. Show that $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ is a field with eight elements. Construct a multiplication table for the multiplicative group of the field.

Hint. Use the fact that the elements of $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ are 0, 1, α, $1 + \alpha$, α^2, $1 + \alpha^2$, $\alpha + \alpha^2$, $1 + \alpha + \alpha^2$ and the fact that $\alpha^3 + \alpha + 1 = 0$.

Solution. Use the fact that the elements of $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ are 0, 1, α, $1 + \alpha$, α^2, $1 + \alpha^2$, $\alpha + \alpha^2$, $1 + \alpha + \alpha^2$ and the fact that $\alpha^3 + \alpha + 1 = 0$.

6. Show that the regular 9-gon is not constructible with a straightedge and compass, but that the regular 20-gon is constructible.

Solution. If a regular 9-gon could be constructed with a straightedge and compass, then a 40° and consequently a 20° could be constructed which is an impossibility. To show that a regular 20-gon is constructible, use the fact that a regular pentagon is constructible.

7. Prove that the cosine of one degree ($\cos 1°$) is algebraic over $\mathbb{Q}$ but not constructible.

Solution. If $\alpha = \cos 1°$, then $(\cos 1° + i \sin 1°)^{180} = -1$. Using the fact that $\sin 1° = \sqrt{1 - \cos^2 1°}$, we have $(\alpha + i\sqrt{1 - \alpha^2}\,)^{180} = -1$. Expanding this equation, we have $f(\alpha) + ig(\alpha) + (h(\alpha) + ik(\alpha))\sqrt{1 - \alpha^2}\,)$, where f, g, h, and k are polynomials in α with integer coefficients. Using this, construct a polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$.

8. Can a cube be constructed with three times the volume of a given cube?

Hint. False.

Solution. False, if the edge of the original cube has length l, the edge of a cube that has three times the volume would be $\sqrt[3]{3}l$; however, $\sqrt[3]{3}$ is not a constructible number.

9. Prove that $\mathbb{Q}(\sqrt{3}, \sqrt[4]{3}, \sqrt[8]{3}, \ldots)$ is an algebraic extension of $\mathbb{Q}$ but not a finite extension.

Solution. Certainly every element is algebraic since $[\mathbb{Q}(\sqrt[n]{3}) : \mathbb{Q}] = n$; however, we have an infinite tower of fields,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[4]{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[4]{3}, \sqrt[8]{3}) \subset \cdots,$$

with each field properly containing the previous field.

10. Prove or disprove: π is algebraic over $\mathbb{Q}(\pi^3)$.

Solution. Since π is a root of $x^3 - \pi^3$, π is algebraic over $\mathbb{Q}(\pi^3)$.

11. Let $p(x)$ be a nonconstant polynomial of degree n in $F[x]$. Prove that there exists a splitting field E for $p(x)$ such that $[E : F] \leq n!$.

Solution. Using the proof of Theorem 21.5, $p(x)$ has a root in some extension E of F, where $[E : F] \leq n$. Write $p(x) = (x-a)q(x)$, where $q(x) \in E[x]$. Using mathematical induction on the degree of the polynomial, $q(x)$ splits in some extension K of E with $[K : E] \leq (n-1)!$. Hence, $p(x)$ must also split in K and $[K : F] = [K : E][E : F] \leq n!$.

12. Prove or disprove: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$.

Solution. False. Assume that there exists an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Then

$$2 = 1 + 1 = \phi(1) + \phi(1) = \phi(1 + 1) = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = [\phi(\sqrt{2})]^2,$$

which contradicts the fact that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$.

13. Prove that the fields $\mathbb{Q}(\sqrt[4]{3})$ and $\mathbb{Q}(\sqrt[4]{3}\, i)$ are isomorphic but not equal.

Solution. Use the obvious isomorphism, $\sqrt[4]{3} \mapsto \sqrt[4]{3}$.

14. Let K be an algebraic extension of E, and E an algebraic extension of F. Prove that K is algebraic over F. [*Caution*: Do not assume that the extensions are finite.]

Hint. Suppose that E is algebraic over F and K is algebraic over E. Let $\alpha \in K$. It suffices to show that α is algebraic over some finite extension of F. Since α is algebraic over E, it must be the zero of some polynomial $p(x) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$ in $E[x]$. Hence α is algebraic over $F(\beta_0, \ldots, \beta_n)$.

Solution. Suppose that E is algebraic over F and K is algebraic over E. Let $\alpha \in K$. It suffices to show that α is algebraic over some finite extension of F. Since α is algebraic over E, it must be the zero of some polynomial $p(x) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$ in $E[x]$. Hence α is algebraic over $F(\beta_0, \ldots, \beta_n)$.

15. Prove or disprove: $\mathbb{Z}[x]/\langle x^3 - 2\rangle$ is a field.

Solution. $\mathbb{Z}[x]/\langle x^3 - 2\rangle$ is not a field.

16. Let F be a field of characteristic p. Prove that $p(x) = x^p - a$ either is irreducible over F or splits in F.

Solution. Use the fact that $(a + b)^p = a^p + b^p$.

17. Let E be the algebraic closure of a field F. Prove that every polynomial $p(x)$ in $F[x]$ splits in E.

Solution. If $p(x)$ does not split in E, then $p(x) = q(x)r(x)$, where $r(x)$ is a nonlinear irreducible factor over E. But this is not possible since $E[x]/\langle r(x)\rangle$ would be a proper algebraic extension of E.

18. If every irreducible polynomial $p(x)$ in $F[x]$ is linear, show that F is an algebraically closed field.

Solution. Apply Theorem 21.13.

19. Prove that if α and β are constructible numbers such that $\beta \neq 0$, then so is α/β.

Solution. Draw a figure similar to Figure 21.1.

20. Show that the set of all elements in $\mathbb{R}$ that are algebraic over $\mathbb{Q}$ form a field extension of $\mathbb{Q}$ that is not finite.

Solution. This is clearly not a finite extension, since it must contain the constructible numbers.

21. Let E be an algebraic extension of a field F, and let σ be an automorphism of E leaving F fixed. Let $\alpha \in E$. Show that σ induces a permutation of the set of all zeros of the minimal polynomial of α that are in E.

Solution. If $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is the minimal polynomial of α, then $p(\alpha) = 0$, and

$$0 = \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0.$$

22. Show that $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3} + \sqrt{7}\,)$. Extend your proof to show that $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,) = \mathbb{Q}(\sqrt{a} + \sqrt{b}\,)$, where $\gcd(a, b) = 1$.

Hint. Since $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,)$ over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) \supset \mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$. Since $[\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) : \mathbb{Q}] = 4$, $[\mathbb{Q}(\sqrt{3}+\sqrt{7}\,) : \mathbb{Q}] = 2$ or 4. Since the degree of the minimal polynomial of $\sqrt{3}+\sqrt{7}$ is 4, $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$.

Solution. Since $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,)$ over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) \supset \mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$. Since $[\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) : \mathbb{Q}] = 4$, $[\mathbb{Q}(\sqrt{3}+\sqrt{7}\,) : \mathbb{Q}] = 2$ or 4. Since the degree of the minimal polynomial of $\sqrt{3}+\sqrt{7}$ is 4, $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$.

23. Let E be a finite extension of a field F. If $[E : F] = 2$, show that E is a splitting field of F for some polynomial $f(x) \in F[x]$.

Solution. If $f(x)$ is an irreducible polynomial of degree 2 in $F[x]$ with a root in E, then $f(x)$ must factor into linear factors in $E[x]$.

24. Prove or disprove: Given a polynomial $p(x)$ in $\mathbb{Z}_6[x]$, it is possible to construct a ring R such that $p(x)$ has a root in R.

Solution. False.

25. Let E be a field extension of F and $\alpha \in E$. Determine $[F(\alpha) : F(\alpha^3)]$.

Solution. $[F(\alpha) : F(\alpha^3)] = 1$ or 3.

26. Let α, β be transcendental over $\mathbb{Q}$. Prove that either $\alpha\beta$ or $\alpha + \beta$ is also transcendental.

Solution. Suppose that $\alpha + \beta$ and $\alpha\beta$ are both algebraic over $\mathbb{Q}$. Then

$$\sqrt{(\alpha+\beta)^2 - 4\alpha\beta} = \sqrt{(\alpha-\beta)^2} = \alpha - \beta$$

is algebraic over $\mathbb{Q}$. But this is a contradiction since $(\alpha+\beta) + (\alpha-\beta) = 2\alpha$ is algebraic.

27. Let E be an extension field of F and $\alpha \in E$ be transcendental over F. Prove that every element in $F(\alpha)$ that is not in F is also transcendental over F.

Hint. Let $\beta \in F(\alpha)$ not in F. Then $\beta = p(\alpha)/q(\alpha)$, where p and q are polynomials in α with $q(\alpha) \neq 0$ and coefficients in F. If β is algebraic over F, then there exists a polynomial $f(x) \in F[x]$ such that $f(\beta) = 0$. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then

$$0 = f(\beta) = f\left(\frac{p(\alpha)}{q(\alpha)}\right) = a_0 + a_1\left(\frac{p(\alpha)}{q(\alpha)}\right) + \cdots + a_n\left(\frac{p(\alpha)}{q(\alpha)}\right)^n.$$

Now multiply both sides by $q(\alpha)^n$ to show that there is a polynomial in $F[x]$ that has α as a zero.

