Selected Solutions for Students

to accompany

Abstract Algebra

Fourth Edition

JOHN A. BEACHY

WILLIAM D. BLAIR

For copies of this supplement, see the website *www.waveland.com* of
Waveland Press, Inc.
4180 IL Route 83, Suite 101
Long Grove, Illinois 60047
(847) 634-0081

Contents

TO THE STUDENT

The text contains a little over $1,000$ exercises. In "Selected Solutions for Students" we have written up complete solutions for a bit more than 10% of them. In many cases we chose these problems to solve because they play a significant role in the general development. Some of the longer problems could probably serve as a "project", taking you along a new pathway. We hope that having these solutions will encourage you to work on some problems that haven't been assigned.

The ideal way to use this set of solutions is to work on a solved exercise, and if you get stuck, uncover just enough of the solution to get started again. We can't emphasize enough that the aim of working on an exercise isn't just to solve the problem. The process is vitally important: it will probably involve a search for theorems in the text that might serve as tools; it may involve making up some examples of your own so that you really understand the question. Hopefully, everthing leading up to a solution will add to the material you have really mastered.

So, good luck, and only peek at the solutions as a last resort!

John Beachy
Bill Blair

1 INTEGERS

1.1. Divisors

17. Show that the positive integer k is the difference of two odd squares if and only if k is divisible by 8.

Solution: If $k = n^2 - m^2$, where m and n are odd integers, then as in Example 1.1.7 we can write $k = (2r + 1 + 2s + 1)(2r + 1 - 2s - 1) = (2)(r + s + 1)(2)(r - s)$ for some $r, s \in \mathbf{Z}$. Now we need to take two cases. First, if $r - s$ is even, then $r - s$ has 2 as a factor, and so k has 8 as a factor. Second, if $r - s$ is odd, then $r + s = (r - s) + (2s)$ is the sum of an odd integer and an even integer, so it must also be odd. That means that $r + s + 1$ is even, so it has 2 as a factor, and therefore k again has 8 as a factor. Showing that we can factor 8 out of $m^2 - n^2$ gives exactly what we were to prove: if m and n are odd, then $m^2 - n^2$ is divisible by 8.

Conversely, if $8 \mid k$, then $k = 8t$ for some $t \in \mathbf{Z}$, and so $(2t+1)^2 - (2t-1)^2 = 4t^2 + 4t + 1 - 4t^2 + 4t - 1 = 8t = k$.

18. Give a detailed proof of the statement in the text that if a and b are integers, then $b \mid a$ if and only if $a\mathbf{Z} \subseteq b\mathbf{Z}$.

Solution: Suppose that $b \mid a$. Then there exists $r \in \mathbf{Z}$ such that $a = br$. If $x \in a\mathbf{Z}$, then $x = at$ for some $t \in \mathbf{Z}$. Hence $x = at = (br)t = b(rt)$ and so $x \in b\mathbf{Z}$.

Conversely, suppose that $a\mathbf{Z} \subseteq b\mathbf{Z}$. Then since $a = a \cdot 1 \in a\mathbf{Z}$ we have $a \in b\mathbf{Z}$. Thus $a = bt$ for some $t \in \mathbf{Z}$ and so $b \mid a$.

1.2. Primes

18. Let a, b be nonzero integers with $(a, b) = 1$. Compute $(a + b, a - b)$.

Solution: Let $d = \gcd(a+b, a-b)$, and divide $a+b$ by $a-b$ to get $a+b = 1(a-b) + 2b$, which shows that $d = \gcd(a-b, 2b)$. Since $\gcd(a, b) = 1$, we can write $ma + nb = 1$ for some $m, n \in \mathbf{Z}$, and then $m(a-b) + (m+n)b = 1$. Because $d \mid (a-b)$, it follows that $\gcd(d, b) = 1$. But then $d \mid 2b$ implies, by Proposition 1.2.3 (b), that $d \mid 2$.
Case 1. If $a-b$ is even, then $\gcd(a-b, 2b) \geq 2$, so $d = 2$.
Case 2: If $a-b$ is odd, then $\gcd(a-b, 2) = 1$. The equation $m(a-b)+(m+n)b = 1$ shows that $\gcd(a-b, b) = 1$, so Proposition 1.2.3 (d) implies that $\gcd(a-b, 2b) = 1$, and therefore $d = 1$.

22. Show that if a, b are positive integers such that $(a, b) = 1$ and ab is a square, then a and b are also squares.

Solution: Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$. Since $\gcd(a, b) = 1$, no p_i is equal to a q_j. Now $ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} q_1^{\beta_1} \cdots q_s^{\beta_s}$ and the prime powers can be reordered to give the factorization of ab into distinct prime powers. Since ab is a square, each α_i and β_j is even, and hence a and b are squares.

30. If a, b, c are positive integers such that $a^2 + b^2 = c^2$, then (a, b, c) is called a Pythagorean triple.

(a) Show that a and b cannot both be odd.

Solution: If $a = 2n + 1$ and $b = 2m + 1$ are odd, then $a^2 + b^2 = (2n + 1)^2 + (2m + 1)^2 = 4n^2 + 4n + 1 + 4m^2 + 4m + 1 = 4t + 2$ for some $t \in \mathbf{Z}$. If c is even, then $c = 2k$ for some k and $c^2 = 4k^2 \neq 4t + 2$. If c is odd, then $c = 2s + 1$ for some s and $c^2 = 4s^2 + 4s + 1 \neq 4t + 2$. Thus one of a or b must be even.

(b) Assume that a is even. Show that there exist relatively prime integers m and n such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Solution: Since a is even we can write $a = 2u$ for some $u \in \mathbf{Z}$. Note that $a^2 = c^2 - b^2 = (c - b)(c + b)$. Since b and c must both be odd, $2|(c - b)$ and $2|(c + b)$, and it also follows from Exercise 18 that $\gcd\left(\frac{c-b}{2}, \frac{c+b}{2}\right) = 1$. Both $\frac{c-b}{2}$ and $\frac{c+b}{2}$ are squares (see Exercise 22), say $\frac{c+b}{2} = m^2$ and $\frac{c-b}{2} = n^2$. Since $u^2 = \left(\frac{c-b}{2}\right)\left(\frac{c+b}{2}\right)$, we have $u = mn$. Therefore $a = 2mn$, $b = \frac{c+b}{2} - \frac{c-b}{2} = m^2 - n^2$, and $c = \frac{c+b}{2} + \frac{c-b}{2} = m^2 + n^2$. Since the greatest common divisor of a, b, and c is 1, the same is true for m and n.

1.3. Congruences

26. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

Solution: Since the question deals with the units digit of n^4, it is asking us to find $n^4 \pmod{10}$. All we need to do is to compute the fourth power of each congruence class modulo 10: $0^4 = 0$, $(\pm 1)^4 = 1$, $(\pm 2)^4 = 16 \equiv 6 \pmod{10}$, $(\pm 3)^4 = 81 \equiv 1 \pmod{10}$, $(\pm 4)^4 \equiv 6^2 \equiv 6 \pmod{10}$, and $5^4 \equiv 5^2 \equiv 5 \pmod{10}$. This shows that the only possible units digits for n^4 are 0, 1, 5, and 6.

30. **(a)** Show that if $m \in \mathbf{Z}$, $m \geq 0$, such that $2^m + 1$ is prime, then $m = 0$ or m is a power of 2.

Solution: If $m = 0$, then $2^m + 1 = 1 + 1 = 2$ is prime.

Suppose that $m > 0$ and $m = rs$, where r is the largest odd divisor of m. Then

$$2^m + 1 = 2^{rs} + 1 = (2^s + 1)(2^{s(r-1)} - 2^{s(r-2)} + \ldots - 2^s + 1)\,.$$

Since 2^m+1 is prime and $2^s+1 > 1$, we must have $2^{s(r-1)}-2^{s(r-2)}+\ldots-2^s+1 = 1$, and thus $r = 1$. Therefore $m = 2^n$ for some $n \in \mathbf{Z}$, $n \geq 0$, since r is the largest odd divisor of m.

(b) Show that F_5 is divisible by 641, providing a counterexample to Fermat's belief that all Fermat numbers are prime.

Solution: We have $641 = 640 + 1 = 5 \cdot 2^7 + 1$ and $641 = 625 + 16 = 5^4 + 2^4$, so $5 \cdot 2^7 \equiv -1 \pmod{641}$ and $2^4 \equiv -5^4 \pmod{641}$. Then $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4 2^{28} + 1 \equiv -5^4 2^{28} + 1 \equiv -(5 \cdot 2^7)^4 + 1 \equiv -(-1)^4 + 1 \equiv 0 \pmod{641}$, showing that F_5 is divisible by 641.

(c) Show that $F_n \equiv 7 \pmod{10}$ for $n \geq 2$.

Solution: To give a proof by induction, we first have $F_2 = 2^{2^2} + 1 = 17 \equiv 7 \pmod{10}$. Suppose that $F_n = 2^{2^n} + 1 \equiv 7 \pmod{10}$. Then $F_{n+1} = 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1$. Since $2^{2^n} = F_n - 1 \equiv 6 \pmod{10}$, we have $\left(2^{2^n}\right)^2 \equiv 6^2 \equiv 6 \pmod{10}$, and so $F_{n+1} = \left(2^{2^n}\right)^2 + 1 \equiv 6 + 1 \equiv 7 \pmod{10}$.

(d) Show that $\prod_{0 \leq k < m} F_k = F_m - 2$.

Solution: We have $F_0 = F_1 - 2$ since $3 = 5 - 2$, so the result is true for $m = 1$. Assume that $\prod_{0 \leq k < m} F_k = F_m - 2$. Then $\prod_{0 \leq k < m+1} F_k = \left(\prod_{0 \leq k < m} F_k\right) F_m = (F_m - 2)\, F_m = \left(2^{2^m} - 1\right)\left(2^{2^m} + 1\right) = 2^{2^{m+1}} - 1 = F_{m+1} - 2$ and the result follows by induction.

(e) Show that $(F_n, F_m) = 1$ if $n \neq m$.

Solution: Without loss of generality, suppose that $n < m$. If $d \mid F_n$ and $d \mid F_m$, then $d \mid \prod_{0 \leq k < m} F_k$ and so $d \mid (F_m - 2)$. But if $d \mid F_m$ and $d \mid (F_m - 2)$, then $d \mid 2$, so $d = 2$ or $d = 1$. Since $F_n = 2^{2^n} + 1$ is odd, we have $d = 1$, and therefore $(F_n, F_m) = 1$.

Alternate proof: Suppose that $n < m$ and p is a common prime divisor of $2^{2^n} + 1$ and $2^{2^m} + 1$. Then $2^{2^n} \equiv -1 \pmod{p}$ and $2^{2^m} \equiv -1 \pmod{p}$. But 2^{2^m} is an even power of 2^{2^n}, since $n < m$, which implies that $2^{2^m} \equiv 1 \pmod{p}$, a contradiction.

(f) Use part (e) to give a new proof that there are infinitely many prime numbers.

Solution: Each F_n is either prime or divisible by a prime. Since $(F_n, F_m) = 1$ for $n \neq m$, each number F_n has a prime divisor that does not divide any other F_n. Since there are infinitely many numbers of the form F_n, there are infinitely many prime numbers.

1.4. Integers Modulo n

14. Show that $\mathbf{Z}_{17}^{\times}$ is cyclic.

Solution: We begin by trying [2]. We have $[2]^2 = [4]$, $[2]^3 = [8]$, and $[2]^4 = [16] = [-1]$. Exercise 10 shows that the multiplicative order of an element has to be a divisor of $\varphi(17) = 16$, so the next possibility to check is 8. Since $[2]^8 = [-1]^2 = [1]$, it follows that [2] has multiplicative order 8.

We next try [3]. We have $[3]^2 = [9]$, $[3]^4 = [81] = [-4]$, and $[3]^8 = [16] = [-1]$. The only divisor of 16 that is left to try is 16 itself, so [3] does in fact have multiplicative order 16, and we are done.

19. Using the formula for $\varphi(n)$, compute $\varphi(27)$, $\varphi(81)$, and $\varphi(p^\alpha)$, where p is a prime number. Give a proof that the formula for $\varphi(n)$ is valid when $n = p^\alpha$, where p is a prime number.

Solution: $\varphi(27) = 27(1 - \frac{1}{3}) = 18 \qquad \varphi(81) = 81(1 - \frac{1}{3}) = 54$
In general, we have $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p}) = p^{\alpha-1}(p - 1)$. We prove this by observing that there are $p^{\alpha-1}$ multiples of p between 1 and p^α, inclusive. Thus there are $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$ numbers that are relatively prime to p in the interval from 1 to p^α.

31. Prove that if m, n are positive integers with $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Solution: By the Chinese remainder theorem the system $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ has a unique solution s modulo mn. Define $f : \mathbf{Z}_m \times \mathbf{Z}_n \to \mathbf{Z}_{mn}$ by $f([a]_m, [b]_n) = [s]_{mn}$. If $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$, then since $s \equiv a \pmod{m}$ and $s \equiv b \pmod{n}$ we have $\gcd(s, m) = 1$ and $\gcd(s, n) = 1$. By Proposition 1.2.3 we have $\gcd(s, mn) = 1$. Conversely, if $\gcd(s, mn) = 1$ then $\gcd(s, m) = 1$ and $\gcd(s, n) = 1$ and since $a \equiv s \pmod{m}$ and $b \equiv s \pmod{n}$ we have $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$. Thus $[a]$ and $[b]$ are units in $\mathbf{Z}_m$ and $\mathbf{Z}_n$ respectively if and only if $[s]$ is a unit in $\mathbf{Z}_{mn}$. Since $\mathbf{Z}_m \times \mathbf{Z}_n$ has $\varphi(m) \cdot \varphi(n)$ units while $\mathbf{Z}_{mn}$ has $\varphi(mn)$ units, we have $\varphi(m)\varphi(n) = \varphi(mn)$.

32. Use Exercise 19 and Exercise 31 to prove Proposition 1.4.8.

Solution: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ be a factorization of n into distinct prime powers. By Exercise 31, $\varphi(n) = \prod_{j=1}^{t} \varphi(p_i^{\alpha_i}) = \prod_{j=1}^{t} p_i^{\alpha_i - 1}(p_i - 1)$. The last equality follows from Exercise 19.

2 FUNCTIONS

2.1. Functions

1. In each of the following parts, determine whether the given function is one-to-one and whether it is onto.

(d) $f : \mathbf{R}^+ \to \mathbf{R}$; $f(x) = \ln x$

Solution: If $\ln x_1 = \ln x_2$ for $x_1, x_2 \in \mathbf{R}^+$, then $x_1 = e^{\ln(x_1)} = e^{\ln(x_2)} = x_2$, showing that f is one-to-one. Given $y \in \mathbf{R}$, we have $y = \ln(e^y)$, and so f is also onto. Note that we have really used the fact that e^x is an inverse function for $\ln x$. (See the solution to Exercise 3 (d).)

Alternate solution: Calculus textbooks often give the following conditions for functions whose domain and codomain are subsets of $\mathbf{R}$. A function is one-to-one if and only if any horizontal line cuts the graph of the function in at most one point. A function is onto if and only if any horizontal line through the codomain (on the y-axis) cuts the graph of the function in at least one point. The graph of $y = \ln x$ meets these criteria, so $\ln x$ is one-to-one and onto.

3. For each one-to-one and onto function in Exercise 1, find the inverse of the function.

(d) $f : \mathbf{R}^+ \to \mathbf{R}$; $f(x) = \ln x$

Solution: Define $g : \mathbf{R} \to \mathbf{R}^+$ by $g(y) = e^y$, for all $y \in \mathbf{R}$. Then $g \circ f(x) = g(f(x)) = e^{\ln x} = x$ for all $x \in \mathbf{R}^+$, and $f \circ g(x) = f(g(x)) = \ln(e^x) = x$ for all $x \in \mathbf{R}$, This shows that g is the inverse function of f.
Note: Given that $\ln x$ has an inverse, we could have used Proposition 2.1.7 to solve Exercise 1 (d).

11. Let k and n be positive integers. For a fixed $m \in \mathbf{Z}$, define the formula $f : \mathbf{Z}_n \to \mathbf{Z}_k$ by $f([x]_n) = [mx]_k$, for $x \in \mathbf{Z}$. Show that f defines a function if and only if $k|mn$.

Solution: First suppose that $k|mn$. If $[x_1]_n = [x_2]_n$ then $x_1 \equiv x_2 \pmod{n}$ and so $n|(x_1 - x_2)$ and thus $mn|(mx_1 - mx_2)$. Since $k|mn$, we then have $k|(mx_1 - mx_2)$, and so $[mx_1]_k = [mx_2]_k$. Hence f is well-defined.

Conversely, suppose that f is well-defined. Then since $[0]_n = [n]_n$ we have $[mn]_k = f([n]_n) = f([0]_n) = [m \cdot 0]_k = [0]_k$. Hence $mn \equiv 0 \pmod{k}$ and $k|mn$.

17. Let $f : A \to B$ be a function. Prove that f is onto if and only if $h \circ f = k \circ f$ implies $h = k$, for every set C and all choices of functions $h : B \to C$ and $k : B \to C$.

Solution: Suppose that f is onto. Let $b \in B$. Then there exists $a \in A$ with $f(a) = b$. If $h \circ f = k \circ f$ then $h(b) = h(f(a)) = (h \circ f)(a) = (k \circ f)(a) = k(f(a)) = k(b)$. Since $h(b) = k(b)$ for all $b \in B$, we have $h = k$.

Suppose that f is not onto. Let $b_0 \in B$ such that $b_0 \notin f(A)$. Let $C = \{1, 2\}$ and define $h : B \to C$ by $h(b) = 1$ for all $b \in B$; define $k : B \to C$ by $k(b) = 1$ for $b \in B$, $b \neq b_0$ and $k(b_0) = 2$. Then $h \neq k$, since $h(b_0) = 1 \neq 2 = k(b_0)$. On the other hand $h \circ f(a) = h(f(a)) = 1$ and $k \circ f(a) = k(f(a)) = 1$ since $f(a) \neq b_0$. Since $h \circ f$ and $k \circ f$ have the same domain and codomain, $h \circ f = k \circ f$.

2.2. Equivalence relations

11. Let W be a subspace of a vector space V over $\mathbf{R}$, (that is, the scalars are assumed to be real numbers). We say that two vectors $\mathbf{u}, \mathbf{v} \in V$ are congruent modulo W if $\mathbf{u} - \mathbf{v} \in W$, written $\mathbf{u} \equiv \mathbf{v} \pmod{W}$.

(d) Let $V = \mathbf{R}^2$, and let $W = \{(x, 0) \mid x \in \mathbf{R}\}$. Describe the equivalence class $[(x, y)]_W$ geometrically. *(This is only the first part of the question.)*

Solution: Since $(x_1, y_1) \equiv (x_2, y_2) \pmod{W}$ if and only if $(x_1, y_1) - (x_2, y_2) \in W$ if and only if $(x_1 - x_2, y_1 - y_2) \in W$ if and only if $y_1 = y_2$, the equivalence class $[(x, y)] = \{(t, y) \mid t \in \mathbf{R}\}$ is the horizontal line through y.

12. Let $T = \{(x, y, z) \in \mathbf{R}^3 \mid (x, y, z) \neq (0, 0, 0)\}$. Define $\sim$ on T by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if there exists a nonzero real number λ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$.

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

Solution: (i) Since $x = 1 \cdot x$, $y = 1 \cdot y$, and $z = 1 \cdot z$ we have $(x, y, z) \sim (x, y, z)$ for any $(x, y, z) \in T$. Hence $\sim$ is reflexive.