Solution. Let $\beta \in F(\alpha)$ not in F. Then $\beta = p(\alpha)/q(\alpha)$, where p and q are polynomials in α with $q(\alpha) \neq 0$ and coefficients in F. If β is algebraic over F, then there exists a polynomial $f(x) \in F[x]$ such that $f(\beta) = 0$. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then

$$0 = f(\beta) = f\left(\frac{p(\alpha)}{q(\alpha)}\right) = a_0 + a_1\left(\frac{p(\alpha)}{q(\alpha)}\right) + \cdots + a_n\left(\frac{p(\alpha)}{q(\alpha)}\right)^n.$$

Now multiply both sides by $q(\alpha)^n$ to show that there is a polynomial in $F[x]$ that has α as a zero.

28. Let α be a root of an irreducible monic polynomial $p(x) \in F[x]$, with $\deg p = n$. Prove that $[F(\alpha) : F] = n$.

Hint. See the comments following Theorem 21.13.

Solution. Since $p(x)$ is irreducible over F, the degree of α is n. By Theorem 21.13, a basis for $F(\alpha)$ over F is $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Thus, $[F(\alpha) : F] = n$.

21.6 Sage Exercises

1. Create the polynomial $p(x) = x^5 + 2x^4 + 1$ over $\mathbb{Z}_3$. Verify that it does not have any linear factors by evaluating $p(x)$ with each element of $\mathbb{Z}_3$, and then check that $p(x)$ is irreducible.

Create a finite field of order 3^5 with the `FiniteField()` command, but include the `modulus` keyword set to the polynomial $p(x)$ to override the default choice.

Recreate $p(x)$ as a polynomial over this field. Check each of the $3^5 = 243$ elements of the field to see if they are roots of the polynomial and list all of the elements which are roots. Finally, request that Sage give a factorization of $p(x)$ over the field, and comment on the relationship between your list of roots and your factorization.

Solution.

```
ZZ3 = Integers(3)
R.<x> = ZZ3[]
p = x^5+2*x^4+1
[p(t) for t in ZZ3]
```

```
[1, 1, 2]
```

```
p.is_irreducible()
```

```
True
```

```
F.<a> = FiniteField(3^5, modulus=p)
[u for u in F if p(u) == 0]
```

```
[a, a^3, 2*a^3 + 2*a^2 + 2*a + 2, 2*a^4 + a^2 + 2*a + 1, a^4
    + a + 1]
```

Note in the following how we can upgrade the polynomial to have coefficients from the new field.

```
S.<y> = F[]
q = S(p)
q.factor()
```

```
(y + 2*a) *
(y + a^3 + a^2 + a + 1) *
(y + 2*a^3) *
(y + a^4 + 2*a^2 + a + 2) *
(y + 2*a^4 + 2*a + 2)
```

2. This problem continues the previous one. Build the ring of polynomials over $\mathbb{Z}_3$ and within this ring use $p(x)$ to generate a principal ideal. Finally construct the quotient of the polynomial ring by the ideal. Since the polynomial is irreducible, this quotient ring is a field, and by Proposition 21.12 this quotient ring is isomorphic to the number field in the previous problem.

Borrowing from your results in the previous question, construct five roots of the polynomial $p(x)$ within this quotient ring, but now as expressions in the generator of the quotient ring (which is technically a coset). Use Sage to verify that they are indeed roots. This demonstrates using a quotient ring to create a splitting field for an irreducible polynomial over a finite field.

Solution.

```
id = R.ideal(p)
Q.<z> = R.quotient(id)
Q
```

```
Univariate Quotient Polynomial Ring in z over
Ring of integers modulo 3 with modulus x^5 + 2*x^4 + 1
```

```
roots = [z, z^3, 2*z^3 + 2*z^2 + 2*z + 2, 2*z^4 + z^2 + 2*z
    + 1, z^4 + z + 1]
[p(r) for r in roots]
```

```
[0, 0, 0, 0, 0]
```

3. The subsection Algebraic Elements relies on techniques from linear algebra and contains Theorem 21.15: every finite extension is an algebraic extension. This exercise will help you understand this proof.

The polynomial $r(x) = x^4 + 2x + 2$ is irreducible over the rationals (Eisenstein's criterion with prime $p = 2$). Create a number field that contains a root of $r(x)$. By Theorem 21.15, and the remark following, every element of this finite field extension is an algebraic number, and hence satisfies some polynomial over the base field (it is this polynomial that Sage will produce with the `.minpoly()` method). This exercise will show how we can use just linear algebra to determine this minimal polynomial.

Suppose that `a` is the generator of the number field you just created with $r(x)$. Then we will determine the minimal polynomial of `t = 3a + 1` using just linear algebra. According to the proof, the first five powers of `t` (start counting

from zero) will be linearly dependent. (Why?) So a nontrivial relation of linear dependence on these powers will provide the coefficients of a polynomial with `t` as a root. Compute these five powers, then construct the correct linear system to determine the coefficients of the minimal polynomial, solve the system, and suitably interpret its solutions.

Hints: The `vector()` and `matrix()` commands will create vectors and matrices, and the `.solve_right()` method for matrices can be used to find solutions. Given an element of the number field, which will necessarily be a polynomial in the generator `a`, the `.vector()` method of the element will provide the coefficients of this polynomial in a list.

Solution.

```
R.<x> = QQ[]
P.<a> = NumberField(x^4+2*x + 2)
t = 3*a + 1
powers = [t^i for i in range(5)]
coeff = matrix([vector(p) for p in powers])
kernel = coeff.kernel()
combo = kernel.basis()[0]
poly = sum([combo[i]*x^i for i in range(5)])
poly
```

```
1/109*x^4 - 4/109*x^3 + 6/109*x^2 + 50/109*x + 1
```

A convenience method can be used to quickly convert to a (monic) polynomial over the integers.

```
poly.denominator()*poly
```

```
x^4 - 4*x^3 + 6*x^2 + 50*x + 109
```

A basic check.

```
poly(t)
```

```
0
```

4. Construct the splitting field of $s(x) = x^4 + x^2 + 1$ and find a factorization of $s(x)$ over this field into linear factors.

Solution. The polynomial factors over the rationals into two quadratics. Adjoining a root of one of these quadratics will allow both to factor into linear factors.

```
R.<x> = QQ[]
s = x^4 + x^2 + 1
s.factor()
```

```
(x^2 - x + 1) * (x^2 + x + 1)
```

```
T.<a> = NumberField(x^2+x+1)
P.<y> = T[]
q = P(s)
q.factor()
```

```
(y - a - 1) * (y + a) * (y - a) * (y + a + 1)
```

5. Form the number field, K, which contains a root of the irreducible polynomial $q(x) = x^3 + 3x^2 + 3x - 2$. Name your root `a`. Verify that $q(x)$ factors, but does not split, over K. With K now as the base field, form an extension

of K where the quadratic factor of $q(x)$ has a root. Name this root `b`, and call this second extension of the tower L.

Use `M.<c> = L.absolute_field()` to form the flattened tower that is the absolute number field `M`. Find the defining polynomial of `M` with the `.polynomial()` method. From this polynomial, which must have the generator `c` as a root, you should be able to use elementary algebra to write the generator as a fairly simple expression.

M should be the splitting field of $q(x)$. To see this, start over, and build from scratch a new number field, P, using the simple expression for `c` that you just found. Use `d` as the name of the root used to construct `P`. Since `d` is a root of the simple minimal polynomial for `c`, you should be able to write an expression for `d` that a pre-calculus student would recognize.

Now factor the original polynomial $q(x)$ (with rational coefficients) over P, to see the polynomial split (as expected). Using this factorization, and your simple expression for `d` write simplified expressions for the three roots of $q(x)$. See if you can convert between the two versions of the roots "by hand", and without using the isomorphisms provided by the `.structure()` method on `M`.

Solution. Build an extension with one of the roots. Notice the "upgrade" of the polynomial via Sage's coercion mechanism. Factor here to see one root, named `a`, and the remainder of the polynomial.

```
R.<x> = QQ[]
q = x^3+3*x^2+3*x-2
K.<a> = NumberField(q)
S.<y> = K[]
S(q).factor()
```

```
(y - a) * (y^2 + (a + 3)*y + a^2 + 3*a + 3)
```

Isolate the quadratic factor, and build an extension of `K` where the quadratic factors, with one of the roots named `b`.

```
r = S(q).factor()[1][0]
L.<b> = NumberField(r)
L
```

```
Number Field in b with defining polynomial y^2 + (a + 3)*y +
    a^2 + 3*a + 3 over its base field
```

Factor the original polynomial in the field extension `L`.

```
T.<z> = L[]
T(q).factor()
```

```
(z + b + a + 3) * (z - b) * (z - a)
```

So the three roots of q are `a`, `b` and `-a-b-3`.