(ii) Suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Then there exists $0 \neq \lambda \in \mathbf{R}$ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$. Now $\lambda^{-1} \in \mathbf{R}$ and $\lambda^{-1} \neq 0$. Since $x_2 = \lambda^{-1} x_1$, $y_2 = \lambda^{-1} y_1$, and $z_2 = \lambda^{-1} z_1$, we have $(x_2, y_2, z_2) \sim (x_1, y_1, z_1)$. Hence $\sim$ is symmetric.

(iii) Suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ and $(x_2, y_2, z_2) \sim (x_3, y_3, z_3)$. Then there exist $0 \neq \lambda \in \mathbf{R}$ and $0 \neq \mu \in \mathbf{R}$ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$ and also $x_2 = \mu x_3$, $y_2 = \mu y_3$, and $z_2 = \mu z_3$. Hence $x_1 = (\lambda\mu) x_3$, $y_1 = (\lambda\mu) y_3$, and $z_1 = (\lambda\mu) z_3$, while $0 \neq \lambda\mu \in \mathbf{R}$. Thus $(x_1, y_1, z_1) \sim (x_3, y_3, z_3)$ and $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric, and transitive it follows that $\sim$ is an equivalence relation on T.

(b) Give a geometric description of the equivalence class of (x, y, z).

Solution: The class $[x, y, z] = \{(\lambda x, \lambda y, \lambda z) \mid \lambda \in \mathbf{R} \text{ and } \lambda \neq 0\}$ is a line through $(0, 0, 0)$ and (x, y, z) with the point $(0, 0, 0)$ deleted.

(c) Let $(a, b, c) \in T$, and suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Show that if $ax_1 + by_1 + cz_1 = 0$, then $ax_2 + by_2 + cz_2 = 0$. Conclude that

$$L = \{[x, y, z] \in \mathbf{P}^2 \mid ax + by + cz = 0\}$$

is a well-defined subset of $\mathbf{P}^2$.

Solution: Suppose that $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Then there exists $0 \neq \lambda \in \mathbf{R}$ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$. Now $0 = ax_1 + by_1 + cz_1 = \lambda(ax_2 + by_2 + cz_2)$. Since $\lambda \neq 0$, we have $ax_2 + by_2 + cz_2 = 0$. Hence $L = \{[x, y, z] \mid ax + by + cz = 0\}$ is well-defined.

(d) Show that the triples $(a_1, b_1, c_1) \in T$ and $(a_2, b_2, c_2) \in T$ determine the same line if and only if $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$.

Solution: Let L_i be the line determined by (a_i, b_i, c_i). Thus $L_i = \{[x, y, z] \mid a_i x + b_i y + c_i z = 0\}$ for $i = 1, 2$. Suppose that $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$. Then there exists $0 \neq \lambda \in \mathbf{R}$ such that $a_1 = \lambda a_2$, $b_1 = \lambda b_2$, and $c_1 = \lambda c_2$. Thus, if $(x, y, z) \in T$ and $a_1 x + b_1 y + c_1 z = 0$, then $(\lambda a_1)x + (\lambda b_1)y + (\lambda c_1)z = 0$ and so $a_2 x + b_2 y + c_2 z = 0$. Hence $L_1 \subseteq L_2$. Since $a_2 = \lambda^{-1} a_1$, $b_2 = \lambda^{-1} b_1$, and $c_2 = \lambda^{-1} c_1$, we also have $L_2 \subseteq L_1$. Hence if $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$, then we have $L_1 = L_2$.

Conversely, suppose that $L_1 = L_2$. Hence for $(x, y, z) \in T$ we have (1) $a_1 x + b_1 y + c_1 z = 0$ if and only if (2) $a_2 x + b_2 y + c_2 z = 0$. One of a_2, b_2, c_2 is nonzero; without loss of generality suppose that $a_2 \neq 0$. Then $a_1 \neq 0$, for otherwise $x = 1$, $y = 0$, $z = 0$ satisfies (1) but not (2). Let $\lambda = \frac{a_1}{a_2}$. Then $0 \neq \lambda \in \mathbf{R}$. Since $x = c_1$, $y = 0$, $z = -a_1$ satisfies (1), it also satisfies (2) and so $a_2 c_1 = c_2 a_1$, and since $x = b_1$, $y = -a_1$, $z = 0$ satisfies (1), it also satisfies (2) and so $a_2 b_1 = b_2 a_1$. Thus $c_1 = \frac{a_1}{a_2} c_2 = \lambda c_2$ and $b_1 = \frac{a_1}{a_2} b_2 = \lambda b_2$. Hence $a_1 = \lambda a_2$, $b_1 = \lambda b_2$, and $c_1 = \lambda c_2$, and so $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$.

(e) Given two distinct points of $\mathbf{P}^2$, show that there exists exactly one line that contains both points.

Solution: Let $[x_1, y_1, z_1] \neq [x_2, y_2, z_2]$, and treat a, b, c as unknowns. Then the system $\begin{cases} ax_1 + by_1 + cz_1 = 0 \\ ax_2 + by_2 + cz_2 = 0 \end{cases}$ has a nontrivial solution (a, b, c) since it consists of 2 homogeneous equations in 3 unknowns. Hence there exists at least one line L determined by (a, b, c) which both points satisfy. To show that the line is unique we use the "Rank-Nullity" theorem of linear algebra. Suppose that both points $[x_1, y_1, z_1]$ and $[x_2, y_2, z_2]$ satisfy the lines $L_1 = \{[x, y, z] \mid a_1 x + b_1 y + c_1 z = 0\}$ and $L_2 = \{[x, y, z] \mid a_2 x + b_2 y + c_2 z = 0\}$. Define $T_i : \mathbf{R}^3 \to \mathbf{R}$ by $T_i(x, y, z) = a_i x + b_i y + c_i z$ for $i = 1, 2$. Clearly T_i is a linear transformation and since at least one of a_i, b_i, c_i is nonzero the rank of T_i is 1 and the nullity

of T_i is 2. Since both (x_1, y_1, z_1) and (x_2, y_2, z_2) belong to the nullspace of T_i and since they are linearly independent, they form a basis for the nullspace of both T_1 and T_2. Consider any vector (x_0, y_0, z_0) which is not in the nullspace of T_1 (or T_2). Then $T_1(x_0, y_0, z_0) = \lambda T_2(x_0, y_0, z_0)$ for some $0 \neq \lambda \in \mathbf{R}$. Consider $T_1 - \lambda T_2$. The nullspace of $T_1 - \lambda T_2$ is spanned by the three linearly independent vectors (x_0, y_0, z_0), (x_1, y_1, z_1), and (x_2, y_2, z_2). Thus the nullspace of $T_1 - \lambda T_2$ is all of $\mathbf{R}^3$ and so $T_1 = \lambda T_2$. Applying T_1 and T_2 to $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ we see that $a_1 = \lambda a_2$, $b_1 = \lambda b_2$, and $c_1 = \lambda c_2$. Thus $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$ and by part (d) they determine the same line.

(f) Given two distinct lines, show that there exists exactly one point that belongs to both lines.

Solution: This is a similar argument to the one in (e).

(g) Show that the function $f : \mathbf{R}^2 \to \mathbf{P}^2$ defined by $f(x, y) = [x, y, 1]$ is a one-to-one function.

Solution: Suppose that $f(x_1, y_1) = f(x_2, y_2)$. Then $[x_1, y_1, 1] = [x_2, y_2, 1]$. Thus $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $1 = \lambda \cdot 1$. Hence $\lambda = 1$ and $(x_1, y_1) = (x_2, y_2)$. Therefore f is one-to-one as required.

(h) Show that the embedding of part (g) takes lines to "lines."

Solution: A line in the affine plane has the form $ax + by + c = 0$ where not both a and b are zero. Thus (x, y) belongs to $ax + by + c = 0$ if and only if $[x, y, 1]$ belongs to $L = \{[x, y, z] \mid ax + by + cz = 0\}$.

(i) If two lines intersect in $\mathbf{R}^2$, show that the image of their intersection is the intersection of their images (under the embedding defined in part (g)).

Solution: Suppose that $a_1x + b_1y + c_1 = 0$ intersects $a_2x + b_2y + c_2 = 0$ at the point (x_0, y_0). If $L_i = \{[x, y, z] \mid a_ix + b_iy + c_iz = 0\}$ for $i = 1, 2$, then we have that $[x_0, y_0, 1]$ belongs to the intersection of L_1 and L_2.

(j) If two lines are parallel in $\mathbf{R}^2$, what happens to their images under the embedding into $\mathbf{P}^2$?

Solution: If $a_1x + b_1y + c_1 = 0$ is parallel to $a_2x + b_2y + c_2 = 0$, then either (1) $b_1 = b_2 = 0$ or (2) $\frac{a_1}{b_1} = \frac{a_2}{b_2}$. Suppose that $b_1 = b_2 = 0$. Then the point $[0, 1, 0]$ belongs to both L_1 and L_2 where as before $L_i = \{[x, y, z] \mid a_ix + b_iy + c_iz = 0\}$ for $i = 1, 2$. On the other hand, if $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, then $[-b_1, a_1, 0] = [-b_2, a_2, 0]$ belongs to L_1 and L_2.

From (i) and (j) we see that in $\mathbf{P}^2$ <u>all</u> lines intersect.

2.3. Permutations

15. Let $\tau \in S_n$ be the cycle $(1, 2, \ldots, k)$ of length k, where $k \leq n$.

(a) Prove that if $\sigma \in S_n$, then $\sigma\tau\sigma^{-1} = (\sigma(1), \sigma(2), \ldots, \sigma(k))$. Thus $\sigma\tau\sigma^{-1}$ is a cycle of length k.

Solution: Assume that $\sigma \in S_n$, where $k \leq n$. If $j \in \{\sigma(1), \sigma(2), \ldots, \sigma(k-1)\}$ then say $j = \sigma(i)$. Now $\sigma\tau\sigma^{-1}(j) = \sigma\tau\sigma^{-1}(\sigma(i)) = \sigma\tau(i) = \sigma(i+1)$. If $j = \sigma(k)$, then $\sigma\tau\sigma^{-1}(j) = \sigma\tau\sigma^{-1}(\sigma(k)) = \sigma\tau(k) = \sigma(1)$. If $j \notin \{\sigma(1), \sigma(2), \ldots, \sigma(k)\}$, then $\sigma^{-1}(j) \notin \{1, 2, \ldots, k\}$ and so $\sigma\tau\sigma^{-1}(j) = \sigma(\sigma^{-1}(j)) = j$. Hence $\sigma\tau\sigma^{-1} = (\sigma(1), \sigma(2), \ldots, \sigma(k))$.

(b) Let ρ be any cycle of length k. Prove that there exists a permutation $\sigma \in S_n$ such that $\sigma\tau\sigma^{-1} = \rho$.

Solution: Assume that $\tau, \rho \in S_n$, where $k \leq n$, and let $\rho = (a_1, a_2, \ldots, a_k)$. For the numbers i, with $i \leq n$, that do *not* appear in ρ, we can choose an ordering $a_{k+1}, \ldots, a_n$. Then we can define $\sigma = \begin{pmatrix} 1 & 2 & \ldots & k & k+1 & \ldots & n \\ a_1 & a_2 & \ldots & a_k & a_{k+1} & \ldots & a_n \end{pmatrix}$ and $\sigma\tau\sigma^{-1} = (\sigma(1), \ldots, \sigma(k)) = (a_1, a_2, \ldots, a_k) = \rho$.

18. View S_3 as a subset of S_5, in the obvious way. For $\sigma, \tau \in S_5$, define $\sigma \sim \tau$ if $\sigma\tau^{-1} \in S_3$.

(d) Determine the total number of equivalence classes.

Solution: The equivalence class of μ is $\{\sigma \in S_5 \mid \sigma \sim \mu\}$, which is equal to $\{\sigma \in S_5 \mid \sigma\mu^{-1} = \tau \text{ for some } \tau \in S_3\} = \{\sigma \in S_5 \mid \sigma = \tau\mu \text{ for some } \tau \in S_3\}$. Thus we can find the equivalence class of $\mu \in S_5$ by finding all products of the form $\tau\mu$, for $\tau \in S_3$. If $\tau_1\mu = \tau_2\mu$ for some τ_1, τ_2, then multiplying on the right by μ^{-1} shows that $\tau_1 = \tau_2$. Thus the 6 permutations in S_3 will yield 6 distinct products of the form $\tau\mu$ in the equivalence class of μ. It follows that every equivalence class has 6 members. Since S_5 has 120 elements, the total number of equivalence classes is $\frac{120}{6} = 20$.

3 GROUPS

3.1. Definition of a Group

4. Prove that multiplication of 2×2 matrices satisfies the associative law.

Solution: Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, and $C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$. Then

$$\begin{aligned} A(BC) &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right) \\ &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11}c_{11} + b_{12}c_{21} & b_{11}c_{12} + b_{12}c_{22} \\ b_{21}c_{11} + b_{22}c_{21} & b_{21}c_{12} + b_{22}c_{22} \end{bmatrix} = \end{aligned}$$

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

$$\begin{aligned} &= \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + b_{22}b_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \\ &= \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \right) \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \\ &= (AB)C \ . \end{aligned}$$

11. Show that the set of all 2×2 matrices over $\mathbf{R}$ of the form $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$ with $m \neq 0$ forms a group under matrix multiplication.

Solution: (i) The product $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} n & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} mn & mc + b \\ 0 & 1 \end{bmatrix}$ of two elements of the given form has the proper form since $mn \neq 0$. Thus matrix multiplication is a binary operation on the given set.

(ii) Matrix multiplication is associative by Exercise 4.

(iii) The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ has the proper form and it is the identity element under matrix multiplication.

(iv) Given $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$, consider $\begin{bmatrix} 1/m & -b/m \\ 0 & 1 \end{bmatrix}$. This matrix has the proper form and is the required inverse since $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/m & -b/m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1/m & -b/m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

13. Define $*$ on $\mathbf{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbf{R}$. Show that $(\mathbf{R}, *)$ is an abelian group.

Solution: Since $a * b = b * a$ for all $a, b \in \mathbf{R}$, the operation is commutative, and this eliminates some calculations.

(i) The operation $* : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ is the composite of ordinary addition followed by the function $f(x) = x - 1$, so it is a well-defined function.

(ii) The operation is associative since
$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$ and
$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$.

(iii) Since $1 * b = 1 + b - 1 = b$ for all $b \in \mathbf{R}$, it follows that 1 is an identity. (We also have $b * 1 = b$ since the operation is commutative.)

(iv) The inverse of a is $2 - a$, since $a * (2 - a) = a + (2 - a) - 1 = 1$. (Again, since the operation is commutative we do not need to check that $(2 - 1) * a = 1$.)

19. Let G be a group. For $a, b \in G$, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbf{Z}$ if and only if $ab = ba$.

Solution: If $(ab)^n = a^n b^n$ for all $n \in \mathbf{Z}$, then in particular $(ab)^2 = a^2 b^2$, so $ab = ba$ by Example 3.1.2.

Conversely, suppose that $a, b \in G$ with $ab = ba$.

We will first show by induction that $ba^n = a^n b$ for all positive integers n. The result holds for $n = 1$ by hypothesis. Now suppose that $ba^k = a^k b$. Then $ba^{k+1} = ba^k a = a^k ba = a^k ab = a^{k+1} b$, so the general result holds.

We next show that $(ab)^n = a^n b^n$ for all positive n. The result holds for $n = 1$ by hypothesis. Now suppose that $(ab)^k = a^k b^k$. Then $(ab)^{k+1} = ab(ab)^k = aba^k b^k = aa^k bb^k = a^{k+1} b^{k+1}$.

We also have $(ab)^0 = e = a^0 b^0$.

Since $ab = ba$, we have $(ab)^{-1} = (ba)^{-1}$, and thus $b^{-1}a^{-1} = a^{-1}b^{-1}$. Finally, if $n < 0$ then say $n = -m$, where $m > 0$. Hence $(ab)^n = (ab)^{-m} = ((ab)^{-1})^m = (b^{-1}a^{-1})^m = (a^{-1}b^{-1})^m = (a^{-1})^m (b^{-1})^m = a^n b^n$ as required.

20. Let G be a group. Prove that $a^m a^n = a^{m+n}$ for all $a \in G$ and all $m, n \in \mathbf{Z}$.

Solution: We let $n \in \mathbf{Z}$ and prove that $a^m a^n = a^{m+n}$ for all a and all positive integers m by induction. If $m = 1$, then $a^1 a^n = a \cdot a^n = a^{n+1}$. If $a^m a^n = a^{m+n}$, then $a^{m+1} a^n = (aa^m)a^n = a(a^m a^n) = a(a^{m+n}) = a^{m+n+1} = a^{(m+1)+n}$.

For $m = 0$ we have $a^0 a^n = e \cdot a^n = a^n = a^{0+n}$.

If $m < 0$, say $m = -r$, then $a^m a^n = a^{-r} a^n = (a^{-1})^r (a^{-1})^{-n} = (a^{-1})^{r+(-n)} = (a^{-1})^{-m+(-n)} = ((a^{-1})^{-1})^{m+n} = a^{m+n}$ as required.

21. Let G be a group. Prove that $(a^m)^n = a^{mn}$ for all $a \in G$ and all $m, n \in \mathbf{Z}$.

Solution: We let $n \in \mathbf{Z}$ and prove that $(a^m)^n = a^{mn}$ for all a and all positive integers m by induction. If $m = 1$, then $(a^1)^n = a^n = a^{1 \cdot n}$. If $(a^m)^n = a^{mn}$,

then $(a^{m+1})^n = (a^m \cdot a)^n = (a^m)^n a^n$ (by the proof in Exercise 19, since a^m and a commute) and so $(a^{m+1})^n = a^{mn} \cdot a^n = a^{mn+n} = a^{(m+1)n}$.

For $m = 0$ we have $(a^m)^n = (a^0)^n = e^n = e = a^0 = a^{0 \cdot n}$.

If $m < 0$, then $m = -r$ for some $r > 0$ and so $(a^m)^n = (a^{-r})^n = ((a^{-1})^r)^n = (a^{-1})^{rn} = a^{-rn} = a^{mn}$, as required.

26. Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.

Solution: If G is any group and $x \in G$ with $x^2 \neq e$, then $x \neq x^{-1}$ and $(x^{-1})^2 = (x^2)^{-1} \neq e$. Thus G has an even number of elements x with $x^2 \neq e$. If G has an even number of elements, this leaves an even number of elements x with $x^2 = e$. There is at least one such element, the identity e. Thus there must be at least one more element a, with $a \neq e$ and $a^2 = e$.

3.2. Subgroups

9. Let $G = \mathrm{GL}_3(\mathbf{R})$. Show that $H = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$ is a subgroup of G.

Solution: We will use Proposition 3.2.2. If $\begin{bmatrix} 1 & 0 & 0 \\ a_1 & 1 & 0 \\ b_1 & c_1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ a_2 & 1 & 0 \\ b_2 & c_2 & 1 \end{bmatrix} \in H$, then $\begin{bmatrix} 1 & 0 & 0 \\ a_1 & 1 & 0 \\ b_1 & c_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ a_2 & 1 & 0 \\ b_2 & c_2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a_1 + a_2 & 1 & 0 \\ b_1 + c_1 a_2 + b_2 & c_1 + c_2 & 1 \end{bmatrix}$ is in H. The identity matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ belongs to H. If $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}$ is in H, then $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ -b + ca & -c & 1 \end{bmatrix}$ is in H. Therefore H is a subgroup of G.

Note: The group H is known as the **continuous Heisenberg group**.