Now "flatten" `L` to create an isomorphic field extension, `M`, over the rationals.

```
M.<c> = L.absolute_field()
M.polynomial()
```

```
x^6 + 243
```

So `M` is a simple extension, with generator `c`. A pre-calculus student would recognize `c` as $c = (-243)^{\frac{1}{6}}$. This is the key observation in this problem.

Here is a "from scratch" version of `M`, a polynomial ring, an upgrade of `q` and a factorization.

```
MM.<d> = NumberField(x^6 + 243)
U.<z> = MM[]
U(q).factor()
```

```
(z - 1/27*d^4 + 1) * (z + 1/54*d^4 - 1/2*d + 1) * (z +
    1/54*d^4 + 1/2*d + 1)
```

These three roots look different than the three roots above, but should be the same (they came from the same polynomial!). Notice that

$$-\left(\frac{1}{27}c^4 - 1\right) - \left(-\frac{1}{54}c^4 + \frac{1}{2}c - 1\right) - 3 = -\frac{1}{54}c^4 - \frac{1}{2}c - 1.$$

This suggests the three different expressions for the three roots of q.

a	1/27*c^4 - 1	$\frac{1}{27}(-243)^{(4/6)} - 1$
b	-1/54*c^4 + 1/2*c - 1	$\frac{-1}{54}(-243)^{(4/6)} + \frac{1}{2}(-243)^{(1/6)} - 1$
-a-b-3	-1/54*c^4 - 1/2*c - 1	$\frac{-1}{54}(-243)^{(4/6)} - \frac{1}{2}(-243)^{(1/6)} - 1$

We can try, with limted success, to verify these more conventional expressions with Sage's symbolic routines. First we build the polynomial as an entirely symbolic expression.

```
t = var('t')
f = t^3 + 3*t^2 + 3*t -2
```

Then test our three roots, requesting explicitly simplification of the result.

```
f(t = 1/27*((-243)^(1/6))^4 - 1).simplify_full()
```

```
0
```

Good, as expected. Now not quite so good.

```
f(t = -1/54*(((-243)^(1/6)))^4 + 1/2*(-243)^(1/6) -
    1).simplify_full()
```

```
3/8*243^(1/6)*9^(1/3)*(-1)^(1/6) + 9/8*I*sqrt(3) -
    27/8*(-1)^(1/3) - 27/8
```

If we think the *only* cube root of -1 is -1, then we can see the last two terms cancelling each other. Similar comments would apply to the first term.

Chapter 22

Finite Fields

22.3 Exercises

1. Calculate each of the following.

(a) $[\mathrm{GF}(3^6) : \mathrm{GF}(3^3)]$

(b) $[\mathrm{GF}(128) : \mathrm{GF}(16)]$

(c) $[\mathrm{GF}(625) : \mathrm{GF}(25)]$

(d) $[\mathrm{GF}(p^{12}) : \mathrm{GF}(p^2)]$

Hint. Make sure that you have a field extension.

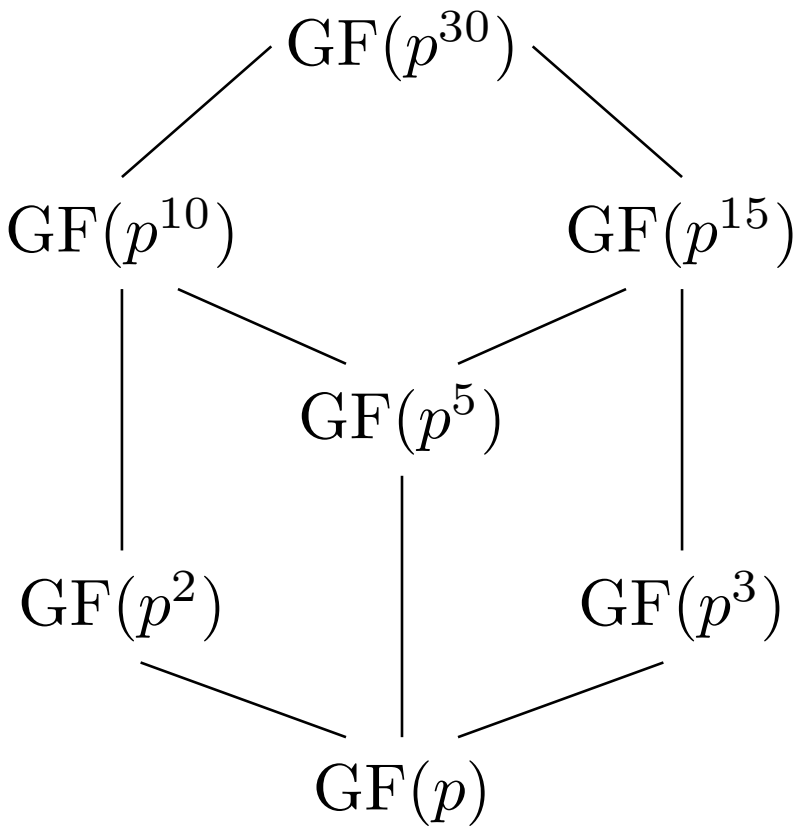
Solution. (a) $[\mathrm{GF}(3^6) : \mathrm{GF}(3^3)] = 6/3 = 2$; (b) since $[\mathrm{GF}(128) : \mathrm{GF}(16)] = [\mathrm{GF}(2^7) : \mathrm{GF}(2^4)] = 7/4$ in not an integer, this is not possible; (c) $[\mathrm{GF}(625) : \mathrm{GF}(25)] = [\mathrm{GF}(5^4) : \mathrm{GF}(5^2)] = 4/2 = 2$; (d) $[\mathrm{GF}(p^{12}) : \mathrm{GF}(p^2)] = 12/2 = 6$.

2. Calculate $[\mathrm{GF}(p^m) : \mathrm{GF}(p^n)]$, where $n \mid m$.

Solution. $[\mathrm{GF}(p^m) : \mathrm{GF}(p^n)] = m/n$.

3. What is the lattice of subfields for $\mathrm{GF}(p^{30})$?

Solution.



4. Let α be a zero of $x^3 + x^2 + 1$ over $\mathbb{Z}_2$. Construct a finite field of order 8. Show that $x^3 + x^2 + 1$ splits in $\mathbb{Z}_2(\alpha)$.

Hint. There are eight elements in $\mathbb{Z}_2(\alpha)$. Exhibit two more zeros of x^3+x^2+1 other than α in these eight elements.

Solution. There are eight elements in $\mathbb{Z}_2(\alpha)$. Exhibit two more zeros of $x^3 + x^2 + 1$ other than α in these eight elements.

5. Construct a finite field of order 27.

Hint. Find an irreducible polynomial $p(x)$ in $\mathbb{Z}_3[x]$ of degree 3 and show that $\mathbb{Z}_3[x]/\langle p(x)\rangle$ has 27 elements.

Solution. Find an irreducible polynomial $p(x)$ in $\mathbb{Z}_3[x]$ of degree 3 and show that $\mathbb{Z}_3[x]/\langle p(x)\rangle$ has 27 elements.

6. Prove or disprove: $\mathbb{Q}^*$ is cyclic.

Solution. Since the subgroup generated by $2^m 3^n$ is isomorphic to the non-cyclic group $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}^*$ is not cyclic.

7. Factor each of the following polynomials in $\mathbb{Z}_2[x]$.

(a) $x^5 - 1$

(b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

(c) $x^9 - 1$

(d) $x^4 + x^3 + x^2 + x + 1$

Hint. (a) $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$; (c) $x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

Solution.

(a) $x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$.

(b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)$.

(c) $x^9 - 1 = (x+1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

(d) $x^4 + x^3 + x^2 + x + 1$ is irreducible.

8. Prove or disprove: $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$.

Hint. True.

Solution. True.

9. Determine the number of cyclic codes of length n for $n = 6$, 7, 8, 10.

Solution. Use the following factorizations of $x^n - 1$.

(a) $x^6 - 1 = (x+1)^2(x^2 + x + 1)^2$

(b) $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$

(c) $x^8 - 1 = (x+1)^8$

(d) $x^{10} - 1 = (x+1)^6(x^4 + x^3 + x^2 + x + 1)$

10. Prove that the ideal $\langle t + 1\rangle$ in R_n is the code in $\mathbb{Z}_2^n$ consisting of all words of even parity.

Solution. Show that every n-tuple gets encoded into a vector of even weight. It suffices to check the result on a basis.

11. Construct all BCH codes of

(a) length 7. (b) length 15.

Hint. (a) Use the fact that $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Solution. Use the following factorizations of $x^n - 1$.

(a) $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$

(b) See Example 8.

12. Prove or disprove: There exists a finite field that is algebraically closed.

Hint. False.

Solution. False. Suppose that $F = \{a_1, a_2, \ldots, a_n\}$. Then

$$p(x) = 1 + \prod_{i=1}^{n}(x - a_i)$$

cannot have a root in F. Hence, F cannot be algebraically closed.