17. Prove that the intersection of any collection of subgroups of a group is again a subgroup.

Solution: We will use Corollary 3.2.3. The identity of the group belongs to each subgroup, so it belongs to their intersection. If elements a, b belong to the intersection, then they belong to each subgroup in the collection, and so ab^{-1} belongs to

each subgroup. This shows that ab^{-1} belongs to the intersection of all subgroups in the collection.

19. Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G \mid xa = ax\}$ of all elements of G that commute with a is called the centralizer of a.

(a) Show that $C(a)$ is a subgroup of G.

Solution: We will use Proposition 3.2.2. (i) Let $x, y \in C(a)$. Then $xa = ax$ and $ya = ay$. Hence $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$ and so $xy \in C(a)$. (ii) Since $ea = a = ae$, we have $e \in C(a)$. (iii) If $x \in C(a)$, then $xa = ax$ and so $x^{-1}a = (x^{-1}a)(xx^{-1}) = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = (x^{-1}x)ax^{-1} = ax^{-1}$ and $x^{-1} \in C(a)$. Therefore $C(a)$ is a subgroup of G.

21. Let G be a group. The set $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ of all elements that commute with every other element of G is called the center of G.

(a) Show that $Z(G)$ is a subgroup of G.

Solution: (i) Let $x, y \in Z(G)$ and $g \in G$. Then $xg = gx$ and $yg = gy$. Hence $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$ for all $g \in G$ and so $xy \in Z(G)$. (ii) Since $eg = ge$ for all $g \in G$, we have $e \in Z(G)$. (iii) Let $x \in Z(G)$ and $g \in G$. Then $xg = gx$ and so $x^{-1}g = x^{-1}gxx^{-1} = x^{-1}xgx^{-1} = gx^{-1}$ for all $g \in G$. Thus $x^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup of G by Proposition 3.2.2.

3.3. Constructing Examples

4. Show that the list of elements of $\mathrm{GL}_2(\mathbf{Z}_2)$ given in Example 3.3.6 is correct.

Solution: To construct an invertible 2×2 matrix A over $\mathbf{Z}_2$, we can use any nonzero vector as the first row. Thus the first row can be $(1, 0)$, $(0, 1)$, or $(1, 1)$. Then the second row must be linearly independent of the first, so it cannot be a multiple of the first row. If $(1, 0)$ is the first row, we can use $(0, 1)$ or $(1, 1)$ as the second. If $(0, 1)$ is the first row, we can use $(1, 0)$ or $(1, 1)$ as the second. If $(1, 1)$ is the first row, we can use $(1, 0)$ or $(0, 1)$ as the second. This gives us the 6 invertible matrices in Example 3.3.6:

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

7. Let F be a field. Compute the center of $\mathrm{GL}_2(F)$.

Solution: As usual, we let 1 denote the multiplicative identity of F. We first note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ are invertible, and so they belong to $\mathrm{GL}_2(F)$. Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(\mathrm{GL}_2(F))$. Then $\begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} =$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix}$ and so $a = a + c$ and $a + b = b + d$. Thus $c = 0$ and $a = d$. Furthermore, $\begin{bmatrix} a+b & b \\ a & a \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} = \begin{bmatrix} a & b \\ a & a+b \end{bmatrix}$ implies $a + b = a$ and so $b = 0$. Thus $X = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and so $Z(\mathrm{GL}_2(F)) \subseteq \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| 0 \neq a \in F \right\}$. Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ is clearly in the center, we have $Z(\mathrm{GL}_2(F)) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| a \in F^\times \right\}$.

Comment: This proof actually computes the center as the intersection of the centralizers of just two elements, the particular matrices used in the proof.

15. **(a)** Generalize Definition 3.3.3 to the case of the direct product of n groups.

Definition: Let $G_1, G_2, \ldots, G_n$ be groups. We define

$$G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in G_i \text{ for } i = 1, 2, \ldots, n\}.$$

(b) Generalize Proposition 3.3.4 to the case of the direct product of n groups. Prove that your generalization is true.

Proposition. Let $G_1, G_2, \ldots, G_n$ be groups.

(i) The direct product $G_1 \times G_2 \times \cdots \times G_n$ is a group under the multiplication

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots a_nb_n) .$$

(ii) If $a_i \in G_i$ has order m_i for $i = 1, 2, \ldots, n$, then in $G_1 \times G_2 \times \cdots \times G_n$ the element $(a_1, a_2, \ldots a_n)$ has order $\mathrm{lcm}[m_1, m_2, \ldots, m_n]$.

Proof: (i) The given multiplication defines a binary operation. The associative law holds since for $1 \leq i \leq n$ and all $a_i, b_i, c_i \in G_i$ we have

$$\begin{aligned}
&(a_1, a_2, \ldots, a_n)((b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)) \\
&\qquad = (a_1, a_2, \ldots, a_n)(b_1c_1, b_2c_2, \ldots b_nc_n) \\
&\qquad = (a_1(b_1c_1), a_2(b_2c_2), \ldots, a_n(b_nc_n)) \\
&\qquad = ((a_1b_1)c_1, (a_2b_2)c_2, \ldots, (a_nb_n)c_n) \\
&\qquad = (a_1b_1, a_2b_2, \ldots, a_nb_n)(c_1, c_2, \ldots, c_n) \\
&\qquad = ((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n))(c_1, c_2, \ldots, c_n).
\end{aligned}$$

If e_i is the identity element of G_i for $i = 1, 2, \ldots, n$, then $(e_1, e_2, \ldots, e_n)$ is easily seen to be the identity element of $G_1 \times G_2 \times \cdots \times G_n$. Finally, for any element $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$, we have $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.

(ii) Let $o(a_i) = m_i$ for $i = 1, 2, \ldots, n$. The order of $(a_1, a_2, \ldots, a_n)$ is the least positive integer m such that $(a_1, a_2, \ldots, a_n)^m = (e_1, e_2, \ldots, e_n)$. Thus for each i, we have $a_i^m = e_i$ and so $m_i \,|\, m$. The least such m such that $m_i \,|\, m$ for $i = 1, 2, \ldots, n$ is lcm$[m_1, m_2, \ldots, m_n]$.

19. Let G be a group of order 6. Show that G must contain an element of order 2. Show that it cannot be true that every element different from e has order 2.

Solution: Since $|G|$ is even, by Exercise 3.1.26 there is at least one element of order 2. Suppose that $|G| = 6$ and every element of G has order 2. Let $a, b \in G$, $a \neq b, a \neq e, b \neq e$. Then $a^2 = b^2 = e$, so $ab = e$ implies $b \neq a$. Thus $ab \neq e$, so $o(ab) = 2$ and then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Hence $H = \{e, a, b, ab\}$ is a subgroup of G of order 4, contradicting Lagrange's theorem.

20. Let G be a group of order 6, and suppose that $a, b \in G$ with a of order 3 and b of order 2. Show that either G is cyclic or $ab \neq ba$.

Solution: Let $a, b \in G$, with $o(a) = 3$ and $o(b) = 2$. We claim that G is cyclic iff $ab = ba$. If $ab = ba$, then $o(ab) = \text{lcm}[2, 3] = 6$ and $G = \langle ab \rangle$ is cyclic. If $ab \neq ba$, then G is not abelian and hence not cyclic.

21. Let G be any group of order 6. Show that if G is not cyclic, then its multiplication table must look like that of S_3.

Solution: By Exercises 19 and 20, if G is not cyclic then there exist an element a of order 3 and an element b of order 2 such that $ab \neq ba$. Now the elements e, a, a^2, b are all distinct. By cancellation $ab \neq a$, $ab \neq a^2$, and $ab \neq b$, and since $a^{-1} = a^2 \neq b$ we have $ab \neq e$. Thus e, a, a^2, b, ab are all distinct. Again by cancellation $a^2b \neq a$, $a^2b \neq a^2$, $a^2b \neq ab$, and $a^2b \neq b$. We also have $a^2 \neq b$, so $a^2b \neq e$. Thus $G = \{e, a, a^2, b, ab, a^2b\}$.

What is ba? By cancellation $ba \neq a$, $ba \neq a^2$, and $ba \neq b$. Since $b \neq a^2$, we have $ba \neq e$. By assumption $ba \neq ab$. By elimination $ba = a^2b$. We can now complete the multiplication table for G.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^b	a^2b	ab	b	a^2	a	e

3.4. Isomorphisms

12. For the field F, let $H = \left\{ \left[\begin{array}{cc} 1 & 0 \\ c & d \end{array} \right] \middle| c, d \in F, \ \ d \neq 0 \right\} \subseteq \mathrm{GL}_2(F)$.

(b) Show that $K = \left\{ \left[\begin{array}{cc} m & b \\ 0 & 1 \end{array} \right] \middle| m, b \in F, \ \ m \neq 0 \right\}$ is a subgroup of $\mathrm{GL}_2(F)$ that is isomorphic to H.

Solution: Let $a = \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \in \mathrm{GL}_2(F)$. Then for $\left[\begin{array}{cc} 1 & 0 \\ c & d \end{array} \right] \in H$ we have

$$a \left[\begin{array}{cc} 1 & 0 \\ c & d \end{array} \right] a^{-1} = \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \left[\begin{array}{cc} 1 & 0 \\ c & d \end{array} \right] \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] = \left[\begin{array}{cc} c & d \\ 1 & 0 \end{array} \right] \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] = \left[\begin{array}{cc} d & c \\ 0 & 1 \end{array} \right].$$

This makes it clear that $aHa^{-1} = K$, so K is a subgroup by Example 3.2.13, and then $H \cong aHa^{-1} = K$ by Example 3.4.3.

26. Define $*$ on $\mathbf{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbf{R}$. (See Exercise 13 of Section 3.1.) Show that the group $G = (\mathbf{R}, *)$ is isomorphic to the group $(\mathbf{R}, +)$.

Discussion: Since we need a one-to-one mapping from $\mathbf{R}$ to $\mathbf{R}$, is it possible that one of the simplest cases, a linear function of the form $\phi(x) = mx+b$, might work? Of course, we need $m \neq 0$ to make certain that ϕ is a one-to-one correspondence. Since the solution to Exercise 13 of Section 3.1 shows that 1 is the identity element of G, and since 0 is the identity element of $\mathbf{R}$, we would need to have $\phi(1) = 0$, which forces $b = -m$.

Solution: For any $0 \neq m \in \mathbf{R}$, define $\phi : G \to \mathbf{R}$ by $\phi(x) = mx - m$, for all $x \in G$. It is clear that ϕ is one-to-one and onto since $m \neq 0$. For all $a, b \in G$ we have $\phi(a * b) = \phi(a + b - 1) = m(a + b - 1) - m = ma + mb - 2m$ and $\phi(a)+\phi(b) = (ma-m)+(mb-m1) = ma+mb-2m$, so $\phi(a*b) = \phi(a)+\phi(b)$. Thus ϕ respects the operations in the two groups, and so ϕ does indeed define an isomorphism from $(G, *)$ onto $(\mathbf{R}, +)$.

Note: We have actually shown that there are infinitely many different possible isomorphisms. Of course, the simplest case would be to let $m = 1$ and just use $\theta(x) = x-1$. Then we can write ϕ as a composite function $\psi\theta$, where $\psi(x) = mx$ defines an isomorphism from $(\mathbf{R}, +)$ onto itself.

3.5. Cyclic Groups

13. Show that in a finite cyclic group of order n, the equation $x^m = e$ has exactly m solutions, for each positive integer m that is a divisor of n.

Solution: Let $G = \langle a \rangle$, where $o(a) = n$. If $m \,|\, n$ then $n = mk$ for some $k \in \mathbf{Z}$. We have $o(a^k) = \frac{n}{(k,n)} = \frac{n}{k} = m$, and so $\{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$ consists of m

distinct solutions of $x^m = e$. Suppose that c is a solution to $x^m = e$. Then $c = a^j$ for some j, and $o(c) = \frac{n}{(j,n)}$, where $\frac{n}{(j,n)} \mid m$. Thus there exists a positive integer t such that $nt = m(j,n)$. Then $mkt = m(j,n)$ and so $(j,n) = kt$. Since $(j,n) \mid j$ we have $j = k \cdot t \cdot r$ for some positive integer r. Thus $c = a^j = a^{k \cdot t r}$ and so $c \in \{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$.

17. Let G be a finite group, and suppose that for any two subgroups H and K either $H \subseteq K$ or $K \subseteq H$. Prove that G is cyclic of prime power order.

Solution: Since G is finite, it has an element of maximal order, say a. Then $\langle a \rangle$ cannot be properly contained in any other cyclic subgroup, so it follows that $\langle b \rangle \subseteq \langle a \rangle$ for every $b \in G$. Thus every element of G is a power of a, and so G is cyclic, with $G = \langle a \rangle$. Suppose that $|G|$ has two distinct prime divisors p and q. By hypothesis we have either $\langle a^p \rangle \subseteq \langle a^q \rangle$ or $\langle a^q \rangle \subseteq \langle a^p \rangle$. But then Corollary 3.5.4 (c) implies that either $q \mid p$ or $p \mid q$, a contradiction. We conclude that G is cyclic of prime power order.

21. Prove that if p and q are different odd primes, then $\mathbf{Z}_{pq}^{\times}$ is not a cyclic group.

Solution: We know that $[-1]_{pq}$ has order 2, so by Exercise 13 it is enough to find one other element of order 2. The Chinese remainder theorem (Theorem 1.3.6) states that the system of congruences $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$ has a solution $[a]_{pq}$, since p and q are relatively prime. Because p is an odd prime, $[-1]_{pq}$ is not a solution, so $[a]_{pq} \neq [-1]_{pq}$. But $a^2 \equiv 1 \pmod{p}$ and $a^2 \equiv 1 \pmod{q}$, so $a^2 \equiv 1 \pmod{pq}$ since p and q are relatively prime. Thus $[a]_{pq}$ has order 2.

3.6. Permutation Groups

21. In the dihedral group $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$ with $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$, find the centralizer $C(a) = \{x \in D_n \mid xa = ax\}$.

Solution: The centralizer $C(a)$ contains all powers of a, so we have $\langle a \rangle \subseteq C(a)$. This shows that $C(a)$ has at least n elements. On the other hand, $C(a) \neq D_n$, since by definition b does not belong to $C(a)$. Since $\langle a \rangle$ contains exactly half of the elements in D_n, Lagrange's theorem show that there is no subgroup that lies strictly between $\langle a \rangle$ and D_n, so $\langle a \rangle \subseteq C(a) \subseteq D_n$ and $C(a) \neq D_n$ together imply that $C(a) = \langle a \rangle$.

22. Find the center of the dihedral group D_n.

Solution: Let $n \geq 3$. Then $D_n = \{a^j, a^j b \mid 0 \leq j < n\}$ with $a^n = b^2 = e$ and $ba = a^{n-1}b$. By induction we have $ba^j = a^{n-j}b$. Now if $x = a^j b$ then $xa = a^j ba = a^{j+n-1}b$ and $ax = a^{j+1}b$. Hence $xa = ax$ if and only if

$j+n-1 \equiv j+1 \pmod{n}$, and this happens if and only if $n = 2$. Hence $x = a^j b$ is never central.

Now let $x = a^j$. Since x commutes with all powers of a, it will be central if $xb = bx$. But $bx = ba^j = a^{n-j}b = a^j b$ if and only if $n - j \equiv j \pmod{n}$. This holds for $0 \leq j < n$ only if $j = 0$ or $j = m$ when $n = 2m$. Thus if $n = 2m$, then $Z(D_n) = \{e, a^m\}$ and if n is odd, then $Z(D_n) = \{e\}$.

3.7. Homomorphisms

6. Let n and m be positive integers, such that m is a divisor of n. Show that $\phi : \mathbf{Z}_n^\times \to \mathbf{Z}_m^\times$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$, is a well-defined group homomorphism.

Solution: First, ϕ is a well-defined function by Exercise 11 of Section 2.1. Next, ϕ is a homomorphism since for $[a]_n, [b]_n \in \mathbf{Z}_n^\times$, we have $\phi([a]_n[b]_n) = \phi([ab]_n) = [ab]_m = [a]_m[b]_m = \phi([a]_n)\phi([b]_n)$.

8. Define $\phi : \mathbf{R} \to \mathbf{C}^\times$ by setting $\phi(\theta) = e^{i\theta}$, for all $\theta \in \mathbf{R}$. Use this version of the formula in Example 3.7.11 to show that ϕ is a group homomorphism.

Solution: We need to be careful, since the operation in the first group is addition, and in the second it is multiplication. If $\theta_1, \theta_2 \in \mathbf{R}$, then $\phi(\theta_1 + \theta_2) = e^{i(\theta_1+\theta_2)} = e^{i\theta_1+i\theta_2} = e^{i\theta_1}e^{i\theta_2} = \phi(\theta_1)\phi(\theta_2)$, and so ϕ preserves the respective operations.

14. Prove that $\mathrm{SL}_n(\mathbf{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$.

Solution: First, $\mathrm{SL}_n(\mathbf{R})$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ since it contains the identity matrix, and if $A, B \in \mathrm{SL}_n(\mathbf{R})$, then $\det(A) = \det(B) = 1$, so $\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1$, and thus $AB^{-1} \in \mathrm{SL}_n(\mathbf{R})$.

If $A \in \mathrm{SL}_n(\mathbf{R})$ and $P \in \mathrm{GL}_n(\mathbf{R})$, then $\det(PAP^{-1}) = \det(P)\det(A)\det(P^{-1})$ $= \det(P) \cdot 1 \cdot \dfrac{1}{\det(P)} = 1$, so $PAP^{-1} \in \mathrm{SL}_n(\mathbf{R})$, showing that $\mathrm{SL}_n(\mathbf{R})$ is normal in $\mathrm{GL}_n(\mathbf{R})$

Alternate solution: Here is a slightly more sophisticated proof. Example 3.7.1 shows that the determinant defines a group homomorphism. After observing that $\mathrm{SL}_n(\mathbf{R})$ is the kernel of the determinant homomorphism from $\mathrm{GL}_n(R)$ into $\mathbf{R}$, the result follows from Proposition 3.7.4 (a) (which shows that the kernel of any group homomorphism is a normal subgroup).

24. Let $G_1, \ldots, G_n$ be groups, for $n \in \mathbf{Z}^+$, and let $G = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$ be the group of n-tuples with entries in G_i.

(a) Define $\theta_i : G_i \to G$ by $\theta_i(g_i) = (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)$, where $g_i \in G_i$ and e_j is the identity element of G_j. Show that θ_i is a group homomorphism

and $H_i = \theta_i(G_i) = \{(e_1, \ldots, g_i, \ldots, e_n) \mid g_i \in G_i\}$ is a subgroup of G with $H_i \cong G_i$.

Solution: Since $\theta_i(a_i b_i) = (e_1, \ldots, a_i b_i, \ldots, e_n) =$
$(e_1, \ldots, a_i, \ldots, e_n)(e_1, \ldots, b_i, \ldots, e_n) = \theta_i(a_i)\theta_i(b_i)$ for $a_i, b_i \in G_i$, it follows that θ_i is a group homomorphism, and then $H_i = \theta_i(G_i)$ is a subgroup of G by Proposition 3.7.6. It is clear that θ_i is one-to-one and maps G_i onto H_i.

(b) Show that $G = H_1 H_2 \cdots H_n$, that elements of H_i and H_j commute, for all $1 \leq i < j \leq n$, and that $H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$, for all $1 \leq i \leq n$.

Solution: We have $(g_1, .., g_i, .., g_n) =$
$(g_1, .., e_i, .., e_n) \cdots (e_1, .., g_i, .., e_n) \cdots (e_1, .., e_i, .., g_n)$ and
$(e_1, .., g_i, .., e_j, .., e_n)(e_1, .., e_i, .., g_j, .., e_n) = (e_1, .., g_i, .., g_j, .., e_n) =$
$(e_1, .., e_i, .., g_j, .., e_n)(e_1, .., g_i, .., e_j, .., e_n)$ for all $g_i \in G_i$ and $g_j \in G_j$. In each element of the product $H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$, the ith entry is e_i, and so the intersection with H_i is $(e_1, .., e_i, .., e_n)$.

(c) For all $(g_1, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_n) \in G$, define $\pi_i : G \to G_i$ by setting $\pi_i((g_1, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_n)) = g_i$. Show that π_i is a group homomorphism with kernel $H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$.

Solution: We have $\pi_i((a_1, .., a_i, .., a_n)(b_1, .., b_i, .., b_n)) =$
$\pi_i((a_1 b_1, .., a_i b_i, .., a_n b_n)) = a_i b_i = \pi_i((a_1, .., a_i, .., a_n))\, \pi_i((b_1, .., b_i, .., b_n))$, for all $a_j, b_j \in G_j$, and so π_i is a group homomorphism. We have
$\pi_i((g_1, .., g_i, .., g_n)) = e_i$ if and only if $g_i = e_i$, and so it is clear that $\ker(\pi_i)$ is the product of the other subgroups H_j, with H_i omitted.

(d) Show that $\pi_i \circ \theta_i = 1_{G_i}$, for $1 \leq i \leq n$.

Solution: We have $(\pi_i \circ \theta_i)(g_i) = \pi_i(\theta_i(g_i)) =$
$\pi_i((e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)) = g_i$, for $g_i \in G_i$.

(e) Define $\psi : G \to G$ by $\psi(g) = (\theta_1\pi_1(g))(\theta_2\pi_2(g)) \cdots (\theta_n\pi_n(g))$, for all $g \in G$. Show that $\psi = 1_G$, and that if $\sigma \in S_n$, then for all $g \in G$ we have $\psi(g) = (\theta_{\sigma(1)}\pi_{\sigma(1)}(g))(\theta_{\sigma(2)}\pi_{\sigma(2)}(g)) \cdots (\theta_{\sigma(n)}\pi_{\sigma(n)}(g))$,

Solution: We have $\theta_i\pi_i(g) = \theta_i(g_i) = (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)$, for any element $g = (g_1, g_2, \ldots, g_n) \in G$. The product of the elements $\theta_i\pi_i(g)$, over all $1 \leq i \leq n$, yields g, and so $\psi(g) = g$. Since the elements $\theta_i\pi_i(g)$ and $\theta_j\pi_j(g)$ commute, the product over all i can be taken in any order.

(f) Let G' be a group. Show that given group homomorphisms $\phi_i : G' \to G_i$, for $1 \leq i \leq n$, there exists a unique group homomorphism $\phi : G' \to G$ such that $\pi_i\phi = \phi_i$, for $1 \leq i \leq n$.

Solution: Suppose that group homomorphisms $\phi_i : G' \to G_i$ are given, for $1 \leq i \leq n$. For $x \in G'$, restating the condition $\pi_i\phi = \phi_i$ shows that the ith component of $\phi(x)$ must be $\phi_i(x)$, so the only way to define $\phi : G' \to G$ is by setting

$\phi(x) = (\phi_1(x), \phi_2(x), \ldots, \phi_n(x))$. But does this define a group homomorphism? Yes, since for $a, b \in G'$ we have

$$\begin{aligned} \phi(ab) &= (\phi_1(ab), \ldots, \phi_i(ab), \ldots, \phi_n(ab)) \\ &= (\phi_1(a)\phi_1(b), \ldots, \phi_i(a)\phi_i(b), \ldots, \phi_n(a)\phi_n(b)) \\ &= (\phi_1(a), \ldots, \phi_i(a), \ldots, \phi_n(a))\ (\phi_1(b), \ldots, \phi_i(b), \ldots, \phi_n(b)) \\ &= \phi(a)\phi(b)\,. \end{aligned}$$

3.8. Cosets, Normal Subgroups, and Factor Groups

5. Use Example 3.8.1 and the parity mapping defined in Example 3.7.8 to give a short proof that in any subgroup H of S_n, either all permutations in H are even, or else half of the permutations in H are even and half are odd.

Solution: Let $\phi : S_n \to \{\pm 1\}$ be the homomorphism defined in Example 3.7.8, which maps even permutations to 1 and odd permutations to -1. Define $\theta : H \to \{\pm 1\}$ to be the inclusion mapping followed by ϕ. Since θ is the composite of two homomorphisms, it is a homomorphism. Then either θ is the trivial mapping, in which case every permutation in H is even, or else there are two cosets of the kernel: the set of even permutations in H and the set of odd permutations in H. This completes the proof, since by Example 3.8.1 both cosets have the same number of elements.

16. Let G_1, G_2, G_3 be groups such that G_1 is a homomorphic image of both G_2 and G_3. If $|G_2| = 24$ and $|G_3| = 30$, list the possibilities for G_1 (up to isomorphism).

Solution: The order of G_1 must be a common divisor of 24 and 30, so it is a divisor of 6. Thus G_1 is isomorphic to one of the groups on this list: the trivial one-element group, $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_6$, or S_3. Recall that by Exercise 21 of Section 3.3 any group of order 6 is either cyclic or isomorphic to the symmetric group S_3.

4 POLYNOMIALS

4.1. Fields; Roots of Polynomials

7. Prove that if p is a prime number, then the multiplicative group $\mathbf{Z}_p^\times$ is cyclic.

Solution: We will use Proposition 3.5.9 (b), which states that a finite abelian group is cyclic if and only if its exponent is equal to its order. Suppose that the exponent of $\mathbf{Z}_p^\times$ is m. Then $a^m = 1$ for all nonzero $a \in \mathbf{Z}_p^\times$, and so the polynomial $x^m - 1$ has $p-1$ distinct roots in $\mathbf{Z}_p^\times$, and it follows from Corollary 4.1.12 that $p-1 \leq m$. By definition, $m \leq p-1 = |\mathbf{Z}_p^\times|$, so $m = |\mathbf{Z}_p^\times|$ and therefore $\mathbf{Z}_p^\times$ is cyclic.

8. Let p be a prime number, and let $a, b \in \mathbf{Z}_p^\times$. Show that if neither a nor b is a square, then ab *is* a square.

Solution: By Exercise 7, we can choose a generator g for $\mathbf{Z}_p^\times$. If neither a nor b is a square, then $a = g^s$ and $b = g^t$, where s and t are odd. Therefore $ab = (g^k)^2$, where $s + t = 2k$, and so ab is a square.

4.2. Factors

12. Find the irreducible factors of $2x^3 + x^2 + 2x + 2$ over $\mathbf{Z}_5$.

Solution: We first factor out 2, using $(2)(-2) = -4 \equiv 1 \pmod 5$. This reduces the question to factoring $p(x) = x^3 - 2x^2 + x + 1$. Checking for roots shows that $p(0) = 1$, $p(1) = 1$, $p(-1) = -3$, $p(2) = 3$, and $p(-2) \equiv -2$, so $p(x)$ has no roots in $\mathbf{Z}_5$. Then $p(x)$ is irreducible over $\mathbf{Z}_5$ by Proposition 4.2.7.

15. Show that $x^4 + 1$ has a proper factorization over $\mathbf{Z}_p$, for all primes p.

Solution: We will show that $x^4 + 1$ can always be factored as the product of two quadratic polynomials.

If $p = 2$, then $x^4 + 1 = (x^2 + 1)^2$.

If $p = 3$, then $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$. (See the answer to Exercise 14 (d).)

If $p \geq 5$, then $\mathbf{Z}_p$ contains the elements $-1, \pm 2$. Exercise 8 of Section 4.1 shows that if neither -1 nor 2 is a square, then their product -2 must be a square.

If -1 is a square, say $a^2 = -1$, then $x^4 + 1 = (x^2 + a)(x^2 - a)$. If 2 is a square, say $a^2 = 2$, then $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$. If -2 is a square, say $a^2 = -2$, then $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$.

This completes the proof.

Comments: The proof gives no idea as to how we arrived at these factorizations. As motivation, we offer the following discussion. Since $x^4 + 1$ is monic, we can

assume that its factors are monic. Suppose we have a factorization $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$. Looking at the coefficients of x^3 and x, we see that $c = -a$, and then $ad = ab$. If $a = 0$, then $x^4 + 1 = (x^2 + b)(x^2 + d)$, forcing $d = -b$ and so the only possible factorization is $x^4 + 1 = (x^2 + b)(x^2 - b)$, with $b^2 = -1$.

If $a \neq 0$, then cancelling yields $d = b$, forcing $b = \pm 1$ since $b^2 = 1$. In this case the factorization must be $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$ or $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$.

4.3. Existence of Roots

2. Prove Proposition 4.3.4.

Solution: **(a)** Given that $a(x) \equiv c(x) \pmod{p(x)}$ and $b(x) \equiv d(x) \pmod{p(x)}$, it follows that $p(x) \mid (a(x) - c(x))$ and $p(x) \mid (b(x) - d(x))$. Therefore $p(x) \mid (a(x) - c(x) + b(x) - d(x))$, and so $p(x) \mid ((a(x) + b(x)) - (c(x) + d(x)))$. Hence $a(x) + b(x) \equiv c(x) + d(x) \pmod{p(x)}$. Furthermore, $a(x)b(x) - c(x)d(x) = a(x)(b(x) - d(x)) + d(x)(a(x) - c(x))$ implies that $p(x) \mid (a(x)b(x) - c(x)d(x))$. Hence $a(x)b(x) \equiv c(x)d(x) \pmod{p(x)}$.

(b) Since $\gcd(a(x), p(x)) = 1$, there exist polynomials $f(x)$ and $g(x)$ such that $f(x)a(x) + g(x)p(x) = 1$. Since $a(x)b(x) \equiv a(x)c(x) \pmod{p(x)}$, we have $p(x) \mid (a(x)b(x) - a(x)c(x))$. Now

$$\begin{aligned} b(x) - c(x) &= f(x)a(x)b(x) + g(x)p(x)b(x) - f(x)a(x)c(x) - g(x)p(x)c(x) \\ &= f(x)(a(x)b(x) - a(x)c(x)) + p(x)(g(x)b(x) - g(x)c(x)). \end{aligned}$$

Since $p(x) \mid a(x)b(x) - a(x)c(x)$, we have $p(x) \mid (b(x) - c(x))$, and therefore $b(x) \equiv c(x) \pmod{p(x)}$.

17. Prove that the set of all matrices over $\mathbf{Z}_3$ of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a field isomorphic to $\mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$.

Solution: Let F be the given set of matrices, and note that F has 9 elements. The formulas in Appendix A.5, although given for matrices with entries in $\mathbf{R}$, remain valid for matrices with entries in $\mathbf{Z}_3$. It is then easy to check that F is closed under addition and multiplication, has a zero element and additive inverses, has a multiplicative identity, and satisfies the associative, distributive, and commutative laws. For a matrix in F, if $a \neq 0$ and $b = 0$, then $a^2 + b^2 = 1$; if $a = 0$ and $b \neq 0$, then $a^2 + b^2 = 1$; if $a \neq 0$ and $b \neq 0$, then $a^2 + b^2 = 2$. Thus the nonzero matrices in F are invertible, since they have a nonzero determinant, and so F is a field.

Define $\phi : \mathbf{Z}_3[x]/\langle x^2+1\rangle \to F$ by $\phi([a+bx]) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.
The mapping is well-defined since each congruence class in $\mathbf{Z}_3[x]/\langle x^2+1\rangle$ contains a unique representative of the form $a+bx$, and simply listing the possible values of ϕ shows it to be a one-to-one correspondence. It is clear that ϕ will preserve addition. That ϕ preserves multiplication depends on the fact that the congruence class $[x]$, which satisfies the equation $[x]^2 = -[1]$, maps to the matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, which satisfies the corresponding equation $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

20. Find all powers of $[x]$ in $\mathbf{Z}_3[x]/\langle x^2+x+2\rangle$, and then find $[x]^{-1}$.

Solution: Since $x^2 \equiv -x-2 \equiv 2x+1 \pmod{x^2+x+2}$, we have the following list:
$[x]^1 = [x]$,
$[x]^2 = [2x+1]$,
$[x]^3 = [x][2x+1] = [2x^2+x] = [4x+2+x)] = [2x+2]$,
$[x]^4 = [x][2x+2] = [2x^2+2x] = [4x+2+2x] = [2] = [-1]$,
$[x]^5 = [-1][x] = [2x]$,
$[x]^6 = [-1][x^2] = [x+2]$,
$[x]^7 = [-1][x]^3 = [x+1]$,
$[x]^8 = ([x]^4)^2 = [1]$.
Since $[x]$ has order 8 in the multiplicative group of the field, its inverse is $[x]^7 = [x+1]$.

Comment: Each nonzero element of $\mathbf{Z}_3/\langle x^2+x-1\rangle$ is a power of $[x]$, so we have shown that the multiplicative group of this finite field is cyclic, with generator $[x]$.

4.4. Polynomials over Z, Q, R, and C

1. Let $f(x), g(x) \in \mathbf{Z}[x]$, and suppose that $g(x)$ is monic. Show that there exist unique polynomials $q(x), r(x) \in \mathbf{Z}[x]$ with $f(x) = q(x)g(x)+r(x)$, where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Solution: Let $f(x) = a_m x^m + \ldots + a_1 x + a_0$, and $g(x) = x^n + \ldots + b_0$, where $a_m \neq 0$. If $f(x)$ has lower degree than $g(x)$, then $q(x) = 0$ and $r(x) = f(x)$ satisfy the requirements. The proof of the other case will use induction on the degree of $f(x)$.

If $f(x)$ has degree zero, it is easy to see that the theorem holds. In order to appeal to the second principle of mathematical induction, assume that the theorem is true for all polynomials $f(x)$ of degree less than m. (We are assuming that $m \geq n$.) The reduction to a polynomial of lower degree is achieved by using the procedure

outlined in Example 4.2.1. We divide $a_m x^m$ by x^n to get $a_m x^{m-n}$, then multiply by $g(x)$ and subtract from $f(x)$. This gives $f_1(x) = f(x) - a_m x^{m-n} g(x)$, where $f_1(x)$ has degree less than m since the leading term of $f(x)$ has been cancelled by $a_m x^{m-n} x^n$. Now by the induction hypothesis there exist $q_1(x), r(x) \in \mathbf{Z}[x]$ such that $f_1(x) = q_1(x)g(x) + r(x)$, where the degree of $r(x)$ is less than n, unless $r(x) = 0$. Since $f(x) = f_1(x) + a_m x^{m-n} g(x)$, substitution gives the desired result:

$$f(x) = \left(q_1(x) + a_m x^{m-n}\right) g(x) + r(x) \ .$$

The quotient $q(x) = q_1(x) + a_m x^{m-n}$ has coefficients in $\mathbf{Z}$, since $a_m \in \mathbf{Z}$ and $q_1(x) \in \mathbf{Z}[x]$. The proof that the quotient $q(x)$ and remainder $r(x)$ are unique follows exactly as in the proof of Theorem 4.2.1.

5 RINGS

5.1. Commutative Rings; Integral Domains

8. Let R be a commutative ring, and let $f(x), g(x) \in R[x]$, where $g(x)$ is monic. Show that there exist unique polynomials $q(x)$, $r(x) \in R[x]$ such that $f(x) = q(x)g(x)+r(x)$, where $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Solution: Let $f(x) = a_m x^m + \ldots + a_1 x + a_0$ and $g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$, where $a_m \neq 0$. In the proof of Theorem 4.2.1, the induction step uses the polynomial $f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$, where b_n is the leading coefficient of $g(x)$. In this case $g(x)$ is monic, so $b_n = 1$, and we can use the polynomial $f_1(x) = f(x) - a_m x^{m-n} g(x)$ instead.

The next difficulty arises in showing that the quotient $q(x)$ and remainder $r(x)$ are unique. The proof of Theorem 4.2.1 uses Proposition 4.1.5, which does hold if R is an integral domain (by Example 5.1.8) but may fail in general. If $f(x) = q_1(x)g(x) + r_1(x)$ and $f(x) = q_2(x)g(x) + r_2(x)$, then $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$, as in the proof of Theorem 4.2.1. If $q_2(x) - q_1(x) \neq 0$, then the degree of $(q_2(x) - q_1(x))g(x)$ is greater than or equal to the degree of $g(x)$ because $g(x)$ is monic. The degree of $r_2(x) - r_1(x)$ is less than the degree of $g(x)$, so we still reach a contradiction, completing the proof.

5.2. Ring Homomorphisms

6. Show that the ring of Gaussian integers $\mathbf{Z}[i]$ defined in Example 5.1.5 is isomorphic to $\mathbf{Z}[x]/\langle x^2 + 1 \rangle$.

Solution: Define $\phi : \mathbf{Z}[x] \to \mathbf{C}$ by $\phi(f(x)) = f(i)$, for all $f(x) \in \mathbf{Z}[x]$. This is the mapping defined in Proposition 5.2.7, and so we know that it is a ring homomorphism. It is clear that $\phi(\mathbf{Z}[x]) = \mathbf{Z}[i]$ and that $x^2 + 1 \in \ker(\phi)$.

To show that $\ker(\phi) = \langle x^2+1 \rangle$, suppose that $f(x) \in \ker(\phi)$. Considering $f(x)$ as an element of $\mathbf{Q}[x]$, we can divide by x^2+1 to get $f(x) = q(x)(x^2+1) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < 2$. Since x^2+1 is monic, it follows from Exercise 1 of Section 4.4 that $q(x)$ and $r(x)$ belong to $\mathbf{Z}[x]$, so $r(x) = m + nx$ for some $m, n \in \mathbf{Z}$. Substituting $x = i$ shows that $m + ni = 0$ in $\mathbf{C}$, so $m = n = 0$, and therefore $r(x)$ is the zero polynomial. Thus we have shown that $f(x) \in \langle x^2 + 1 \rangle$.

Since $\ker(\phi) = \langle x^2 + 1 \rangle$ and $\phi(\mathbf{Z}[x]) = \mathbf{Z}[i]$, it follows from the fundamental homomorphism theorem that $\mathbf{Z}[i] \cong \mathbf{Z}[x]/\langle x^2 + 1 \rangle$.

8. Let F be the field $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$ defined in Example 4.3.4. Show that F has precisely two automorphisms.

Solution: Any automorphism maps 0 to 0 and 1 to 1. Using the congruence classes given in Example 4.3.4, the only possibility to define an automorphism $\phi : F \to F$ that is not the identity mapping is to define $\phi([x]) = [1 + x]$ and $\phi([1 + x]) = [x]$. To show that this defines an automorphism, note that $[1 + x] = [x^2] = [x]^2$, and consider the formula $\theta(r) = r^2$, for all $r \in F$. Then $\theta(0) = 0$ and $\theta(1) = 1$, $\theta([x]) = [x]^2 = [1+x]$, and $\theta([1+x]) = [1+x]^2 = [x]$, by the multiplication table given in Example 4.3.4. For $r, s \in F$, we have $\theta(rs) = (rs)^2 = r^2s^2 = \theta(r)\theta(s)$. We also have $\theta(r + s) = (r + s)^2 = r^2 + 2rs + s^2$. But since $[1] + [1] = [0]$, the field F has characteristic 2, so we have $2rs = 0$. Thus $\theta(r + s) = \theta(r) + \theta(s)$, verifying that $\phi = \theta$ is the second automorphism of F.

Looking ahead: The mapping θ is a special case of the *Frobenius automorphism* introduced in Definition 8.1.8.