13. Let p be prime. Prove that the field of rational functions $\mathbb{Z}_p(x)$ is an infinite field of characteristic p.

Solution. See Exercise 7 in Chapter 18.

14. Let D be an integral domain of characteristic p. Prove that $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ for all $a, b \in D$.

Solution. Use the proof of Lemma 22.3.

15. Show that every element in a finite field can be written as the sum of two squares.

Solution. Let F be a finite field. If the characteristic of F is 2, then the map $\Phi : F \to F$ defined by $x \mapsto x^2$ is an automorphism. This is the Frobenius map (see Exercise 22.3.21) or can be proven directly. Therefore, every element $y \in F$ is the pre-image of some $x \in F$ under this map, or $y = x^2$ for some $x \in F$. Consquently, $y = x^2 + 0^2$.

If the characteristic of F is odd, then let $F^* = \langle a \rangle$. Then $x \in F^*$ is a perfect square exactly when $x = a^{2k}$ for some $k \in \mathbb{N}$. Thus, including 0, there must be $|F-1|/2+1$ squares in F. Let S denote the set of all squares in F. If b is an arbitrary element in F, define $T = \{b - s : s \in S\}$. Then

$$|S \cap T| = |S| + |T| - |S \cup T| = 2(|F-1|/2+1) - |F| = |F-1| + 2 - |F| > 0,$$

and the intersection S and T is never empty. Thus, for any b in F, there exists a $t \in S \cap T$ such that $t = b - s$ or $b = s + t$. Thus, b can b e written as the sum of two squares.

16. Let E and F be subfields of a finite field K. If E is isomorphic to F, show that $E = F$.

Solution. Use Theorem 20.6.

17. Let $F \subset E \subset K$ be fields. If K is a separable extension of F, show that K is also separable extension of E.

Hint. If $p(x) \in F[x]$, then $p(x) \in E[x]$.

Solution. If $p(x) \in F[x]$, then $p(x) \in E[x]$.

18. Let E be an extension of a finite field F, where F has q elements. Let $\alpha \in E$ be algebraic over F of degree n. Prove that $F(\alpha)$ has q^n elements.

Hint. Since α is algebraic over F of degree n, we can write any element $\beta \in F(\alpha)$ uniquely as $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ with $a_i \in F$. There are q^n possible n-tuples $(a_0, a_1, \ldots, a_{n-1})$.

Solution. Since α is algebraic over F of degree n, we can write any element $\beta \in F(\alpha)$ uniquely as $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ with $a_i \in F$. There are q^n possible n-tuples $(a_0, a_1, \ldots, a_{n-1})$.

19. Show that every finite extension of a finite field F is simple; that is, if E is a finite extension of a finite field F, prove that there exists an $\alpha \in E$ such that $E = F(\alpha)$.

Solution. Corollary 22.9.

20. Show that for every n there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.

Solution. Induct on n.

21. Prove that the **Frobenius map** $\Phi : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ given by $\Phi : \alpha \mapsto \alpha^p$ is an automorphism of order n.

Solution. Let $\alpha, \beta \in \mathrm{GF}(p^n)$. Applying the binomial theorem to $(a+b)^p$, we see that

$$\Phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \cdots + \binom{p}{k}\alpha^{p-k}\beta^k + \cdots + \beta^p,$$

where

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Since all of the intermediate terms are divisible by p, we have

$$\Phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \Phi(\alpha) + \Phi(\beta).$$

Since $\Phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \Phi(\alpha)\Phi(\beta)$, ϕ is a homomorphism. If $\Phi(\alpha) = 0$, then $\alpha = 0$, since the multiplicative group of $\mathrm{GF}(p^n)$ is closed under multiplication. Thus, Φ is one-to-one. Since $\mathrm{GF}(p^n)$ is finite, the homomorphism must also be onto.

To show that Φ has order n, we first show that $\Phi^k(\alpha) = \alpha^{p^k}$. Clearly,

$$\Phi^1(\alpha) = \Phi(\alpha) = \alpha^p.$$

Since

$$\Phi^{r+1}(\alpha) = \Phi\Phi^r(\alpha) = \Phi(\alpha^{p^r}) = \alpha^{p^{r+1}},$$

the result follows from mathematical induction. By Theorem 22.6, $\Phi^n(\alpha) = \alpha^{p^n} = \alpha$, since the elements of $\mathrm{GF}(p^n)$ are the roots of $x^{p^n} - x \in \mathbb{Z}_p[x]$. Now suppose that $\Phi^k(\alpha) = \alpha$ for all $\alpha \in \mathrm{GF}(p^n)$. Thus, $\alpha^{p^k} - \alpha = 0$ for all α. Therefore, each α is a root of $x^{p^k} - x$. Consequently, $k \geq n$.

22. Show that every element in $\mathrm{GF}(p^n)$ can be written in the form a^p for some unique $a \in \mathrm{GF}(p^n)$.

Solution. Use Exercise 21.

23. Let E and F be subfields of $\mathrm{GF}(p^n)$. If $|E| = p^r$ and $|F| = p^s$, what is the order of $E \cap F$?

Solution. The order of $E \cap F$ is $|E \cap F| = p^d$, where $d = \gcd(r, s)$.

24. Wilson's Theorem. Let p be prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.

Hint. Factor $x^{p-1} - 1$ over $\mathbb{Z}_p$.

Solution. Factor $x^{p-1} - 1$ over $\mathbb{Z}_p$.

25. If $g(t)$ is the minimal generator polynomial for a cyclic code C in R_n, prove that the constant term of $g(x)$ is 1.

Solution. $g(x)$ must divide $x^n - 1$.

26. Often it is conceivable that a burst of errors might occur during transmission, as in the case of a power surge. Such a momentary burst of interference might alter several consecutive bits in a codeword. Cyclic codes permit the detection of such error bursts. Let C be an (n, k)-cyclic code. Prove that any error burst up to $n - k$ digits can be detected.

Solution. Let C be a cyclic code. Suppose that x is a received n-tuple with $n - k$ consecutive errors. Show that if x were in C, then every other n-tuple must also be in C.

27. Prove that the rings R_n and $\mathbb{Z}_2^n$ are isomorphic as vector spaces.

Solution. Use the map $\phi : R_n \to \mathbb{Z}_2^n$ given by $\phi(a_0 + a_1t + \cdots + a_{n-1}t^{n-1}) = (a_0, a_1, \ldots, a_{n-1})$.

28. Let C be a code in R_n that is generated by $g(t)$. If $\langle f(t)\rangle$ is another code in R_n, show that $\langle g(t)\rangle \subset \langle f(t)\rangle$ if and only if $f(x)$ divides $g(x)$ in $\mathbb{Z}_2[x]$.

Solution. Use Lemma 16.7 and the fact that $\mathbb{Z}_2[x]$ is a PID.

29. Let $C = \langle g(t)\rangle$ be a cyclic code in R_n and suppose that $x^n - 1 = g(x)h(x)$, where $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ and $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Define G to be the $n \times k$ matrix

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{pmatrix}$$

and H to be the $(n-k) \times n$ matrix

$$H = \begin{pmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(a) Prove that G is a generator matrix for C.

(b) Prove that H is a parity-check matrix for C.

(c) Show that $HG = 0$.

Solution.

(a) G is a generator matrix for C, since $\{g(x), xg(x), \ldots, x^{n-k}g(x)\}$ is a basis for C.

(b) If $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ is a codeword, then show that

$$\begin{aligned} c_{n-k}h_k + \cdots + c_n h_0 &= 0 \\ c_{n-k-1}h_k + \cdots + c_{n-1}h_0 &= 0 \\ &\vdots \\ c_0 h_k + \cdots + c_k h_0 &= 0. \end{aligned}$$

(c) Combine parts (a) and (b).

22.6 Sage Exercises

1. Create a finite field of order 5^2 and then factor $p(x) = x^{25} - x$ over this field. Comment on what is interesting about this result and why it is not a surprise.

Solution. By Theorem 22.6 we expect this polynomial to split in this field, and thus every element of the field appears in exactly one linear factor.

```
F.<a> = GF(5^2)
x = polygen(F, 'x')
poly = x^25-x
poly.factor()
```

```
x * (x + 1) * (x + 2) * (x + 3) * (x + 4) *
(x + a) * (x + a + 1) * (x + a + 2) * (x + a + 3) * (x + a +
    4) *
(x + 2*a) * (x + 2*a + 1) * (x + 2*a + 2) * (x + 2*a + 3) *
    (x + 2*a + 4) *
(x + 3*a) * (x + 3*a + 1) * (x + 3*a + 2) * (x + 3*a + 3) *
    (x + 3*a + 4) *
(x + 4*a) * (x + 4*a + 1) * (x + 4*a + 2) * (x + 4*a + 3) *
    (x + 4*a + 4)
```

2. Corollary 22.11 says that the nonzero elements of a finite field are a cyclic group under multiplication. The generator used in Sage is also a generator of this multiplicative group. To see this, create a finite field of order 2^7. Create two lists of the elements of the field: first, use the `.list()` method, then use a

list comprehension to generate the proper powers of the generator you specified when you created the field.

The second list should be the whole field, but will be missing zero. Create the zero element of the field (perhaps by coercing 0 into the field) and `.append()` it to the list of powers. Apply the `sorted()` command to each list and then test the lists for equality.

Solution.

```
F.<a> = GF(2^7)
z = F.multiplicative_generator()
powers = [F(0)] + [z^i for i in range(2^7-1)]
Flist = F.list()
sorted(powers) == sorted(Flist)
```

```
True
```

3. Subfields of a finite field are completely classified by Theorem 22.7. It is possible to create two finite fields of the correct orders for the supefield/subfield realtionship to hold, and to translate between one and the other. However, in this exercise we will create a subfield of a finite field from scratch. Since the group of nonzero elements in a finite field is cyclic, the nonzero elements of a subfield will form a subgroup of the cyclic group, and necessarily will be cyclic.

Create a finite field of order 3^6. Theory says there is a subfield of order 3^2, since $2|6$. Determine a generator of multiplicative order 8 for the nonzero elements of this subfield, and construct these 8 elements. Add in the field's zero element to this list. It should be clear that this set of 9 elements is closed under multiplication. Absent our theorems about finite fields and cyclic groups, the closure under addition is not a given. Write a single statement that checks if this set is also closed under addition, by considering all possible sums of elements from the set.

Solution.

```
F.<a> = GF(3^6)
b = a^((3^6-1)/(3^2-1))
b.multiplicative_order()
```

```
8
```

```
B = [F(0)] + [b^i for i in srange(3^2-1)]
all([x + y in B for x in B for y in B])
```

```
True
```

4. This problem investigates the "separableness" of $\mathbb{Q}(\sqrt{3}, \sqrt{7})$. You can create this number field quickly with the `NumberFieldTower` constructor, along with the polynomials x^2-3 and x^2-7. Flatten the tower with the `.absolute_field()` method and use the `.structure()` method to retrieve mappings between the tower and the flattened version. Name the tower `N` and use `a` and `b` as generators. Name the flattened version `L` with `c` as a generator.

Create a nontrivial ("random") element of `L` using as many powers of `c` as possible (check the degree of `L` to see how many linearly independent powers there are). Request from Sage the minimum polynomial of your random element, thus ensuring the element is a root. Construct the minimum polynomial as a polynomial over `N`, the field tower, and find its factorization. Your factorization should have only linear factors. Each root should be an expression in `a` and `b`, so convert each root into an expression with mathematical notation

involving $\sqrt{3}$ and $\sqrt{7}$. Use one of the mappings to verify that one of the roots is indeed the original random element.

Create a few more random elements, and find a factorization (in `N` or in `L`). For a field to be separable, every element of the field should be a root of *some* separable polynomial. The minimal polynomial is a good polynomial to test. (Why?) Based on the evidence, does it appear that $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ is a separable extension?

Solution.

```
x = var('x')
N.<a,b> = NumberFieldTower([x^2-3, x^2-7])
L.<c> = N.absolute_field()
L
```

```
Number Field in c with defining polynomial x^4 - 20*x^2 + 16
```

`a` and `b` are, respectively, $\sqrt{3}$ and $\sqrt{7}$.

```
a^2, b^2
```

```
(3, 7)
```

`r` is arbitrary, though uses up to a third power of the generator `c`.

```
r = 34*c^3 + 2*c^2 - 8*c + 23
p = r.minpoly()
p
```

```
x^4 - 172*x^3 - 7928906*x^2 + 391486836*x - 2076481263
```

```
y = polygen(N, 'y')
q = y^4 - 172*y^3 - 7928906*y^2 + 391486836*y - 2076481263
q.factor()
```

```
(y + (-4*b - 808)*a - 536*b - 43) *
(y + (4*b - 808)*a + 536*b - 43) *
(y + (4*b + 808)*a - 536*b - 43) *
(y + (-4*b + 808)*a + 536*b - 43)
```

```
fromL, toL = L.structure()
roots = [
    -((-4*b - 808)*a - 536*b - 43),
    -((4*b - 808)*a + 536*b - 43),
    -((4*b + 808)*a - 536*b - 43),
    -((-4*b + 808)*a + 536*b - 43)]
rootsL = [toL(root) for root in roots]
rootsL
```

```
[168*c^3 -  2*c^2 - 3224*c + 63,
  34*c^3 +  2*c^2 - 8*c +    23,
 -34*c^3 +  2*c^2 + 8*c +    23,
 -168*c^3 - 2*c^2 + 3224*c + 63]
```

You might notice the field automorphism $c \to -c$ creating an order 2 permutation of the 4 roots, presaging results from Galois Theory in the next chapter.

```
rootsL.index(r)
```

```
1
```

So our original, arbitrary, element is the second item in the list of roots, converted to expressions in the lone generator `c` of the flattened tower.

5. Exercise 22.3.21 describes the Frobenius Map, an automorphism of a finite field. If `F` is a finite field in Sage, then `End(F)` will create the automorphism group of F, the set of all bijective mappings between the field and itself.

(a) Work Exercise 22.3.21 to gain an understanding of how and why the Frobenius mapping is a field automorphism. (Do not include any of this in your answer to this question, but understand that the following will be much easier if you do this problem first.)

(b) For some small, but not trivial, finite fields locate the Frobenius map in the automorphism group. Small might mean $p = 2, 3, 5, 7$ and $3 \leq n \leq 10$, with n prime versus composite.

(c) Once you have located the Frobenius map, describe the other automorphisms. In other words, with a bit of investigation, you should find a description of the automorphisms which will allow you to accurately predict the entire automorphism group for a finite field you have not already explored. (Hint: the automorphism group is a group. What if you "do the operation" between the Frobenius map and itself? Just what is the operation? Try using Sage's multiplicative notation with the elements of the automorphism group.)

(d) What is the "structure" of the automorphism group? What special status does the Frobenius map have in this group?

(e) For any field, the subfield known as the fixed field is an important construction, and will be especially important in the next chapter. Given an automorphism τ of a field E, the subset, $K = \{b \in E \mid \tau(b) = b\}$, can be shown to be a subfield of E. It is known as the **fixed field** of τ in E. For each automorphism of $E = GF(3^6)$ identify the fixed field of the automorphism. Since we understand the structure of subfields of a finite field, it is enough to just determine the order of the fixed field to be able to identify the subfield precisely.

Solution.

```
F.<a> = GF(3^6)
G = End(F)
G.list()
```

```
[
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> a,
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> a^3,
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> a^4 + a^2 + a,
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> 2*a^5 + 2*a^4 + 2*a + 1,
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> 2*a^5 + 2*a^4 + 2*a^3,
Ring endomorphism of Finite Field in a of size 3^6
  Defn: a |--> 2*a^5 + a^4 + 2*a^2 + 2*a + 2
]
```

The group of automorphisms is cyclic. The identity map is first, followed by a generator, the Frobenius map, ϕ. Then, for example,

$$\phi^2(a) = \phi(\phi(a)) = \phi\left(a^3\right) = \left(a^3\right)^3 = a^9 = a^4 + a^2 + a$$

which we recognize as the third element in the group.

```
frob = G[1]
frob^2 == G[2]
```

```
True
```

As a cyclic group of order 6 the even powers of the generator form a subgroup of order 3. The zero power produces an identity map, but it does not play nicely with the group (see error below), so we use the sixth power instead.

```
G(frob^0)
```

```
Traceback (most recent call last):
...
TypeError: unable to convert Identity endomorphism of Finite
    Field in a of size 3^6 to an element of Finite Field in a
    of size 3^6
```

```
G.multiplication_table(elements=[frob^6, frob^2, frob^4])
```

```
*  a b c
 +------
a| a b c
b| b c a
c| c a b
```

The sizes of the fixed fields are allowable powers of the prime 3.

```
[len([x for x in F if tau(x) == x]) for tau in G]
```

```
[729, 3, 9, 27, 9, 3]
```

6. Exercise 22.3.15 suggests that every element of a finite field may be written (expressed) as a sum of squares. This exercise suggests computational experiments which might help you formulate a proof for the exercise.

(a) Construct two small, but not too small, finite fields, one with $p = 2$ and the other with an odd prime. Repeat the following for each field, F.

(b) Choose a "random" element of the field, say $a \in F$. Construct the sets

$$\{x^2 | x \in F\} \qquad \{a - x^2 | x \in F\}$$

using Sage sets with the $Set()$ constructor. (Be careful: `set()` is a Python command which behaves differently in fundamental ways.)

(c) Examine the size of the two sets and the size of their intersection (`.intersection()`). Try different elements for a, perhaps writing a loop to try *all* possible values. Note that $p = 2$ will behave quite differently.

(d) Suppose you have an element of the intersection. (You can get one with `.an_element()`.) How does this lead to the sum of squares proposed in the exercise?

(e) Can you write a Python function that accepts a finite field whose order is a power of an odd prime and then lists each element as a sum of squares?