5.3. Ideals and Factor Rings

11. Show that if R is a Boolean ring, then every prime ideal of R is maximal.

Solution: We will prove a stronger result: if R is a Boolean ring and P is a prime ideal of R, then $R/P \cong \mathbf{Z}_2$. Since $\mathbf{Z}_2$ is a field, Proposition 5.3.9 (a) implies that P is a maximal ideal.

If $a \in R$, then $a^2 = a$, and so $a(a - 1) = 0$. Since P is an ideal, it contains 0, and then $a(a - 1) \in P$ implies $a \in P$ or $a - 1 \in P$, since P is prime. Thus each element of R is in either P or $1 + P$, so there are only two cosets of P in R/P, and therefore R/P must be the ring $\mathbf{Z}_2$.

17. Let I, J be ideals of the commutative ring R, and for $r \in R$, define the function $\phi : R \to R/I \oplus R/J$ by $\phi(r) = (r + I, r + J)$.

(a) Show that ϕ is a ring homomorphism, with $\ker(\phi) = I \cap J$.

Solution: The fact that ϕ is a ring homomorphism follows immediately from the definitions of the operations in a direct sum and in a factor ring. Since the zero element of $R/I \oplus R/J$ is $(0 + I, 0 + J)$, we have $r \in \ker(\phi)$ if and only if $r \in I$ and $r \in J$, so $\ker(\phi) = I \cap J$.

(b) Show that if $I + J = R$, then ϕ is onto, and thus $R/(I \cap J) \cong R/I \oplus R/J$.

Solution: If $I + J = R$, then we can write $1 = x + y$, for some $x \in I$ and $y \in J$. Given any element $(a + I, b + J) \in R/I \oplus R/J$, consider $r = bx + ay$. Then $r + I = bx + ay + I = ay + I = a(1 - x) + I = a + I$, and similarly $r + J = b + J$. Thus $\phi(r) = (a + I, b + J)$, and ϕ is onto. The isomorphism follows from the fundamental homomorphism theorem.

Note: This can be called the Chinese remainder theorem for commutative rings. It is interesting to compare the above proof with the one given for Theorem 1.3.6.

20. Let I, J be ideals of the commutative ring R. Show that if $I + J = R$, then $I^2 + J^2 = R$.

Solution: If $I + J = R$, then there exist $a \in I$ and $b \in J$ with $a + b = 1$. Cubing both sides gives us $a^3 + 3a^2b + 3ab^2 + b^3 = 1$. Then $a^3 + 3a^2b \in I^2$ and $3ab^2 + b^3 \in J^2$, so $I^2 + J^2 = R$.

32. Let R be the set of all rational numbers m/n such that n is odd.

(a) Show that R is a subring of $\mathbf{Q}$.

Solution: If $\frac{m_1}{n_1}$, $\frac{m_2}{n_2} \in R$, then n_1 and n_2 are odd. Since n_1n_2 is odd, we have $\frac{m_1}{n_1} \pm \frac{m_2}{n_2} = \frac{m_1n_2 \pm m_2n_1}{n_1n_2} \in R$ and $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1m_2}{n_1n_2} \in R$. Thus R is a subring of $\mathbf{Q}$.

(b) Let $2^kR = \{m/n \in R \mid m \text{ is a multiple of } 2^k \text{ and } n \text{ is odd}\}$, for any positive integer k. Show that 2^kR is an ideal of R.

Solution: If $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ belong to 2^kR, then n_1 and n_2 are odd and $2^k \mid m_1$ and $2^k \mid m_2$. Then n_1n_2 is odd and $2^k \mid (m_1n_2 \pm m_2n_1)$, and so $\frac{m_1}{n_1} \pm \frac{m_2}{n_2} = \frac{m_1n_2 \pm m_2n_1}{n_1n_2}$ belongs to 2^kR. If $\frac{r}{s} \in R$ and $\frac{m}{n} \in 2^kR$, then s and n are odd and $2^k \mid m$. Then ns is odd and $2^k \mid mr$. Hence $\frac{r}{s} \cdot \frac{m}{n} = \frac{rm}{ns} \in 2^kR$. Therefore 2^kR is an ideal of R.

(c) Show that each proper nonzero ideal of R has the form 2^kR, for some positive integer k.

Solution: Let I be a proper nonzero ideal of R, with $0 \neq \frac{m_0}{n_0} \in I$. Then it is easy to check that $I \cap \mathbf{Z}$ is an ideal of $\mathbf{Z}$, and $m_0 = n_0 \cdot \frac{m_0}{n_0}$ is a nonzero element of $I \cap \mathbf{Z}$. Therefore $I \cap \mathbf{Z} = u\mathbf{Z}$, for some nonzero $u \in \mathbf{Z}$. Then u cannot be odd, since this would imply that $1 = \frac{1}{u} \cdot u \in I$, so we can write $u = 2^kv$, where $2 \nmid v$ and k is positive. Then for any $\frac{m}{n} \in I$, we have $n \cdot \frac{m}{n} = qu$, for some $q \in \mathbf{Z}$. Therefore $\frac{m}{n} = 2^k \cdot \frac{qv}{n}$, as required.

(d) Show that $R/2^kR$ is isomorphic to $\mathbf{Z}_{2^k}$.

Solution: Given $\frac{m}{n} \in R$, since $(n, 2^k) = 1$ there exist $u, v \in \mathbf{Z}$ with $2^kv + nu = 1$. Hence $m = mnu + mv2^k$, and so $\frac{m}{n} = \frac{mu + mv2^k}{n}$, which implies that $\frac{m}{n} + 2^kR = mu + 2^kR$. Write $mu = 2^kq + r$, where $0 \leq r < 2^k$. Then $mu + 2^kR = r + 2^kR$ where $0 \leq r < 2^k$. If $r_1 + 2^kR = r_2 + 2^kR$ where $0 \leq r_1 < 2^k$ and $0 \leq r_2 < 2^k$, then $r_1 - r_2 = \frac{m2^k}{n}$, where n is odd. Hence $2^k \mid n(r_1 - r_2)$, and since $(2^k, n) = 1$ we have $r_1 \equiv r_2 \pmod{2^k}$. Since $0 \leq r_1 < 2^k$ and $0 \leq r_2 < 2^k$ we have $r_1 = r_2$. Thus every element of $R/2^kR$ can be written uniquely in the form $r + 2^kR$ where

$0 \leq r < 2^k$ and $r \in \mathbf{Z}$. Define $\phi : R/2^kR \to \mathbf{Z}_{2^k}$ by $\phi(r + 2^kR) = [r]_{2^k}$. Since

$$\begin{aligned} \phi((r_1 + 2^kR) + (r_2 + 2^kR)) &= \phi(r + 2^kR) = [r]_{2^k} \\ &= [r_1]_{2^k} + [r_2]_{2^k} \\ &= \phi(r_1 + 2^kR) + \phi(r_2 + 2^kR) \end{aligned}$$

and

$$\begin{aligned} \phi((r_1 + 2^kR)(r_2 + 2^kR)) &= \phi(r_1r_2 + 2^kR) = \phi(s + 2^kR) \\ &= [s]_{2^k} = [r_1]_{2^k}[r_2]_{2^k} \\ &= \phi(r_1 + 2^kR)\phi(r_2 + 2^kR) \end{aligned}$$

where $r \equiv r_1 + r_2 \pmod{2^k}$ with $0 \leq r < 2^k$ and $s \equiv r_1r_2 \pmod{2^k}$ with $0 \leq s < 2^k$, it follows that ϕ is a ring homomorphism.

Given $[r]_{2^k} \in \mathbf{Z}_{2^k}$ we have $\phi(r + 2^kR) = [r]_{2^k}$ and so ϕ is onto.

(e) Show that $2R$ is the unique maximal ideal of R.

Solution: It follows from part (d) that $2R$ is a maximal ideal, since $R/2R$ is a field. It follows from part (c) that every other proper ideal is contained in $2R$.

5.4. Quotient Fields

12. Show that if P is a prime ideal of D, then $D_P = \{a/b \in Q(D) \mid b \notin P\}$ is an integral domain with $D \subseteq D_P \subseteq Q(D)$.

Solution: Let a/b and c/d belong to D_P. Then $b, d \in D - P$, and so $bd \in D - P$ since P is a prime ideal. It follows that $a/b + c/d = (ad + bc)/(bd) \in D_P$ and $(a/b)(c/d) = (ac)/(bd) \in D_P$, and so D_P is closed under addition and multiplication. Since $1 \notin P$, the given set includes D. Finally, since $Q(D)$ is a field, the subring D_P is an integral domain.

13. In the ring D_P defined in Exercise 12, let $M = \{a/b \in D_P \mid a \in P\}$.

(a) Show that M is an ideal of D_P.

Solution: The subset M is nonempty, since $0 = 0/1 \in M$. Let a/b and c/d belong to M. Then $(a/b) \pm (c/d) = (ad \pm bc)/(bd) \in M$ since $a, c \in P$ implies that $ad \pm bc \in P$. If $r/s \in D_P$, then $(r/s) \cdot (a/b) = ra/sb \in M$ since $ra \in P$. Therefore M is an ideal of D_P.

(b) Show that $D_P/M \cong Q(D/P)$, and conclude that M is a maximal ideal of D_P.

Solution: Note that we have the following chain of subrings: $D \subseteq D_P \subseteq Q(D)$. It is clear that $P \subseteq D \cap M$. If $a/b \in D \cap M$, then $a/b \sim r/1$ for some $r \in D$, so

$rb = a \in P$. Since P is a prime ideal and $b \notin P$, we must have $r \in P$, showing that $P = D \cap M$.

Since $P = D \cap M$, the inclusion $\theta : D \to D_P$ maps P into M, and therefore $\overline{\theta} : D/P \to D_P/M$ defined by $\overline{\theta}(x+P) = (x/1)+M$ is well-defined. It is easy to check that $\overline{\theta}$ is a ring homomorphism, since its definition just depends on an inclusion mapping. If $b \notin P$, then $b/1 \notin M$, and so $\overline{\theta}$ has zero kernel, and is therefore one-to-one.

For $b \notin P$, the element $b+P$ is invertible in $Q(D/P)$, and $\overline{\theta}(b+P) = (b/1)+M$ is invertible in D_P/M since $((b/1)+M)((1/b)+M) = 1+M$. As in Theorem 5.4.6 it can be shown that there exists a one-to-one ring homomorphism $\widehat{\theta} : Q(D/P) \to D_P/M$ defined by $\widehat{\theta}\left(\dfrac{x+P}{y+P}\right) = \overline{\theta}(x+P)\left(\overline{\theta}(y+P)\right)^{-1}$, for $x+P$, $y+P$ in $Q(D/P)$, where $y+P$ is nonzero. For each $(a/b)+M$ in D_P/M, we have

$$(a/b)+M = ((a/1)+M)\,((b/1)+M)^{-1} = \widehat{\theta}(a+P)\widehat{\theta}(b+P)^{-1} = \widehat{\theta}\left(\frac{a+P}{b+P}\right),$$

and so $\widehat{\theta}$ is onto. Thus D_P/M is isomorphic to a field, and so M is a maximal ideal. The following diagram shows the mappings $\overline{\theta}$ and $\widehat{\theta}$.

$$\begin{array}{ccc} D/P & \subseteq & Q(D/P) \\ & \overline{\theta}\searrow \quad \downarrow \widehat{\theta} & \\ & D_P/M & \end{array}$$

6 FIELDS

6.1. Algebraic Elements

7. Let $u, v \in \mathbf{Q}^+$, where $u \neq v$ and u, v, uv are not squares. Find the minimal polynomial for $\sqrt{u} + \sqrt{v}$ over $\mathbf{Q}$.

Solution: Let $\alpha = \sqrt{u} + \sqrt{v}$. Then $\left(\alpha - \sqrt{u}\right)^2 = v$ and so $\alpha^2 - 2\sqrt{u}\alpha + u = v$. Thus $\alpha^2 + u - v = 2\sqrt{u}\alpha$ and therefore $\left(\alpha^2 + u - v\right)^2 = 4u\alpha^2$. Hence $\alpha^4 + 2(u-v)\alpha^2 + (u-v)^2 = 4u\alpha^2$ and so $\alpha^4 - 2(u+v)\alpha^2 + (u-v)^2 = 0$. Thus α is a root of $f(x) = x^4 - 2(u+v)x^2 + (u-v)^2$.

We will find all the roots of $f(x)$. By the quadratic formula, we have

$$\begin{aligned} x^2 &= \frac{2(u+v) \pm \sqrt{4(u+v)^2 - 4(u-v)^2}}{2} \\ &= u + v \pm \sqrt{4uv} \\ &= u \pm 2\sqrt{u}\sqrt{v} + v \\ &= (\sqrt{u} \pm \sqrt{v})^2 . \end{aligned}$$

Thus $x = \pm(\sqrt{u} \pm \sqrt{v})$, so the set S of four roots of $f(x)$ is $S = \{\pm\sqrt{u} \pm \sqrt{v}\}$.

We will show that $f(x)$ is irreducible in $\mathbf{Q}[x]$. Since none of the four roots of $f(x)$ is an element of $\mathbf{Q}$, $f(x)$ has no factor of degree 1 in $\mathbf{Q}[x]$. If $f(x)$ had a factor $h(x)$ of degree 2 in $\mathbf{Q}[x]$, then $h(x)$ would have two roots in the set S. Let $r_1 = \sqrt{u} + \sqrt{v}, r_2 = \sqrt{u} - \sqrt{v}, r_3 = -\sqrt{u} + \sqrt{v}, r_4 = -\sqrt{u} - \sqrt{v}$. If r_i, r_j are two roots of $h(x)$, then $r_i + r_j \in \mathbf{Q}$ and $r_i r_j \in \mathbf{Q}$ by Exercise 10 of Section 4.4. Since $r_1 + r_2 \notin \mathbf{Q}$, $r_1 + r_3 \notin \mathbf{Q}$, $r_1 r_4 \notin \mathbf{Q}$, $r_2 r_3 \notin \mathbf{Q}$, $r_2 + r_4 \notin \mathbf{Q}$, $r_3 + r_4 \notin \mathbf{Q}$, no such factor $h(x)$ of degree 2 exists.

Since $f(x)$ is irreducible, it is the minimal polynomial of $\sqrt{v} + \sqrt{v}$ over $\mathbf{Q}$.

6.2. Finite and Algebraic Elements

5. Let $F \supset K$ be an extension field, with $u \in F$. Show that if $[K(u) : K]$ is an odd number, then $K(u^2) = K(u)$.

Solution: Since $u^2 \in K(u)$, we have $K(u) \supseteq K(u^2) \supset K$. Suppose that $u \notin K(u^2)$. Then $x^2 - u^2$ is irreducible over $K(u^2)$ since it has no roots in $K(u^2)$, so u is a root of the irreducible polynomial $x^2 - u^2$ over $K(u^2)$. Thus $[K(u) : K(u^2)] = 2$, and therefore 2 is a factor of $[K(u) : K]$. This contracts the assumption that $[K(u) : K]$ is odd.

7. Let F be a field generated over the field K by u and v of relatively prime degrees m and n, respectively, over K. Prove that $[F : K] = mn$.

Solution: Since $F = K(u, v) \supseteq K(u) \supseteq K$, where $[K(u) : K] = m$ and $[K(u, v) : K(u)] \leq n$, we have $[F : K] \leq mn$. But $[K(v) : K] = n$ is a divisor of $[F : K]$, and since $\gcd(m, n) = 1$, we must have $[F : K] = mn$.
Note: A proof can also be given using Exercise 6.

8. Find the degree of $\sqrt[3]{2} + i$ over $\mathbf{Q}$

Solution: Let $u = \sqrt[3]{2} + i$, so that $u - i = \sqrt[3]{2}$. Then $(u - i)^3 = 2$, so we have $u^3 - 3iu^2 + 3i^2u - i^3 = 2$, or $u^3 - 3iu^2 - 3u + i = 2$. Solving for i we get $i = (u^3 - 3u - 2)/(3u^2 - 1)$, and this shows that $i \in \mathbf{Q}(\sqrt[3]{2} + i)$. Thus $\sqrt[3]{2} \in \mathbf{Q}(\sqrt[3]{2} + i)$, and so $\mathbf{Q}(\sqrt[3]{2} + i) = \mathbf{Q}(\sqrt[3]{2}, i)$.

Since $x^3 - 2$ is irreducible over $\mathbf{Q}$, the number $\sqrt[3]{2}$ has degree 3 over $\mathbf{Q}$. Since $x^2 + 1$ is irreducible over $\mathbf{Q}$, we see that i has degree 2 over $\mathbf{Q}$. It follows from Exercise 7 that therefore $[\mathbf{Q}(\sqrt[3]{2} + i) : \mathbf{Q}] = 6$.

6.4. Splitting Fields

1. Determine the splitting fields in $\mathbf{C}$ for the following polynomials (over $\mathbf{Q}$).

(c) $x^4 + 4$

Solution: We have $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, where the factors are irreducible by Eisenstein's criterion, with $p = 2$. Applying the quadratic formula, we see that the roots are $\pm 1 \pm i$, so the splitting field is $\mathbf{Q}(i)$, which has degree 2 over $\mathbf{Q}$.

Alternate solution: We could also solve the equation $x^4 = -4$. To find one root, use DeMoivre's theorem to get $\sqrt[4]{-1} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$, and then multiply by $\sqrt[4]{4} = \sqrt{2}$, to get $1 + i$. The other roots are found by multiplying by the powers of i, because it is a primitive 4th root of unity.

2. Determine the splitting fields in $\mathbf{C}$ for the following polynomials (over $\mathbf{Q}$).

(c) $x^4 + 1$

Solution: Let F be the splitting field for $x^4 + 1$ over Q. Since $(x + 1)^4 + 1$ satisfies Eisenstein's criterion, $x^4 + 1$ is irreducible over $\mathbf{Q}$, and so adjoining a root of $x^4 + 1$ to $\mathbf{Q}$ will produce an extension of degree 4 by Proposition 6.2.2. Thus $[F : \mathbf{Q}] \geq 4$.

To find a 4th root of -1, we can use the procedure outlined in Example A.5.3 of Appendix A.5, which yields the root $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$. To find all roots, we can multiply this one by the 4th roots of unity: $\pm 1, \pm i$. It is then clear that $F \subseteq \mathbf{Q}(\sqrt{2}, i)$, and since $[\mathbf{Q}(\sqrt{2}, i) : \mathbf{Q}] = 4$, we must have $F = \mathbf{Q}(\sqrt{2}, i)$.

Alternate solution: We have
$x^4 + 1 = (x^2 + i)(x^2 - i) = (x + i\sqrt{i})(x - i\sqrt{i})(x + \sqrt{i})(x - \sqrt{i})$.
Since $\sqrt{i} = (\sqrt{2} + \sqrt{2}i)/2$ it follows that the splitting field of $x^4 + 1$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{i}) = \mathbf{Q}(i\sqrt{i}, \sqrt{i}) = \mathbf{Q}(\sqrt{2}, i)$.

(d) $x^6 - 1$

Discussion: Be careful here–this polynomial is not irreducible. In fact, $x^6 - 1$ factors in two ways, and provides an important clue. Note that $x^6-1 = (x^3)^2-1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$ and $x^6-1 = (x^2)^3-1 = (x^2-1)(x^4+x^2+1)$.

Solution: We have
$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$.
The roots of $x^2 + x + 1$ are the primitive third roots of unity. (See Definition 4.4.8 and Example A.5.1). The roots of $x^2 - x + 1$ are therefore the primitive sixth roots of unity. Adjoining a root $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ of $x^2 - x + 1$ gives all four of these roots, and so $\mathbf{Q}(\omega)$ is the splitting field of $x^6 - 1$ over $\mathbf{Q}$, with $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$.