Solution.

```
def sum_of_squares(F):
    for z in F:
        sq = Set([x^2 for x in F])
        sqq = Set([z-x^2 for x in F])
        y = sq.intersection(sqq).an_element()
        first = sqrt(y)
        second = sqrt(z-y)
        print(z == first^2 + second^2, "{} = ({})^2 + ({})^2".format(z, first,  second))
```

```
F.<a> = GF(3^2)
sum_of_squares(F)
```

```
True 0 = (0)^2 + (0)^2
True a = (a + 1)^2 + (a)^2
True a + 1 = (0)^2 + (a)^2
True 2*a + 1 = (2*a + 1)^2 + (a + 1)^2
True 2 = (0)^2 + (a + 1)^2
True 2*a = (2*a + 1)^2 + (1)^2
True 2*a + 2 = (2*a + 1)^2 + (0)^2
True a + 2 = (1)^2 + (a)^2
True 1 = (0)^2 + (1)^2
```

Chapter 23

Galois Theory

23.4 Exercises

1. Compute each of the following Galois groups. Which of these field extensions are normal field extensions? If the extension is not normal, find a normal extension of $\mathbb{Q}$ in which the extension field is contained.

(a) $G(\mathbb{Q}(\sqrt{30})/\mathbb{Q})$

(b) $G(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q})$

(c) $G(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$

(d) $G(\mathbb{Q}(\sqrt{2},\sqrt[3]{2},i)/\mathbb{Q})$

(e) $G(\mathbb{Q}(\sqrt{6},i)/\mathbb{Q})$

Hint. (a) $\mathbb{Z}_2$; (c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution.

(a) $\mathbb{Z}_2$

(b) Although $G(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}) \cong \mathbb{Z}_2$, $\mathbb{Q}(\sqrt[4]{5})$ is not a normal extension of $\mathbb{Q}$. A normal extension is $\mathbb{Q}(\sqrt[4]{5}, i)$. As in Example 23.24, it can be shown $G(\mathbb{Q}(\sqrt[4]{5}, i)/\mathbb{Q}) \cong D_4$.

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

(d) $S_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

(e) Although $G(\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i)/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, the field $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i)$ is not a normal extension of $\mathbb{Q}$. A normal extension is $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i, \omega)$, where $\omega^2 + \omega + 1 = 0$. In this case, $G(\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i, \omega)/\mathbb{Q}) \cong S_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Determine the separability of each of the following polynomials.

(a) $x^3 + 2x^2 - x - 2$ over $\mathbb{Q}$

(b) $x^4 + 2x^2 + 1$ over $\mathbb{Q}$

(c) $x^4 + x^2 + 1$ over $\mathbb{Z}_3$

(d) $x^3 + x^2 + 1$ over $\mathbb{Z}_2$

Hint. (a) Separable over $\mathbb{Q}$ since $x^3 + 2x^2 - x - 2 = (x-1)(x+1)(x+2)$; (c) not separable over $\mathbb{Z}_3$ since $x^4 + x^2 + 1 = (x+1)^2(x+2)^2$.

Solution.

(a) Separable over $\mathbb{Q}$ since $x^3 + 2x^2 - x - 2 = (x-1)(x+1)(x+2)$

(b) Not separable over $\mathbb{Q}$ since $x^4 + 2x^2 + 1 = (x^2+1)^2$.

(c) Not separable over $\mathbb{Z}_3$ since $x^4 + x^2 + 1 = (x + 1)^2(x + 2)^2$.

(d) Separable over $\mathbb{Z}_2$ since $x^3+x^2+1 = (x+\alpha+1)(x+\alpha^2+1)(x+\alpha^2+\alpha+1)$, where

$$\alpha \in \mathrm{GF}(2^3) = \{a_0 + a_1\alpha + a_2\alpha^2 : a_i \in \mathbb{Z}_2 \text{ and } \alpha^3 + \alpha^2 + 1 = 0\}.$$

3. Give the order and describe a generator of the Galois group of GF(729) over GF(9).

Hint. If

$$[\mathrm{GF}(729) : \mathrm{GF}(9)] = [\mathrm{GF}(729) : \mathrm{GF}(3)]/[\mathrm{GF}(9) : \mathrm{GF}(3)] = 6/2 = 3,$$

then $G(\mathrm{GF}(729)/\mathrm{GF}(9)) \cong \mathbb{Z}_3$. A generator for $G(\mathrm{GF}(729)/\mathrm{GF}(9))$ is σ, where $\sigma_{3^6}(\alpha) = \alpha^{3^6} = \alpha^{729}$ for $\alpha \in \mathrm{GF}(729)$.

Solution. If

$$[\mathrm{GF}(729) : \mathrm{GF}(9)] = [\mathrm{GF}(729) : \mathrm{GF}(3)]/[\mathrm{GF}(9) : \mathrm{GF}(3)] = 6/2 = 3,$$

then $G(\mathrm{GF}(729)/\mathrm{GF}(9)) \cong \mathbb{Z}_3$. A generator for $G(\mathrm{GF}(729)/\mathrm{GF}(9))$ is σ, where $\sigma_{3^6}(\alpha) = \alpha^{3^6} = \alpha^{729}$ for $\alpha \in \mathrm{GF}(729)$.

4. Determine the Galois groups of each of the following polynomials in $\mathbb{Q}[x]$; hence, determine the solvability by radicals of each of the polynomials.

(a) $x^5 - 12x^2 + 2$

(b) $x^5 - 4x^4 + 2x + 2$

(c) $x^3 - 5$

(d) $x^4 - x^2 - 6$

(e) $x^5 + 1$

(f) $(x^2 - 2)(x^2 + 2)$

(g) $x^8 - 1$

(h) $x^8 + 1$

(i) $x^4 - 3x^2 - 10$

Hint. (a) S_5; (c) S_3; (g) see Example 23.10.

Solution.

(a) S_5

(b) S_5

(c) S_3

(d) $\mathbb{Z}_2 \times \mathbb{Z}_2$

(e) $\mathbb{Z}_5$

(f) $\mathbb{Z}_2 \times \mathbb{Z}_2$

(g) The roots of $f(x) = x^8 - 1$ are ω^i, where $i = 1, \ldots, 8$ and

$$\omega = \cos(2\pi/8) + i\sin(2\pi/8) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Hence, the splitting field of $f(x)$ must be $\mathbb{Q}(\omega)$. We can define automorphisms σ_i of $\mathbb{Q}(\omega)$ by $\sigma_i(\omega) = \omega^i$ for $i = 1, \ldots, 8$. It is easy to check that these are indeed distinct automorphisms in $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Since

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = |G(\mathbb{Q}(\omega)/\mathbb{Q})| = 4,$$

the σ_i's must be all of $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Since $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{2}, i)$, we know that the Galois group of $f(x) = x^8 - 1$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(h) $\mathbb{Z}_8$

(i) $\mathbb{Z}_8$

5. Find a primitive element in the splitting field of each of the following polynomials in $\mathbb{Q}[x]$.

(a) $x^4 - 1$

(b) $x^4 - 8x^2 + 15$

(c) $x^4 - 2x^2 - 15$

(d) $x^3 - 2$

Hint. (a) $\mathbb{Q}(i)$

Solution.

(a) $\mathbb{Q}(i)$

(b) $\mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$

(c) $\mathbb{Q}(\sqrt{5} + \sqrt{3}\,i)$

(d) $\mathbb{Q}(\omega)$, where ω is one of the nonreal cube roots of 2.

6. Prove that the Galois group of an irreducible quadratic polynomial is isomorphic to $\mathbb{Z}_2$.

Solution. Any element in the Galois group of $f(x) = ax^2 + bx + c$ must permute the roots of $f(x)$. However, the roots can easily be determined by the quadratic formula.

7. Prove that the Galois group of an irreducible cubic polynomial is isomorphic to S_3 or $\mathbb{Z}_3$.

Hint. Let E be the splitting field of a cubic polynomial in $F[x]$. Show that $[E : F]$ is less than or equal to 6 and is divisible by 3. Since $G(E/F)$ is a subgroup of S_3 whose order is divisible by 3, conclude that this group must be isomorphic to $\mathbb{Z}_3$ or S_3.

Solution. Let E be the splitting field of a cubic polynomial in $F[x]$. Show that $[E : F]$ is less than or equal to 6 and is divisible by 3. Since $G(E/F)$ is a subgroup of S_3 whose order is divisible by 3, conclude that this group must be isomorphic to $\mathbb{Z}_3$ or S_3.

8. Let $F \subset K \subset E$ be fields. If E is a normal extension of F, show that E must also be a normal extension of K.

Solution. The proof is straight forward from the definition of a normal extension.

9. Let G be the Galois group of a polynomial of degree n. Prove that $|G|$ divides $n!$.

Hint. G is a subgroup of S_n.

Solution. G is a subgroup of S_n.

10. Let $F \subset E$. If $f(x)$ is solvable over F, show that $f(x)$ is also solvable over E.

Solution. Use the fact that any subgroup of a solvable group is also solvable (Chapter 13, Exercise 14) together with the Fundamental Theorem of Galois Theory.

11. Construct a polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree 7 that is not solvable by radicals.

Solution. $(x^2+1)p(x)$, where $p(x)$ is a polynomial with five real non-rational roots.