11. Let K be a field, and let F be an extension field of K. Let $\phi : F \to F$ be an automorphism of F such that $\phi(a) = a$, for all $a \in K$. Show that for any polynomial $f(x) \in K[x]$, and any root $u \in F$ of $f(x)$, the image $\phi(u)$ must be a root of $f(x)$.

Solution: Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$, where $a_i \in K$, for $i = 0, 1, \ldots, n$. If $u \in F$ with $f(u) = 0$, then we have $\phi(f(u)) = \phi(a_0 + a_1u + \ldots + a_nu^n) = \phi(a_0) + \phi(a_1u) + \ldots + \phi(a_nu^n) = \phi(a_0) + \phi(a_1)\phi(u) + \ldots + \phi(a_n)(\phi(u))^n$ since ϕ preserves sums and products. Finally, since $\phi(a_i) = a_i$ for $i = 0, 1, \ldots, n$, we have $\phi(f(u)) = a_0 + a_1\phi(u) + \ldots + a_n(\phi(u))^n$. Since $f(u) = 0$, we must have $\phi(f(u)) = 0$, and thus $a_0 + a_1\phi(u) + \ldots + a_n(\phi(u))^n = 0$, showing that $f(\phi(u)) = 0$. This completes the proof that $\phi(u)$ is a root of $f(x)$.

6.5. Finite Fields

4. **(a)** Factor $x^6 - 1$ over GF(7)

Solution: This is a direct application of Theorem 6.5.2. We have
$x^6 - 1 = (x - 1)(x + 1)(x - 2)(x + 2)(x - 3)(x + 3)$.

(b) Factor $x^5 - 1$ over GF(11)

Solution: Looking for roots of $x^5 - 1$ in GF(11) is the same as looking for elements whose order is a divisor of 5 in the multiplicative group GF(11)$^\times$. Theorem 6.5.10 implies that GF(11)$^\times$ is cyclic of order 10. Thus it contains 4 elements of order 5, which means the $x^5 - 1$ must split over GF(11). To look for a generator, we begin with 2. The relevant powers of 2 are $2^2 = 4$ and $2^5 \equiv -1$, so 2 must be a generator

since it has order 10. The even powers of 2 have order 5, and these are $2^2 = 4$, $2^4 \equiv 5, 2^6 \equiv 9$, and $2^8 \equiv 3$. Therefore $x^5 - 1 = (x-1)(x-3)(x-4)(x-5)(x-9)$ over GF(11).

6. Find the splitting field of $x^4 - 1$ over GF(7).

Solution: We have $x^4 - 1 = (x-1)(x+1)(x^2+1)$. A quick check of ± 2 and ± 3 shows that they are not roots of $x^2 + 1$, so $x^2 + 1$ is irreducible over GF(7). To obtain the splitting field we must adjoin a root of $x^2 + 1$, so we get a splitting field $\mathrm{GF}(7^2) \cong \mathbf{Z}_7[x]/\langle x^2 + 1 \rangle$ of degree 2 over GF(7).

15. Let F be a field whose multiplicative group $F^\times$ is cyclic. Prove that F must be a finite field.

Solution: Suppose that $F^\times = \langle u \rangle$. If $\mathrm{char}(F) \neq 2$, then $-1 \neq 1$, so $-1 \in F^\times$ and therefore $-1 = u^n$ for some nonzero integer n. Then $u^{2n} = 1$, so $\langle u \rangle$ is finite, and therefore F is finite.

If $\mathrm{char}(F) = 2$, and $u \neq 1$, then $1 + u \neq 0$, so $1 + u = u^n$ or $1 + u = u^{-n}$, for some positive integer n. Then $u^n - u - 1 = 0$ in the first case, and $u^{n+1} + u^n - 1 = 0$ in the second, so u is algebraic over the base field GF(2). Thus $F = \mathrm{GF}(2)(u)$ is finite.

7 STRUCTURE OF GROUPS

7.1. Isomorphism Theorems; Automorphisms

6. Prove that a finite group whose only automorphism is the identity map must have order at most two.

Solution: Let G be a nontrivial finite group with $\mathrm{Aut}(G) = \{1_G\}$. Since all inner automorphisms are trivial, G is abelian. Then $\alpha : G \to G$ defined by $\alpha(g) = g^{-1}$, for all $g \in G$, is an automorphism since it is a one-to-one correspondence and $\alpha(ab) = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1} = \alpha(a)\alpha(b)$, for all $a, b \in G$. Since α is trivial, we have $g = g^{-1}$ for all $g \in G$, and thus every nontrivial element of G has order 2. If G is written additively, we can therefore define a vector space structure over the field $\mathbf{Z}_2$ by defining $0 \cdot x = 0$ and $1 \cdot x = x$, for all $x \in G$. Since G is finite, it has a basis by Theorem A.7.10. If $\dim(G) \geq 2$, then the function that interchanges two basis elements is a nontrivial automorphism of G. We conclude that $\dim(G) = 1$, and so $|G| = 2$.

19. Let G be a group and let N be a normal subgroup of G of finite index. Suppose that H is a finite subgroup of G and that the order of H is relatively prime to the index of N in G. Prove that H is contained in N.

Solution: Let $\pi : G \to G/N$ be the natural projection. Then $\pi(H)$ is a subgroup of G/N, so its order must be a divisor of $|G/N|$. On the other hand, $|\pi(H)|$ must be a divisor of $|H|$. Since $\gcd(|H|, [G : N]) = 1$, we must have $|\pi(H)| = 1$, which implies that $H \subseteq \ker(\pi) = N$.

7.2. Conjugacy

9. Let G be a finite group with $[G : Z(G)] = n$. Show that the number of elements in each conjugacy class of G is a divisor of n.

Solution: By Proposition 7.2.5, the conjugacy class of $a \in G$ has $[G : C(a)]$ elements. Since $Z(G) \subseteq C(a) \subseteq G$, it follows from Lagrange's theorem that $|G| = [G : Z(G)] \cdot |Z(G)|$ and then

$$|G| = [G : C(a)] \cdot |C(a)| = [G : C(a)] \cdot [C(a) : Z(G)] \cdot |Z(G)| .$$

Therefore $n = [G : Z(G)] = [G : C(a)] \cdot [C(a) : Z(G)]$, completing the proof.

18. Let $\sigma \in A_n$, and let $C_{S_n}(\sigma)$ and $C_{A_n}(\sigma)$ denote the centralizers of σ in S_n and A_n, respectively.

(a) Show that either $C_{A_n}(\sigma) = C_{S_n}(\sigma)$ or $[C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2$.

Solution: By Exercise 5 of Section 3.8 we know that if H is any subgroup of S_n, then either $H \cap A_n = H$ or $H \cap A_n$ has index 2 in H. Since $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, either $C_{A_n}(\sigma) = C_{S_n}(\sigma)$ or else $C_{A_n}(\sigma)$ has index 2 in $C_{S_n}(\sigma)$.

(b) Show that the conjugacy class of σ in A_n is either the same as its conjugacy class in S_n or else has half as many elements.

Solution: Since $C_{A_n}(\sigma) \subseteq C_{S_n}(\sigma) \subseteq S_n$ and $C_{A_n}(\sigma) \subseteq A_n \subset S_n$, we have

$$[S_n : C_{S_n}(\sigma)][C_{S_n}(\sigma) : C_{A_n}(\sigma)] = [S_n : C_{A_n}(\sigma)] = [S_n : A_n][A_n : C_{A_n}(\sigma)] .$$

If $[C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2$ (the second case in part (a)), then dividing the above equation by 2 gives us $[A_n : C_{A_n}(\sigma)] = [S_n : C_{S_n}(\sigma)]$, and so σ has the same number of conjugates in A_n as in S_n.

If $C_{S_n}(\sigma) = C_{A_n}(\sigma)$ (the first case in part (a)), then $[S_n : C_{S_n}(\sigma)] = [S_n : C_{A_n}(\sigma)] = 2[A_n : C_{A_n}(\sigma)]$, and so σ has the half the number of conjugates in A_n as in S_n.

(c) Find the center of the alternating group A_n.

Solution: In the case $n = 3$, we have $Z(A_3) = A_3$ since A_3 is abelian. If $n \geq 4$, then we claim that $Z(A_n) = \{(1)\}$. This proof illustrates the use of conjugacy classes, but we note that Theorem 7.7.4, which shows that A_n is simple for $n \geq 5$, gives a much shorter proof for $n \geq 5$.

Since the conjugacy class of an element $\sigma \neq (1)$ in S_n consists of all permutations with a given cycle structure, it has more than 2 elements if $n \geq 4$, and therefore its conjugacy class in A_n has more than 1 element. Thus the identity (1) is the only element whose conjugacy class consists of exactly one element, which shows that the center is $\{(1)\}$.

22. Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and $|G|$ is odd. Prove that N is contained in the center of G.

Solution: Since $|N| = 5$, the subgroup N is cyclic, say $N = \langle a \rangle$. It suffices to show that $a \in Z(G)$, which is equivalent to showing that a has no conjugates other than itself. We first note that since N is normal in G, any conjugate of a must be in N. We next note that if x is conjugate to y, which we will write $x \sim y$, then $x^n \sim y^n$. Finally, we note that the number of conjugates of a must be a divisor of G.

Case 1. If $a \sim a^2$, then $a^2 \sim a^4$, and $a^4 \sim a^8 = a^3$.

Case 2. If $a \sim a^3$, then $a^3 \sim a^9 = a^4$, and $a^4 \sim a^{12} = a^2$.

Case 3. If $a \sim a^4$, then $a^2 \sim a^8 = a^3$.

In the first two cases a has 4 conjugates, which contradicts the assumption that G has odd order. In the last case, a has either 2 or 4 conjugates, which again leads to the same contradiction.

7.3. Groups Acting on Sets

2. Let H be a subgroup of G, and let S denote the set of left cosets of H. Define a group action of G on S by setting $a \cdot (xH) = axH$, for all $a, x \in G$.

(a) Let $\phi : G \to \mathrm{Sym}(S)$ be the homomorphism that corresponds to the group action defined above. Show that $\ker(\phi)$ is the largest normal subgroup of G that is contained in H.

Solution: For $a \in G$ we have $\phi(a) = \lambda_a$, where $\lambda_a : S \to S$ is given by $\lambda_a(xH) = a(xH)$. It is routine to check that λ_a is well-defined, one-to-one, and onto. Now

$$\begin{aligned} \ker(\phi) &= \{a \in G \mid \lambda_a(xH) = xH \text{ for all } x \in G\} \\ &= \{a \in G \mid axH = xH \text{ for all } x \in G\} \\ &= \{a \in G \mid x^{-1}ax \in H \text{ for all } x \in G\} \, . \end{aligned}$$

Clearly, $\ker(\phi) \subseteq H$ and $\ker(\phi)$ is a normal subgroup of G. Let N be a normal subgroup of G with $N \subseteq H$. Then for all $x \in G$, we have $x^{-1}Nx \subseteq N \subseteq H$, and so $N \subseteq \ker(\phi)$.

(b) Assume that G is finite and let $[G : H] = n$. Show that if $n!$ is not divisible by $|G|$, then H must contain a nontrivial normal subgroup of G.

Solution: Since $[G : H] = n$, we have $|S| = n$ and $|\mathrm{Sym}(S)| = n!$. If $|G| \not| n!$, then the homomorphism ϕ of part (a) is not one-to-one, and so $\ker(\phi) \neq \{e\}$. Hence $\ker(\phi)$ is a nontrivial normal subgroup of G, and $\ker(\phi) \subseteq H$.

3. Let G be a group which has a subgroup of index 6. Prove that G has a normal subgroup whose index is a divisor of 720.

Solution: Suppose that H is a subgroup with index 6. Letting G act by multiplication on the left cosets of H (as in Exercise 2) produces a homomorphism from G into S_6. The order of the image must be a divisor of $|S_6| = 720$, and so the index of the kernel is a divisor of 720.

4. Let G act on the subgroup H by conjugation, let S be the set of all conjugates of H, and let $\phi : G \to \mathrm{Sym}(S)$ be the corresponding homomorphism. Show that $\ker(\phi)$ is the intersection of the normalizers $N(aHa^{-1})$ of all conjugates of H.

Solution: We have $x \in \ker(\phi)$ iff $x(aHa^{-1})x^{-1} = aHa^{-1}$ for all $a \in G$.

10. Let $F = \mathrm{GF}(3)$, $G = \mathrm{GL}_2(F)$, and let N be the center of G. Prove that $G/N \cong S_4$ by defining an action of G on the four one-dimensional subspaces of F^2.

Solution: In F^2 there are 4 one-dimensional subspaces, with respective basis elements $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}$. Each matrix in G represents an isomorphism of F^2, and so it simply permutes these one-dimensional subspaces. Thus we can let S be the set of one-dimensional subspaces, and let G act on them as described above. Multiplying by a scalar leaves each one-dimensional subspace fixed, and the two scalar transformations $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, are the only linear transformations to do so. Thus the action of G defines a homomorphism into S_4 whose kernel is the set of scalar matrices, which is precisely the center N by Exercise 7 of Section 3.3. Since $|G| = 48$ by Exercise 5 of Section 3.3 and N consists of two scalar matrices, we have $|G/N| = 24$. It follows that the homomorphism must map G/N onto S_4, since $|S_4| = 4! = 24$, and thus $G/N \cong S_4$.

16. If G is a finite group of order n and p is the least prime such that $p|n$, show that any subgroup of index p is normal in G.

Solution: Let H be a subgroup of index p, and let $S = \{xH \mid x \in G\}$. Let $\phi : G \to \text{Sym}(S)$ be the homomorphism of Exercise 2 (a). If $n \mid p!$, then $p \mid n$ implies that $n = p$, in which case $H = \{e\}$. Thus we may assume that $n \nmid p!$, in which case $\ker(\phi)$ is a nontrivial normal subgroup of G that is contained in H, by Exercise 2 (b). If we let $k = [G : \ker(\phi)]$, then $k \mid p!$ and $k \mid n$. Since p is the smallest prime that divides n, we have $k = p$, and so $H = \ker(\phi)$ is a normal subgroup.

7.4. The Sylow Theorems

3. Prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G.

Solution: Suppose that N contains the Sylow p-subgroup P. Then since N is normal it also contains all of the conjugates of P. But this means that N contains all of the Sylow p-subgroups of G, since they are all conjugate by Theorem 7.4.4 (a). We conclude that N and G have the same number of Sylow p-subgroups.

4. Prove that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Solution: Since $105 = 3 \cdot 5 \cdot 7$, the number of Sylow 3-subgroups must be 1 or 7, the number of Sylow 5-subgroups must be 1 or 21, and the number of Sylow 7-subgroups must be 1 or 15. Let P be a Sylow 5-subgroup and let Q be a Sylow 7-subgroup. At least one of these subgroups must be normal, since otherwise we would have $21 \cdot 4$ elements of order 5 and $15 \cdot 6$ elements of order 7. Therefore PQ is a subgroup, and it must be normal since its index is the smallest prime divisor of

$|G|$. (See Exercise 16 of Section 7.3.) It follows that we can apply Exercise 3. Since PQ is normal and contains a Sylow 5-subgroup, we can reduce to the number 35 when considering the number of Sylow 5-subgroups, and thus the number of Sylow 5-subgroups of G is the same as the number of Sylow 5-subgroups of PQ, which is 1. Similarly, since PQ is normal and contains a Sylow 7-subgroup, the number of Sylow 7-subgroups of G is the same as the number of Sylow 7-subgroups of PQ, which is 1.

9. Let p be a prime number. Find all Sylow p-subgroups of the symmetric group S_p.

Solution: Since $|S_p| = p!$, and p is a prime number, the highest power of p that divides $|S_p|$ is p. Therefore the Sylow p-subgroups are precisely the cyclic subgroups of order p, each generated by a p-cycle. There are $(p-1)! = p!/p$ ways to construct a p-cycle $(a_1, \ldots, a_p)$. The subgroup generated by a given p-cycle will contain the identity and the $p-1$ powers of the cycle. Two different such subgroups intersect in the identity, since they are of prime order, so the total number of subgroups of order p in S_p is $(p-2)! = (p-1)!/(p-1)$.

16. Find the normalizer of $\langle(1,2,3,4,5)\rangle$ in A_5 and in S_5.

Solution: Let $\langle(1,2,3,4,5)\rangle = H$. Note that H is a Sylow 5-subgroup of S_5, that S_5 had 6 Sylow 5-subgroups by Exercise 9, and that A_5 also has 6 Sylow 5-subgroups by Exercise 3.

First consider $H = \langle(1,2,3,4,5)\rangle$ as a subgroup of A_5. Since there are 6 subgroups conjugate to H, it follows from Theorem 7.3.4 (b) that $[A_5 : N(H)] = 6$, and so $|N(H)| = 10$. Letting $\sigma = (1,2,3,4,5)$, a solution τ of the equation $\tau\sigma\tau^{-1} = \sigma^{-1}$ certainly belongs to $N(H)$, since $\tau\sigma^i\tau^{-1} = \sigma^{-i}$ for $i = 1,2,3,4$. As in Exercise 15 (b) of Section 2.3, we can solve to obtain $\tau = (2,5)(3,4)$, and note that $\tau \in A_5$. Since $|N(H)| = 10$, we must have $N(H) = \langle\sigma, \tau\rangle$.

Now consider H as a subgroup of S_5. Arguing as above on the number of Sylow 5-subgroups, we have $[S_5 : N(H)] = 6$, and so in this case $|N(H)| = 20$. To look for an element in $N(H)$, consider $\nu = (2,3,5,4)$, since $(2,3,5,4)^2 = (2,5)(3,4)$. We have $(2,3,5,4)(1,2,3,4,5)(2,3,5,4)^{-1} = (1,3,5,2,4) = \sigma^2$, and so, as before, $\nu \in N(H)$. Since $o(\nu) = 4$, we see that $\langle\sigma, \nu\rangle = N(H)$.

Note: Given the relation $\tau\sigma = \sigma^{-1}\tau$, it follows that the normalizer of H in A_5 is isomorphic to D_5. Similarly, given the relation $\nu\sigma = \sigma^2\nu$, it follows from Exercise 17 (a) of Section 7.1 that the normalizer of H in S_5 is isomorphic to F_{20}. (This is also shown directly in Exercise 21 of Section 7.2.)

20. Let G be a group of order 340. Prove that G has a normal cyclic subgroup of order 85 and an abelian subgroup of order 4.

Solution: First, $340 = 2^2 \cdot 5 \cdot 17$. There exists a Sylow 2-subgroup of order 4, and it must be abelian. No nontrivial divisor of $68 = 2^2 \cdot 17$ is congruent to 1 mod 5,

so the Sylow 5-subgroup is normal. Similarly, the Sylow 17-subgroup is normal. These subgroups have trivial intersection, so their product is a direct product, and hence must be cyclic of order $85 = 5 \cdot 17$. The product of two normal subgroups is again normal, so this produces the required normal cyclic subgroup of order 85.

21. Show that a group of order 108 has a normal subgroup of order 9 or 27.

Solution: Let S be a Sylow 3-subgroup of G. Then $[G : S] = 4$, since $|G| = 2^2 3^3$, so we can let G act by multiplication on the cosets of S. This defines a homomorphism $\phi : G \to S_4$, so it follows that $|\phi(G)|$ is a divisor of 12, since it must be a common divisor of 108 and 24. Thus $|\ker(\phi)| \geq 9$, and it follows from Exercise 2 (a) of Section 7.3 that $\ker(\phi) \subseteq S$. Thus $|\ker(\phi)|$ must be a divisor of 27, and so either $|\ker(\phi)| = 9$ or $|\ker(\phi)| = 27$.