12. Let p be prime. Prove that there exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree p with Galois group isomorphic to S_p. Conclude that for each prime p with $p \geq 5$ there exists a polynomial of degree p that is not solvable by radicals.

Solution. Find a polynomial with 2 complex roots and $p-2$ real nonrational roots.

13. Let p be a prime and $\mathbb{Z}_p(t)$ be the field of rational functions over $\mathbb{Z}_p$. Prove that $f(x) = x^p - t$ is an irreducible polynomial in $\mathbb{Z}_p(t)[x]$. Show that $f(x)$ is not separable.

Solution. There is an excellent proof of this result in Fraleigh's book, *A First Course in Abstract Algebra*.

14. Let E be an extension field of F. Suppose that K and L are two intermediate fields. If there exists an element $\sigma \in G(E/F)$ such that $\sigma(K) = L$, then K and L are said to be **conjugate fields.** Prove that K and L are conjugate if and only if $G(E/K)$ and $G(E/L)$ are conjugate subgroups of $G(E/F)$.

Solution. Look at the proof of (4) in the proof of the Fundamental Theorem of Galois Theory.

15. Let $\sigma \in \mathrm{Aut}(\mathbb{R})$. If a is a positive real number, show that $\sigma(a) > 0$.

Solution. If $a > 0$, then there exists a $b \in \mathbb{R}$ such that $b^2 = a$. Thus, $\sigma(a) = \sigma(b^2) = [\sigma(b)]^2 > 0$.

16. Let K be the splitting field of $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Prove or disprove that K is an extension by radicals.

Hint. True.

Solution. True.

17. Let F be a field such that $\mathrm{char}\, F \neq 2$. Prove that the splitting field of $f(x) = ax^2 + bx + c$ is $F(\sqrt{\alpha}\,)$, where $\alpha = b^2 - 4ac$.

Solution. Look at the quadratic formula.

18. Prove or disprove: Two different subgroups of a Galois group will have different fixed fields.

Solution. False, by the Fundamental Theorem of Galois Theory.

19. Let K be the splitting field of a polynomial over F. If E is a field extension of F contained in K and $[E : F] = 2$, then E is the splitting field of some polynomial in $F[x]$.

Solution. If $\{1, \alpha\}$ is a basis for E over F, then E is the splitting field of $x^2 - \alpha^2$.

20. We know that the cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$ for every prime p. Let ω be a zero of $\Phi_p(x)$, and consider the field $\mathbb{Q}(\omega)$.

(a) Show that $\omega, \omega^2, \ldots, \omega^{p-1}$ are distinct zeros of $\Phi_p(x)$, and conclude that they are all the zeros of $\Phi_p(x)$.

(b) Show that $G(\mathbb{Q}(\omega)/\mathbb{Q})$ is abelian of order $p - 1$.

(c) Show that the fixed field of $G(\mathbb{Q}(\omega)/\mathbb{Q})$ is $\mathbb{Q}$.

Hint.

(a) Clearly $\omega, \omega^2, \ldots, \omega^{p-1}$ are distinct since $\omega \neq 1$ or 0. To show that ω^i is a zero of Φ_p, calculate $\Phi_p(\omega^i)$.

(b) The conjugates of ω are $\omega, \omega^2, \ldots, \omega^{p-1}$. Define a map $\phi_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ by

$$\phi_i(a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}) = a_0 + a_1\omega^i + \cdots + c_{p-2}(\omega^i)^{p-2},$$

where $a_i \in \mathbb{Q}$. Prove that ϕ_i is an isomorphism of fields. Show that ϕ_2 generates $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

(c) Show that $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, and consider which linear combinations of $\omega, \omega^2, \ldots, \omega^{p-1}$ are left fixed by all elements of $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

Solution.

(a) Clearly $\omega, \omega^2, \ldots, \omega^{p-1}$ are distinct since $\omega \neq 1$ or 0. To show that ω^i is a zero of Φ_p, calculate $\Phi_p(\omega^i)$.

(b) The conjugates of ω are $\omega, \omega^2, \ldots, \omega^{p-1}$. Define a map $\phi_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ by

$$\phi_i(a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}) = a_0 + a_1\omega^i + \cdots + c_{p-2}(\omega^i)^{p-2},$$

where $a_i \in \mathbb{Q}$. Prove that ϕ_i is an isomorphism of fields. Show that ϕ_2 generates $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

(c) Show that $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, and consider which linear combinations of $\omega, \omega^2, \ldots, \omega^{p-1}$ are left fixed by all elements of $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

21. Let F be a finite field or a field of characteristic zero. Let E be a finite normal extension of F with Galois group $G(E/F)$. Prove that $F \subset K \subset L \subset E$ if and only if $\{\text{id}\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.

Solution. Use Part (1) of the Fundamental Theorem of Galois Theory and the fact that if $\sigma \in G(E/F)$ fixes L then it must also fix K.

22. Let F be a field of characteristic zero and let $f(x) \in F[x]$ be a separable polynomial of degree n. If E is the splitting field of $f(x)$, let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in E. Let $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. We define the **discriminant** of $f(x)$ to be Δ^2.

(a) If $f(x) = x^2 + bx + c$, show that $\Delta^2 = b^2 - 4c$.

(b) If $f(x) = x^3 + px + q$, show that $\Delta^2 = -4p^3 - 27q^2$.

(c) Prove that Δ^2 is in F.

(d) If $\sigma \in G(E/F)$ is a transposition of two roots of $f(x)$, show that $\sigma(\Delta) = -\Delta$.

(e) If $\sigma \in G(E/F)$ is an even permutation of the roots of $f(x)$, show that $\sigma(\Delta) = \Delta$.

(f) Prove that $G(E/F)$ is isomorphic to a subgroup of A_n if and only if $\Delta \in F$.

(g) Determine the Galois groups of $x^3 + 2x - 4$ and $x^3 + x - 3$.

Solution.

(a) The roots of $x^2 + bx + c$ are $\alpha = (-b + \sqrt{b^2 - 4c})/2$ and $\beta = (-b - \sqrt{b^2 - 4c})/2$. Therefore, $\Delta = \alpha - \beta = \sqrt{b^2 - 4c}$ and the discriminant is $\Delta^2 = b^2 - 4c$.

(b) Suppose that the roots of $f(x) = x^3 + px + q$ are u, v, and w. Refering to the cubic formula in the additional exercises at the end of Chapter 17 (Polynomials), we see that

$$u = \alpha + \beta, \qquad v = \omega\alpha + \omega^2\beta, \qquad w = \omega^2\alpha + \omega\beta,$$

where

$$\begin{aligned}
\omega &= \frac{-1 + \sqrt{3}\, i}{2} \\
\omega^2 &= \frac{-1 - \sqrt{3}\, i}{2} \\
\omega^3 &= 1 \\
D &= \frac{p^3}{27} + \frac{q^2}{4} \\
\alpha &= \left(-\frac{q}{2} + \sqrt{D}\right)^{1/3} \\
\beta &= \left(-\frac{q}{2} - \sqrt{D}\right)^{1/3}
\end{aligned}$$

A straightforward calculation shows that

$$\begin{aligned}
u - v &= \alpha + \beta - \omega\alpha - \omega^2\beta = (1 - \omega)(\alpha - \omega^2\beta) \\
u - w &= \alpha + \beta - \omega^2\alpha - \omega\beta = -\omega^2(1 - \omega)(\alpha - \omega\beta) \\
v - w &= \omega\alpha + \omega^2\beta - \omega^2\alpha - \omega\beta = \omega(1 - \omega)(\alpha - \beta).
\end{aligned}$$

Consequently,

$$\begin{aligned}
\Delta &= (u - v)(u - w)(v - w) \\
&= -\omega^3(1 - \omega)^3(\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta).
\end{aligned}$$

Noting that $\omega^3 = 1$ and $(1 - \omega)^3 = -3(\omega - \omega^2) = -3\sqrt{3}$, we can further conclude that

$$\Delta = 3\sqrt{3}\, i(\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^{\,2}\beta).$$

Since

$$\begin{aligned}
(\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta) &= (\alpha - \beta)[\alpha^2 - (\omega + \omega^2)\alpha\beta + \beta^2] \\
&= (\alpha - \beta)[\alpha^2 + \alpha\beta + \beta^2] \\
&= \alpha^3 - \beta^3 \\
&= \left(-\frac{q}{2} + \sqrt{D}\right) - \left(-\frac{q}{2} - \sqrt{D}\right) \\
&= 2\sqrt{D},
\end{aligned}$$

we know that

$$\Delta^2 = -27 \cdot 4D = -4p^3 - 27q^2.$$

(c) If $\sigma \in G(E/F)$, then σ will permute the roots of $f(x)$. That is, $\sigma : \alpha_i \mapsto \alpha_{\sigma(i)}$. Thus,

$$\sigma(\Delta) = \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}).$$

Since σ is a permutation, each factor $\alpha_i - \alpha_j$ of Δ appears in $\sigma(\Delta)$ as either $\alpha_i - \alpha_j$ or $\alpha_j - \alpha_i$. Thus, $\sigma(\Delta) = \pm\Delta$ or $\sigma(\Delta^2) = \Delta^2$.