7.5. Finite Abelian Groups

4. Let G be an abelian group, written additively, which has 8 elements of order 3, 18 elements of order 9, and no other elements besides the identity. Find (with proof) the decomposition of G as a direct sum of cyclic groups.

Solution: We have $|G| = 27$. First, G is not cyclic since there is no element of order 27. Since there are elements of order 9, G must have $\mathbf{Z}_9$ as a factor. To give a total of 27 elements, the only possibility is $G \cong \mathbf{Z}_9 \oplus \mathbf{Z}_3$.
Check: The elements 3 and 6 have order 3 in $\mathbf{Z}_9$, while 1 and 2 have order 3 in $\mathbf{Z}_3$. Thus the following 8 elements have order 3 in the direct product: $(3, 0)$, $(6, 0)$, $(3, 1)$, $(6, 1)$, $(3, 2)$, $(6, 2)$, $(0, 1)$, and $(0, 2)$.

10. Let G and H be finite abelian groups, and assume that they have the following property. For each positive integer m, G and H have the same number of elements of order m. Prove that G and H are isomorphic.

Solution: We first reduce the case to that of p-groups. Let p be a prime divisor of $|G|$, and let G_p and H_p be the Sylow p-subgroups of G and H, respectively. If we can show that $G_p \cong H_p$ for all p, then it will follow that $G \cong H$, since G and H are direct products of their Sylow subgroups.

Let $|G| = p^k$ for $k \in \mathbf{Z}^+$ and suppose that $G \cong \mathbf{Z}_{p^{\alpha_1}} \oplus \mathbf{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{\alpha_t}}$, where $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_t$ and $\sum_{i=1}^{t} \alpha_i = k$. Consider the number of elements of order p in G. There are $p - 1$ such elements in $\mathbf{Z}_{p^\alpha}$; in G the elements of order p have the form $(a_1, \ldots, a_t)$, where $a_i = 0$ or has order p, and at least one a_i is nonzero. Thus there are $p^t - 1$ elements of order p in G.

Suppose that $H \cong \mathbf{Z}_{p^{\beta_1}} \oplus \mathbf{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{\beta_s}}$, where $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_s$ and $\sum_{i=1}^{t} \beta_i = k$. There are $p^s - 1$ elements of order p in H, and therefore $s = t$.

Now consider pG, in which each element of order p^j in G becomes an element of order p^{j-1}. Then pG and pH have the same number of elements of each

order, so by induction on the order of the groups we must have $pG \cong pH$. Since $p\mathbf{Z}_{p^\alpha} \cong \mathbf{Z}_{p^{\alpha-1}}$, we have $pG \cong \mathbf{Z}_{p^{\alpha_1-1}} \oplus \mathbf{Z}_{p^{\alpha_2-1}} \oplus \cdots \oplus \mathbf{Z}_{p^{\alpha_t-1}}$, and $pH \cong \mathbf{Z}_{p^{\beta_1-1}} \oplus \mathbf{Z}_{p^{\beta_2-1}} \oplus \cdots \oplus \mathbf{Z}_{p^{\beta_t-1}}$. Therefore $pG \cong pH$ implies $\alpha_1 - 1 = \beta_1 - 1$, $\alpha_2 - 1 = \beta_2 - 1, \ldots, \alpha_t - 1 = \beta_t - 1$, so $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_t = \beta_t$, and therefore $G \cong H$.

13. Let G and H be finite abelian groups, written additively, and assume that $G \oplus G$ is isomorphic to $H \oplus H$. Prove that G is isomorphic to H.

Solution: Let p be a prime divisor of $|G|$, and let $q = p^\alpha$ be the order of a cyclic component of G. If G has k such components, then $G \oplus G$ has $2k$ components of order q. An isomorphism between $G \oplus G$ and $H \oplus H$ must preserve these components, so it follows that H also has k cyclic components of order q. Since this is true for every such q, Theorem 7.5.6 gives identical decompositions for G and H. It follows that $G \cong H$.

7.6. Solvable Groups

2. **(a)** Find the commutator subgroup D_n' of D_n

Solution: Using the standard description of D_n via generators and relations, consider the cases $x = a^i$ or $x = a^i b$ and $y = a^j$ or $y = a^j b$.

Case 1: If $x = a^i$ and $y = a^j$, the commutator is trivial.

Case 2: If $x = a^i$ and $y = a^j b$, then $xyx^{-1}y^{-1} = a^i a^j b a^{-i} a^j b = a^i a^j a^i b a^j b = a^i a^j a^i a^{-j} b^2 = a^{2i}$, and thus each even power of a is a commutator.

Case 3: If $x = a^j b$ and $y = a^i$, we get the inverse of the element in Case 2.

Case 4: If $x = a^i b$ and $y = a^j b$, then $xyx^{-1}y^{-1} = a^i b a^j b a^i b a^j b$, and so we get $xyx^{-1}y^{-1} = a^i a^{-j} b^2 a^i a^{-j} b^2 = a^{2(i-j)}$, and again we get even powers of a.

This gives the result we are looking for. If n is odd, then the commutators form the subgroup $\langle a \rangle$. If n is even, then the commutators form the subgroup $\langle a^2 \rangle$.

(b) Prove that the dihedral group D_n is solvable for all n.

Solution: By part (a) the commutator subgroup D_n' is either $\langle a \rangle$ or $\langle a^2 \rangle$. In either case, the commutator subgroup is abelian, so $D_n'' = \langle 1 \rangle$, showing that D_n is solvable.

7. Example 7.6.3 constructed a composition series $S_4 \supset N_1 \supset N_2 \supset N_3 \supset \langle 1 \rangle$ for S_4 in which $N_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Show that although S_4 has subgroups isomorphic to $\mathbf{Z}_4$, there is no composition series for S_4 in which $N_2 \cong \mathbf{Z}_4$.

Solution: Any subgroup H of S_4 that is isomorphic to $\mathbf{Z}_4$ must be generated by a 4-cycle (a, b, c, d). By Exercise 15 (b) of Section 2.3 there exists $\sigma \in S_4$ with

$\sigma(1,2,3,4)\sigma^{-1} = (a,b,c,d)$. That is, there exists an inner automorphism of S_4 that maps $(1,2,3,4)$ to (a,b,c,d). Since any isomorphism will map one composition series to another, this shows that to answer the question it suffices to show that the second term in the composition series cannot be $\langle(1,2,3,4)\rangle$.

Suppose that we have a composition series $S_4 \supset K_1 \supset K_2 \supset K_3 \supset \langle 1\rangle$ in which $K_2 = \langle(1,2,3,4)\rangle$. Then K_2 is a normal subgroup of K_1, so this means we should compute the normalizer $N(K_2)$. We know that K_2 is normal in the subgroup D generated by $(1,2,3,4)$ and $(2,4)$, since $D \cong D_4$ (see Table 3.6.1). We could also show that K_2 is a normal subgroup of D by observing that fact K_2 has index 2 in D.

Now $K_2 \subset D \subseteq N(K_2) \subseteq S_4$, and since D has index 3 in S_4, it follows that either $D = N(K_2)$ or $N(K_2) = S_4$. Because $(1,2)(1,2,3,4)(1,2) = (1,3,4,2) \notin K_2$, it follows that K_2 is not a normal subgroup of S_4, and so $D = N(K_2)$. This forces $K_1 = D$ in our supposed composition series, which is impossible since D is not a normal subgroup of S_4. (In the above calculation, $(1,2)(1,2,3,4)(1,2) = (1,3,4,2) \notin D$.)

10. Let p and q be primes, not necessarily distinct.

(a) Show that any group of order pq is solvable.

Solution: If $p = q$, then G has order p^2 and is thus abelian. Hence G is solvable. If $p < q$, then the number of Sylow q-subgroups divides p and is congruent to 1 modulo q. Thus there is only one Sylow q-subgroup H of G, and so it must be normal in G. The subgroup H is simple since $|H| = q$, and G/H is also simple since $|G/H| = p$. The sequence $G \supset H \supset \{e\}$ shows that G is solvable.

(b) Show that any group of order p^2q is solvable.

Solution: If $p = q$, then there exists a subgroup H of G with $|H| = p^2$ and a subgroup K of H such that $|K| = p$. The sequence $G \supset H \supset K \supset \{e\}$ shows that G is solvable.

If $p \neq q$, then we claim that one of the Sylow p-subgroups or Sylow q-subgroups is normal. If there is more than one Sylow p-subgroup, then there are q Sylow p-subgroups, and $p \,|\, (q-1)$. If there is more than one Sylow q-subgroup, then there are p or p^2 Sylow q-subgroups and $q \,|\, (p-1)$ or $q \,|\, (p^2-1)$. Since $p \,|\, (q-1)$ implies $p \leq q-1$, we cannot have $q \,|\, (p-1)$. Thus there cannot be p Sylow q-subgroups and q Sylow p-subgroups. Since $p \,|\, (q-1)$ we have $p \leq q-1$, and since $q \,|\, (p+1)(p-1)$, we must have $q = p+1$. We conclude that $p = 2$ and $q = 3$, and our group is of order 12. The number of Sylow 3-subgroups of a group of order 12 is 1 or 4. If there are 4 Sylow 3-subgroups, then since any two of these Sylow 3-subgroups must intersect in the identity element, there are $4 \cdot (3-1) = 8$ elements of order 3. The remaining 4 elements form the unique Sylow 2-subgroup, and so the Sylow 2-subgroup is normal.

Now consider the sequence $G \supset H \supset \{e\}$, where H is the normal Sylow subgroup. Then G/H either has order p^2 or order q. In either case G/H is abelian, and so G is solvable since both G/H and H are solvable.

(c) Show that any group of order $p^n q$ is solvable if $p > q$.

Solution: Let G have order $p^n q$, with $p > q$. Since $p > q$ there is only one Sylow p-subgroup H of G, which must be normal in G. Since $|G/H| = q$, it is certainly true that G/H is solvable. Since H is a p-group, it is also solvable, and thus G is solvable.

12. Prove that any group of order 588 is solvable.

Solution: We have $588 = 2^2 \cdot 3 \cdot 7^2$. Let S be the Sylow 7-subgroup. It must be normal, since 1 is the only divisor of 12 that is $\equiv 1 \pmod 7$. Since $|G/S| = 12$, it is solvable by Exercise 10 (b). Furthermore, S is solvable since it is a p-group. Since both S and G/S are solvable, it follows from Corollary 7.6.8 (b) that G is solvable.

14. Let G be a finite group and suppose that N is a normal subgroup of G for which $\gcd(|N|, [G : N]) = 1$. Prove that N is a characteristic subgroup of G.

Solution: Let ϕ be any automorphism of G. Then $\phi(N)$ is a subgroup of G, with $|N|$ elements. Since $\gcd(|N|, [G : N]) = 1$, we can apply the result in the Exercise 19 of Section 7.1, which implies that $\phi(N) \subseteq N$.

7.7. Simple Groups

11. Show that there is no simple group of order 132.

Solution: Since $132 = 2^2 \cdot 3 \cdot 11$, the number of Sylow 2-subgroups is 1, 3, 11, or 33; the number of Sylow 3-subgroups is 1, 4, or 22; and the number of Sylow 11-subgroups is 1 or 12. We will focus on the Sylow 3 and 11 subgroups. If there are 4 Sylow 3-subgroups, then as in Exercise 10, we can let the group act on them to produce a homomorphism into S_4. Because 132 is not a divisor of $24 = |S_4|$, this cannot be one-to-one and therefore has a nontrivial kernel. If there are 22 Sylow 3-subgroups and 12 Sylow 11-subgroups, we get too many elements: 44 of order 3 and 120 of order 11. Thus the group has either 1 Sylow 3-subgroup or 1 Sylow 11-subgroup. We conclude that a group of order 132 has a proper nontrivial normal subgroup.

17. Let F be a finite field, with $|F| = p$ (a prime number), and let P be the subgroup of $\mathrm{GL}_n(F)$ consisting of all upper triangular matrices with 1 in each entry along the main diagonal. Show that P is a Sylow p-subgroup of $\mathrm{GL}_n(F)$.

Solution: The answer to Exercise 15 gives us

$$|\,\mathrm{GL}_n(F)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})\,,$$

which can be rewritten as

$$(p^n - 1)p(p^{n-1} - 1)\cdots p^{n-1}(p - 1) = p^{1+\cdots+(n-1)}m = p^{n(n-1)/2}m\,,$$

where $p \nmid m$ since $p \nmid (p^i - 1)$ for $i = 1, \ldots, n$.

To construct a matrix in P, we have 1 choice in the first column, p choices in the second, etc., with p^{n-1} choices in the last column. Thus $|P| = p^{n(n-1)/2}$, and so P is a maximal p-subgroup of $\mathrm{GL}_n(F)$, and is therefore a Sylow p-subgroup of $\mathrm{GL}_n(F)$.

20. Let F be any field, and let G be the set of all rational functions over F of the form $f(x) = \dfrac{ax + b}{cx + d}$, where $a, b, c, d \in F$ and $ad - bc = 1$. Prove that G is a group under composition of functions, and that G is isomorphic to $\mathrm{PSL}_2(F)$.

Solution: Define $\phi : \mathrm{SL}_2(F) \to G$ by setting $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = f(x) = \dfrac{ax + b}{cx + d}$, for each matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(F)$. Of course $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$ in $\mathrm{SL}_2(F)$. In G the operation is given as composition of functions, and so if we let $f_i(x) = \dfrac{a_ix + b_i}{c_ix + d_i}$, then we have the following calculation, which shows that ϕ respects the given operations.

$$\begin{aligned}(f_1 \circ f_2)(x) \;=\; f_1(f_2(x)) \;&=\; \frac{a_1\left(\dfrac{a_2x + b_2}{c_2x + d_2}\right) + b_1}{c_1\left(\dfrac{a_2x + b_2}{c_2x + d_2}\right) + d_1} \\ &=\; \frac{a_1\,(a_2x + b_2) + b_1\,(c_2x + d_2)}{c_1\,(a_2x + b_2) + d_1\,(c_2x + d_2)} \\ &=\; \frac{(a_1a_2 + b_1c_2)\,x + a_1b_2 + b_1d_2}{(c_1a_2 + d_1c_2)\,x + c_1b_2 + d_1d_2}\end{aligned}$$

It is clear that ϕ is onto. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \ker(\phi)$. Then $\phi(A)$ is the rational function $f(x) = \dfrac{ax + b}{cx + d}$, which is the identity function x if and only

if $a = d$ and $b = c = 0$. It follows from Exercise 7 of Section 3.3 that $A \in Z(\mathrm{GL}_2(F))$. The proof of that exercise uses the centralizers of two matrices in $\mathrm{SL}_n(F)$, so in fact $A \in Z(\mathrm{SL}_2(F))$, and therefore $\ker(\phi) = Z(\mathrm{SL}_2(F))$. We conclude that G is a group isomorphic to $\mathrm{PSL}_2(F)$.

8 Galois Theory

8.1. The Galois Group of a Polynomial

8. For each of the following fields, find the Galois group of $x^3 - 2$ over the field.

(a) GF(5)

Solution: A search in GF(5) for roots of $x^3 - 2$ yields one and only one: $x = -2$. Thus $x^3 - 2$ factors as $x^3 - 2 = (x + 2)(x^2 - 2x - 1)$. The irreducible quadratic factor will have a splitting field of degree 2 over GF(5), so by Theorem 8.1.8 the Galois group of $x^3 - 2$ over GF(5) is cyclic of order 2.

(b) GF(7)

Solution: In this case, $x^3 - 2$ has no roots in GF(7), so it is irreducible. If we adjoin a root α of $x^3 - 2$ to GF(7), it follows from Corollary 6.6.2 that GF(7)(α) is the splitting field of $x^3 - 2$ over GF(7). Since the splitting field has degree 3 over GF(7), it follows from Theorem 8.1.8 that the Galois group of the polynomial is cyclic of order 3.

Comment: To show directly that we have found the correct splitting field, division of $x^3 - 2$ by $x - \alpha$ shows that $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$. The quadratic formula then shows that 2α and 4α are the roots of $x^2 + \alpha x + \alpha^2$, and so $x^3 - 2$ splits over GF(7)(α) as $x^3 - 2 = (x - \alpha)(x - 2\alpha)(x - 4\alpha)$.

(c) GF(11)

Solution: A search in GF(11) for roots of $x^3 - 2$ yields one and only one: $x = 7$. Then $x^3 - 2$ can be factored as $x^3 - 2 = (x - 7)(x^2 + 7x + 5)$, and the second factor must be irreducible. The splitting field has degree 2 over GF(11), and can be described as GF(11)$[x]/\langle x^2 + 7x + 5\rangle$. Thus by Theorem 8.1.8 the Galois group of $x^3 - 2$ over GF(11) is cyclic of order 2, as in part (a).

9. Find the Galois group of $x^4 - 1$ over the field GF(7).

Solution: We first need to find the splitting field of $x^4 - 1$ over GF(7). We have $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$. A quick check of ± 2 and ± 3 shows that they are not roots of $x^2 + 1$ over GF(7), so $x^2 + 1$ is irreducible over GF(7). To obtain the splitting field we must adjoin a root of $x^2 + 1$, so we get a splitting field GF(7)$[x]/\langle x^2 + 1\rangle$ of degree 2 over GF(7).

It follows from Theorem 8.1.8 that the Galois group of $x^4 - 1$ over GF(7) is cyclic of order 2.

8.2. Multiplicity of Roots

4. Find the Galois group of $x^6 - 1$ over GF(7).

Solution: The Galois group is trivial because $x^6 - 1$ already splits over GF(7). In fact, $x^6 - 1 = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$.

Comment: By Theorem 6.5.2, GF(7) is the splitting field of $x^7 - x = x(x^6 - 1)$.

8. Find a primitive element for the extension $\mathbf{Q}(\sqrt{2}, i)$ over $\mathbf{Q}$.

Solution: The solution of Exercise 2 (c) of Section 6.4 shows that $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha)$ for $\alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$.

Alternate solution: If we follow the proof of Theorem 8.2.8, we have $u = u_1 = \sqrt{2}$, $u_2 = -\sqrt{2}$, $v = v_1 = i$, and $v_2 = -i$. The proof shows the existence of an element a with $u + av \neq u_i + av_j$ for all i and all $j \neq 1$. To find such an element we need $\sqrt{2} + ai \neq \sqrt{2} + a(-i)$ and $\sqrt{2} + ai \neq -\sqrt{2} + a(-i)$. The easiest solution is to take $a = 1$, and so we consider the element $\alpha = \sqrt{2} + i$. We have $\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\sqrt{2}, i)$, and since $\alpha^{-1} \in \mathbf{Q}(\alpha)$, we must have $(\sqrt{2} + i)^{-1} = (\sqrt{2} - i)/3 \in \mathbf{Q}(\alpha)$. But then $\sqrt{2} - i$ belongs, and it follows immediately that $\sqrt{2}$ and i both belong to $\mathbf{Q}(\alpha)$, which gives us the desired equality $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, i)$.

10. Let $f(x) \in \mathbf{Q}[x]$ be irreducible over $\mathbf{Q}$, and let F be the splitting field of $f(x)$ in $\mathbf{C}$. If $[F : \mathbf{Q}]$ is odd, prove that all of the roots of $f(x)$ are real.

Solution: We can assume without loss of generality that $f(x)$ is monic, so let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$, where $a_i \in \mathbf{Q}$ for $0 \leq i < n$. Define $\phi : F \to \mathbf{C}$ by setting $\phi(z) = \overline{z}$, for all $z \in F$, where $\overline{z}$ denotes the complex conjugate of z. For $z_1, z_2 \in F$ we have $\phi(z_1 + z_2) = \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} = \phi(z_1) + \phi(z_2)$ and $\phi(z_1 z_2) = \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} = \phi(z_1)\phi(z_2)$, so ϕ is a ring homomorphism since $\phi(1) = 1$. Since $\ker(\phi)$ is a proper ideal of the field F it must be (0), and thus ϕ is one-to-one.