(d) Without loss of generality, we may assume that $\sigma = (12)$. Then

$$\begin{aligned}
\sigma(\Delta) &= \sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) \\
&= \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) \\
&= (\alpha_2 - \alpha_1) \prod_{\substack{i<j \\ i\neq 1, j\neq 2}} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) \\
&= -(\alpha_1 - \alpha_2) \prod_{\substack{i<j \\ i\neq 1, j\neq 2}} (\alpha_i - \alpha_j) \\
&= -\prod_{i<j}(\alpha_i - \alpha_j) \\
&= -\Delta.
\end{aligned}$$

(e) Suppose that σ is an even permutation. Then $\sigma = \tau_1\tau_2\cdots\tau_{2k}$ is the product of an even number of transpositions. Hence, $\sigma(\Delta) = (-1)^{2k}\Delta = \Delta$ by part (d).

(f) First note that $\Delta \neq -\Delta$, since F has characteristic zero. Suppose that $\sigma \in G(E/F)$ is a subgroup of A_n. If $\sigma \in G(E/F)$, then it must be an even permutation of the roots of $f(x)$. By part (e), $\sigma(\Delta) = \Delta$ and $\Delta \in F$. Conversely, suppose that $\Delta \in F$ and $\sigma \in G(E/F)$. If σ is not even, then we can write it as $\sigma = \tau\mu$, where τ is a transpostion and μ is an even permutation. By part (d), $\sigma(\Delta) = \tau\mu(\Delta) = \tau(\Delta) = -\Delta$, which tells us that σ does not fix Δ, which contradicts the fact that $\sigma \in G(E/F)$. Therefore, $\sigma \in A_n$.

(g) The discriminants of $x^3 + 2x - 4$ and $x^3 + x - 3$ are $\Delta = 4\sqrt{29}\,i$ and $\Delta = \sqrt{247}\,i$, respectively. Since $\Delta \notin \mathbb{Q}$ for either polynomial, the Galois group of each polynomial cannot be A_3 or the identity and must either be a subgroup of order 2 of S_3 or all of S_3. However, if the Galois group is of order 2, one root must be in $\mathbb{Z}$. Since this is not the case, S_3 is the Galois group of both polynomials.

23.6 Sage Exercises

1. In the analysis of Example 23.24 with Sage, two subgroups of order 2 and one subgroup of order 4 were not analyzed. Determine the fixed fields of these three subgroups.

2. Build the splitting field of $p(x) = x^3 - 6x^2 + 12x - 10$ and then determine the Galois group of $p(x)$ as a concrete group of explicit permutations. Build the lattice of subgroups of the Galois group, again using the same explicit permutations. Using the Fundamental Theorem of Galois Theory, construct the subfields of the splitting field. Include your supporting documentation in your submitted Sage worksheet. Also, submit a written component of this assignment containing a complete layout of the subgroups and subfields, written entirely with mathematical notation and with no Sage commands, designed to illustrate the correspondence between the two. All you need here is the graphical layout, suitably labeled — the Sage worksheet will substantiate your work.

3. The polynomial $x^5 - x - 1$ has all of the symmetric group S_5 as its Galois group. Because S_5 is not solvable, we know this polynomial to be an example of a quintic polynomial that is not solvable by radicals. Unfortunately, asking Sage to compute this Galois group takes far too long. So this exercise will simulate that experience with a slightly smaller example.

Consider the polynomial $p(x) = x^4 + x + 1$.

(a) Build the splitting field of $p(x)$ one root at a time. Create an extension, factor there, discard linear factors, use the remaining irreducible factor to extend once more. Repeat until $p(x)$ factors completely. Be sure to do a final extension via just a linear factor. This is a little silly, and Sage will seem to ignore your final generator (so you will want to setermine what it is equivalent to in terms of the previous gfenerators). Directions below depend on taking this extra step.

(b) Factor the original polynomial over the final extension field in the tower. What is boring about this factorization in comparison to some other examples we have done?

(c) Construct the full tower as an absolute field over $\mathbb{Q}$. From the degree of this extension and the degree of the original polynomial, infer the Galois group of the polynomial.

(d) Using the mappings that allow you to translate between the tower and the absolute field (obtained from the `.structure()` method), choose one of the roots (any one) and express it in terms of the single generator of the absolute field. Then reverse the procedure and express the single generator of the absolute field in terms of the roots in the tower.

(e) Compute the group of automorphisms of the absolute field (but don't display the whole group in what you submit). Take all four roots (including your silly one from the last step of the tower construction) and apply each field automorphism to the four roots (creating the guaranteed permutations of the roots). Comment on what you see.

(f) There is one nontrivial automorphism that has an especially simple form (it is the second one for me) when applied to the generator of the absolute field. What does this automorphism do to the roots of $p(x)$?

(g) Consider the extension of $\mathbb{Q}$ formed by adjoining just one of the roots. This is a subfield of the splitting field of the polynomial, so is the fixed field of a subgroup of the Galois group. Give a simple description of the corresponding subgroup using language we typically only apply to permutation groups.

4. Return to the splitting field of the quintic discussed in the introduction to the previous problem ($x^5 - x - 1$). Create the first two intermediate fields by adjoining two roots (one at a time). But instead of factoring at each step to get a new irreducible polynomial, *divide* by the linear factor you *know* is a factor. In general, the quotient might factor further, but in this exercise presume it does not. In other words, act as if your quotient by the linear factor is irreducible. If it is not, then the `NumberField()` command should complain (which it will not).

After adjoining two roots, create the extension producing a third root, and do the division. You should now have a quadratic factor. Assuming the quadratic is irreducible (it is) argue that you have enough evidence to establish the order of the Galois group, and hence can determine *exactly* which group it is.

You can try to use this quadratic factor to create one more step in the extensions, and you will arrive at the splitting field, as can be seen with logic or division. However, this could take a long time to complete (save your work beforehand!). You can try passing the `check=False` argument to the `NumberField()` command — this will bypass checking irreducibility.

5. Create the finite field of order 3^6, letting Sage supply the default polynomial for its construction. The polynomial $x^6 + x^2 + 2x + 1$ is irreducible over this finite field. Check that this polynomial splits in the finite field, and then use the `.roots()` method to collect the roots of the polynomial. Get the group of automorphisms of the field with the `End()` command.

You now have all of the pieces to associate each field automorphism with a permutation of the roots. From this, identify the Galois group and all of its subgroups. For each subgroup, determine the fixed field. You might find the roots easier to work with if you use the `.log()` method to identify them as powers of the field's multiplicative generator.

Your Galois group in this example will be abelian. So every subgroup is normal, and hence any extension is also normal. Can you extend this example by choosing a nontrivial intermediate field with a nontrivial irreducible polynomial that has all of its roots in the intermediate field and a nontrivial irreducible polynomial with none of its roots in the intermediate field?

Your results here are "typical" in the sense that the particular field or irreducible polynomial makes little difference in the qualitative nature of the results.

6. The splitting field for the irreducible polynomial $p(x) = x^7 - 7x + 3$ has degree 168 (hence this is the order of the Galois group). This polynomial is derived from an "Elkies trinomial curve," a hyperelliptic curve (below) that produces polynomials with interesting Galois groups:

$$y^2 = x(81x^5 + 396x^4 + 738x^3 + 660x^2 + 269x + 48)$$

For $p(x)$ the resulting Galois group is $PSL(2, 7)$, a simple group. If $SL(2, 7)$ is all 2×2 matrices over $\mathbb{Z}_7$ with determinant 1, then $PSL(2, 7)$ is the quotient by the subgroup $\{I_2, -I_2\}$. It is the second-smallest non-abelian simple group (after A_5).

See how far you can get in using Sage to build this splitting field. A degree 7 extension will yield one linear factor, and a subsequent degree 6 extension will yield two linear factors, leaving a quartic factor. Here is where the computations begin to slow down. If we believe that the splitting field has degree 168, then we know that adding a root from this degree 4 factor will get us to the splitting field. Creating this extension may be possible computationally, but verifying that the quartic splits into linear factors here seems to be infeasible.

7. Return to Example 23.24, and the complete list of subfields obtainable from the `.subfields()` method applied to the flattened tower. As mentioned, these are technically not subfields, but do have embeddings into the tower. Given two subfields, their respective primitive elements are embedded into the tower, with an image that is a linear combination of powers of the primitive element for the tower.

If one subfield is contained in the other, then the image of the primitive element for the smaller field should be a linear combination of the (appropriate) powers of the image of the primitive element for the larger field. This is a linear algebra computation that should be possible in the tower, relative to the power basis for the whole tower.

Write a procedure to determine if two subfields are related by one being a subset of the other. Then use this procedure to create the lattice of subfields. The eventual goal would be a graphical display of the lattice, using the existing plotting facilities available for lattices, similar to the top half of Figure 23.25. This is a "challenging" exercise, which is code for "it is speculative and has not been tested."