Since $f(x)$ has real coefficients, we have $\phi(a_i) = a_i$ for $0 \leq i < n$. If r is a root of $f(x)$, then $f(\overline{r}) = \phi(f(r)) = \phi(0) = 0$, so $\overline{r}$ is also a root of $f(x)$. Since F is the splitting field for $f(x)$, it is the smallest subfield of $\mathbf{C}$ that contains all roots of $f(x)$. We conclude that $\phi(F) = F$, and so $\phi \in \mathrm{Gal}(F/\mathbf{Q})$.

Since $\mathbf{Q}$ has characteristic zero, Theorem 8.2.6 implies that $f(x)$ has no repeated roots, and then Theorem 8.1.6 shows that $|\mathrm{Gal}(F/\mathbf{Q})| = [F : Q]$, so $\mathrm{Gal}(F/\mathbf{Q})$ has odd order. Since $|\mathrm{Gal}(F/\mathbf{Q})|$ is odd and $\phi^2 = 1_F$, it follows that ϕ must be the identity mapping. We conclude that $F \subseteq \mathbf{R}$, and so every root of $f(x)$ must be real.

8.3. The Fundamental Theorem of Galois Theory

4. Let $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$. Find $[F : \mathbf{Q}]$ and prove that F is not normal over $\mathbf{Q}$.

Solution: The element $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbf{Q}$. Since $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbf{Q}$, we see that $\mathbf{Q}(\sqrt{2})$ cannot be contained in $\mathbf{Q}(\sqrt[3]{2})$ since the first extension has degree 2 over $\mathbf{Q}$ while the second has degree 3 over $\mathbf{Q}$. It follows that $[F : \mathbf{Q}] = 6$.

If F were a normal extension of $\mathbf{Q}$, then since it contains one root $\sqrt[3]{2}$ of the irreducible polynomial $x^3 - 2$ it would have to contain all of the roots. But $F \subseteq \mathbf{R}$, while the other two roots of $x^3 - 2$ are non-real, so F cannot be a normal extension of $\mathbf{Q}$.

7. Find the order of the Galois group of $x^5 - 2$ over $\mathbf{Q}$.

Solution: Let G be the Galois group in question, and let ζ be a primitive 5th root of unity. Then the roots of $x^5 - 2$ are $\alpha = \sqrt[5]{2}$ and $\alpha\zeta^j$, for $1 \leq j \leq 4$. The splitting field over $\mathbf{Q}$ is $F = \mathbf{Q}(\sqrt[5]{2}, \zeta)$. Since $p(x) = x^5 - 2$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion, it is the minimal polynomial of $\sqrt[5]{2}$. The element ζ is a root of $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$, so its minimal polynomial is $q(x) = x^4 + x^3 + x^2 + x + 1$. Thus $[F : \mathbf{Q}] \leq 20$, but since the degree must be divisible by 5 and 4, it follows that $[F : \mathbf{Q}] = 20$, and therefore $|G| = 20$.

Note: By Section 8.6 we will have the tools to actually compute the Galois group, which is shown in Example 8.6.2 to be F_{20}.

9. Let F be the splitting field over K of a separable polynomial. Prove that if $\mathrm{Gal}(F/K)$ is cyclic, then for each divisor d of $[F : K]$ there is exactly one field E with $K \subseteq E \subseteq F$ and $[E : K] = d$.

Solution: By assumption we are in the situation of the fundamental theorem of Galois theory, so that there is a one-to-one order-reversing correspondence between subfields of F that contain K and subgroups of $G = \mathrm{Gal}(F/K)$. Because G is cyclic of order $[F : K]$, there is a one-to-one correspondence between subgroups of G and divisors of $[F : K]$. Thus for each divisor d of $[F : K]$ there is a unique subgroup H of *index* d. By the fundamental theorem, $[F^H : K] = [G : H]$, and so $E = F^H$ is the unique subfield with $[E : K] = d$.

8.4. Solvability by Radicals

1. Let $f(x)$ be irreducible over $\mathbf{Q}$, and let F be its splitting field over $\mathbf{Q}$. Show that if $\mathrm{Gal}(F/\mathbf{Q})$ is abelian, then $F = \mathbf{Q}(u)$ for all roots u of $f(x)$.

Solution: Since F has characteristic zero, we are in the situation of the fundamental theorem of Galois theory. Because $\mathrm{Gal}(F/\mathbf{Q})$ is abelian, every intermediate extension between $\mathbf{Q}$ and F must be normal. Therefore if we adjoin any root u of $f(x)$, the extension $\mathbf{Q}(u)$ must contain all other roots of $f(x)$, since it is irreducible over $\mathbf{Q}$. Thus $\mathbf{Q}(u)$ is a splitting field for $f(x)$, so $\mathbf{Q}(u) = F$.

2. Show that $x^5 - 4x + 2$ is irreducible over $\mathbf{Q}$, and is not solvable by radicals.

Solution: The polynomial $p(x) = x^5 - 4x + 2$ is irreducible over $\mathbf{Q}$, since it satisfies Eisenstein's criterion for the prime 2. Since $p(-2) = -22$, $p(-1) = 5$, $p(0) = 2$ $p(1) = -1$, and $p(2) = 26$, we see that $p(x)$ has a real root between -2 and -1, another between 0 and 1, and a third between 1 and 2. The derivative $p'(x) = 5x^4 - 4$ has two real roots, so $p(x)$ has one relative maximum and one relative minimum, and thus it must have exactly three real roots. It follows as in the proof of Theorem 8.4.8 that the Galois group of $p(x)$ over $\mathbf{Q}$ is S_5, and so it is not solvable.

8. Show that $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbf{Q}$, and use it to find the Galois group of $x^{10} - 1$ over $\mathbf{Q}$.

Solution: We can construct the splitting field F of $x^{10} - 1$ over $\mathbf{Q}$ by adjoining a primitive 10th root of unity to $\mathbf{Q}$. We have $x^{10} - 1 = (x^5 - 1)(x^5 + 1) = (x-1)(x^4 + x^3 + x^2 + x + 1)(x + 1)(x^4 - x^3 + x^2 - x + 1)$. Substituting $x - 1$ in the last factor yields $(x-1)^4 - (x-1)^3 + (x-1)^2 - (x-1) + 1 = (x^4 - 4x^3 + 6x^2 - 4x + 1) - (x^3 - 3x^2 + 3x - 1) + (x^2 - 2x + 1) - (x - 1) + 1 = x^4 - 5x^3 + 10x^2 - 10x + 5$. This polynomial satisfies Eisenstein's criterion for the prime 5, which implies that the factor $x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbf{Q}$.

The roots of this factor are the primitive 10th roots of unity, so it follows that $[F : \mathbf{Q}] = \varphi(10) = 4$. The proof of Theorem 8.4.2 shows that $\mathrm{Gal}(F/\mathbf{Q}) \cong \mathbf{Z}_{10}^{\times}$, and so the Galois group is cyclic of order 4.

8.5. Cyclotomic Polynomials

12. Calculate $\Phi_{105}(x)$.

Solution: We first note that $\varphi(105) = 48$. Since $\Phi_{105}(x) = \prod_{n|105}(x^n - 1)^{\mu(105/n)}$ by Exercise 9, we have $\Phi_{105}(x) = \dfrac{(x^3-1)(x^5-1)(x^7-1)(x^{105}-1)}{(x-1)(x^{15}-1)(x^{21}-1)(x^{35}-1)}$. By Exercise 11, because of the symmetry involved and the fact that $\deg(\Phi_{105}(x)) = 48$, we only need to compute the first 24 coefficients of $\Phi_{105}(x)$, so we can work with powers of x modulo x^{25}.

Note that $(x^{15}-1)(x^{15}+1) \equiv -1 \pmod{x^{25}}$, $(x^{21}-1)(x^{21}+1) \equiv -1 \pmod{x^{25}}$, $x^{35}-1 \equiv -1 \pmod{x^{25}}$, and $x^{105}-1 \equiv -1 \pmod{x^{25}}$, Thus after making these substitutions in our formula for $\Phi_{105}(x)$, we have

$$\begin{aligned}\Phi_{105}(x) &\equiv (x^2+x+1)(x^5-1)(x^7-1)(x^{15}+1)(x^{21}+1) \pmod{x^{25}} \\ &\equiv (1+x+x^2)(1-x^5-x^7+x^{12}+x^{15}-x^{20}+x^{21}-x^{22}) \pmod{x^{25}} \\ &\equiv (1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}+x^{13}+x^{14} \\ &\qquad +x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}-x^{24}) \pmod{x^{25}},\end{aligned}$$

and so we finally obtain $\Phi_{105}(x) =$
$x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}-x^{28}-x^{26}$
$-x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^9-x^8-2x^7-x^6-x^5+x^2+x+1$.

Remark: All of the polynomials $\Phi_n(x)$ that we have computed up to now have only the coefficients 0, 1, or -1, and so one might have conjectured that this was the case for all $\Phi_n(x)$. However $\Phi_{105}(x)$ has the coefficient -2 for the degree 7 and degree 41 terms.

8.6. Computing Galois Groups

5. Show that the following is a complete list of the transitive subgroups of S_4: (i) S_4; (ii) A_4; (iii) the Sylow 2-subgroups (isomorphic to D_4); (iv) the cyclic subgroups of order 4; (v) the subgroup $V = \{(1), (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\}$.

Solution: Let H be a subgroup of S_4 that acts transitively on $S = \{1,2,3,4\}$. This is equivalent to saying that the orbit of each $x \in S$, under the action of H, must be all of S, and so $[H : H_x] = |Hx| = |S| = 4$ for all $x \in S$. Therefore $|H|$ is divisible by 4, so we can only have $|H| = 24$, 12, 8, or 4.

It is clear that the subgroups listed in (i), (ii), (iv), and (v) are transitive. The only subgroup of order 12 is A_4, and any subgroup of order 8 is, of course, a Sylow 2-subgroup. We know that D_4 is isomorphic to a subgroup of S_4, so it follows from the Sylow theorems that every subgroup of order 8 is isomorphic to D_4 and therefore is transitive since it contains a 4-cycle.

We must now eliminate the subgroups of order 4 that are not on our list. Any subgroup of order 4 is contained in a Sylow 2-subgroup, so we only need to consider subgroups isomorphic to a subgroup of D_4. The three subgroups of D_4 of order 4 are given in Example 3.6.5. Letting $a = (1,2,3,4)$ and $b = (2,4)$, these subgroups are $H_1 = \{e, a^2, b, a^2b\} = \{(1), (1,3)(2,4), (2,4), (1,3)\}$, $H_2 = \langle a \rangle$, and $H_3 = \{e, a^2, ab, a^3b\} = V$. Since H_2 is cyclic and $H_3 = V$, these are on our list. Since H_1 is not transitive, it follows that any subgroup of S_4 isomorphic to H_1 is not transitive.

Thus our list of transitive subgroups of S_4 is complete.

8. Show that the following is a complete list of the transitive subgroups of S_5: (i) S_5; (ii) A_5; (iii) any cyclic subgroup of order 5; (iv) the normalizer in A_5 of any cyclic subgroup of order 5 (isomorphic to the dihedral group D_5); (v) the normalizer in S_5 of any cyclic subgroup of order 5 (isomorphic to the Frobenius group F_{20}).

Solution: Let H be a subgroup of S_5 that acts transitively on $S = \{1, 2, 3, 4, 5\}$. This is equivalent to saying that the orbit of each $x \in S$, under the action of H, must be all of S, and so $[H : H_x] = |Hx| = |S| = 5$ for all $x \in S$. Therefore $|H|$ is divisible by 5, and so H contains a cycle of length 5 by Cauchy's theorem. This cycle generates a Sylow 5-subgroup of H. By the Sylow theorems, the number of Sylow 5-subgroups in H is $\equiv 1 \pmod 5$, so this number must be either 6 or 1. We consider these two cases.

Case 1. Suppose that H contains 6 Sylow 5-subgroups. Then H contains all 24 cycles of length 5, and so $|H \cap A_5| \geq 25$. Since A_5 is simple it cannot contain a subgroup of order 30, so in this case $H \cap A_5 = A_5$, and thus either $H = A_5$ or $H = S_5$.

Case 2. Suppose that H contains only 1 Sylow 5-subgroup P, which is then normal in H. If $H \subseteq A_5$, then H contained in the normalizer of P in A_5, which is shown in Exercise 16 of Section 7.4 to be isomorphic to D_5. (Remember that P is generated by a 5-cyclic.) Therefore $H \cong Z_5$ or $H \cong D_5$.

If H is not contained in A_5, then H must be contained in the normalizer of P in S_5. As shown in Exercise 16 of Section 7.4, this normalizer is isomorphic to F_{20}. The only possibility for a subgroup of F_{20} isomorphic to H is one of the subgroups isomorphic to $\mathbf{Z}_5$, D_5, or F_{20} itself.

Thus our list of transitive subgroups of S_5 is complete.

9 UNIQUE FACTORIZATION

9.1. Unique Factorization

11. Show that $\mathbf{Z}[x]$ is not a principal ideal domain.

Solution: The factor ring $\mathbf{Z}[x]/\langle x\rangle$ is isomorphic to $\mathbf{Z}$, so $\langle x\rangle$ is a nonzero prime ideal that is not maximal, since $\mathbf{Z}$ is an integral domain that is not a field. This contradicts Theorem 5.3.10.

9.2. Unique Factorization Domains

8. A commutative ring R is said to be a *Noetherian* ring if every ideal of R has a finite set of generators. Prove that if R is a commutative ring, then R is Noetherian if and only if for any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ there exists a positive integer n such that $I_k = I_n$ for all $k > n$.

Solution: First assume that R is a Noetherian ring, and let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals of R. Let I be the union of the chain, so that $I = \{x \in R \mid x \in I_k \text{ for some } k\}$. If $x, y \in I$, then there exist integers k, m such that $x \in I_k$ and $y \in I_m$. Assume without loss of generality that $k \leq m$. Then $I_k \subseteq I_m$, so $x \in I_m$, and therefore $x + y \in I_m$ since I_m is an ideal of R. Thus we have shown that $x + y \in I$. For any $r \in R$ we have $rx \in I_k$, so $rx \in I$. This shows that the union I is an ideal, so it has a finite set of generators. Each of these generators belongs to I_k for some k, so if we let n be the maximum of these indices, then because the ideals I_k form a chain it follows that all of the generators of I belong to I_n. Therefore $I \subseteq I_n$, so we must have $I_n = I_{n+1} = I_{n+2} = \ldots$.

Conversely, assume that the given condition holds for ascending chains of ideals of R, and let I be any ideal of R. Let x_1 be a nonzero element of I. If $I = \langle x_1\rangle$, then I has a finite set of generators, and we are done. If not, let $I_1 = \langle x_1\rangle$, Then there exists $x_2 \in I - I_1$, and so we consider $I_2 = \{a_1x_1 + a_2x_2 \mid a_1, a_2 \in R\}$. The set I_2 is an ideal, with $I_1 \subset I_2 \subseteq I$. If $I_2 = I$, then I has two generators, and we are done. If not, we can choose $x_3 \in I - I_2$, and then we consider $I_3 = \{a_1x_1 + a_2x_2 + a_3x_3 \mid a_1, a_2, a_3 \in R\}$. Because of the condition on ascending chains, this procedure cannot produce an infinite ascending chain of ideals, each properly contained in the next, and so we conclude that for some n we have $I_n = I$. This shows that I has n generators, completing the proof.

9. Let R be a commutative Noetherian ring. This exercise provides an outline of the steps in a proof of the Hilbert basis theorem, which states that the polynomial ring $R[x]$ is a Noetherian ring.

(a) Let I be any ideal of $R[x]$, and let I_k be the set of all $r \in R$ such that $r = 0$ or r occurs as the leading coefficient of a polynomial of degree k in I. Prove that I_k is an ideal of R.

Solution: If $r, s \in I_k$, and either $r = 0$ or $s = 0$, then it is clear that $r + s \in I_k$. If $r \neq 0$ and $s \neq 0$, then there exist polynomials $p(x)$ and $q(x)$, each of degree k, such that r is the leading coefficient of $p(x)$, and s is the leading coefficient of $q(x)$. If $r + s = 0$, then $r + s \in I_k$ by definition, and if not, then $r + s$ is the leading coefficient of $p(x) + q(x)$, which has degree k and belongs to I. If $a \in R$, then either $ar = 0 \in I_k$, or ar is the leading coefficient of $ap(x)$, which belongs to I and has degree k.

(b) For the ideals I_k in part (a), prove that there exists an integer n such that $I_n = I_{n+1} = \cdots$.

Solution: Since $I_k \subseteq I_{k+1} \subseteq \cdots$ is an ascending chain of left ideals in R, this follows from Exercise 8.

(c) By assumption, each left ideal I_k is finitely generated (for $k \leq n$), and we can assume that it has $m(k)$ generators. Each generator of I_k is the leading coefficient of a polynomial of degree k, so we let $\{p_{jk}(x)\}_{j=1}^{m(k)}$ be the corresponding polynomials. Prove that $\mathcal{B} = \cup_{k=1}^{n} \{p_{jk}(x)\}_{j=1}^{m(k)}$ is a set of generators for I.

Solution: If the set $\mathcal{B}$ is not a generating set, then among the polynomials that cannot be expressed as linear combinations of polynomials in $\mathcal{B}$ there exists one of minimal degree, say $f(x) = ax^k + \cdots$. If $k < n$, then $a \in I_k$, and so $a = \sum_{j=1}^{m(k)} r_j a_{jk}$ for the generators $\{a_{jk}\}_{j=1}^{m(k)}$ of I_k. Then $f(x) - \sum_{j=1}^{m(k)} r_j p_{jk}(x)$ has lower degree, and still cannot be expressed as a linear combination of elements of $\mathcal{B}$. This is a contradiction. If $k \geq n$, then we have $a \in I_n$, and we can repeat the argument using the generators of I_n

Comment: We present another proof that if R is a commutative Noetherian ring, then $R[x]$ is Noetherian. It was given by Sarges, in *J. reine angew. Math.* 283/284 (1976), 436-437, and may be the shortest proof known.

Proof: We show that if $R[x]$ fails to be Noetherian, then so does R. Let I be an ideal of $R[x]$ that is not finitely generated, and let f_1 be a polynomial of minimal degree in I. If such polynomials f_i have already been chosen, for $1 \leq i < k-1$, let f_k be a polynomial of minimal degree in I such that f_k does not belong to the ideal $\langle f_1, \ldots, f_{k-1} \rangle$. For $1 \leq i < k$, let $n(i)$ be the degree f_i, and let $a_i \in R$ be the leading coefficient of f_i. By the choice of f_i we have $n(1) \leq n(2) \leq \cdots$. We will show that the ideals $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \cdots$ form a strictly ascending chain of ideals that does not become stationary. Suppose that $\langle a_1, \ldots, a_{k-1} \rangle = \langle a_1, \ldots, a_k \rangle$. Then $a_k \in \langle a_1, \ldots, a_{k-1} \rangle$, and so there exist $r_i \in R$ with $a_k = \sum_{i=1}^{k-1} r_i a_i$. Therefore the polynomial g defined by $g = f_k - \sum_{i=1}^{k-1} r_i x^{n(k)-n(i)} f_i$ belongs

to I, but not to the ideal $\langle f_1, \ldots, f_{k-1} \rangle$, and has lower degree than f_k. This contradicts the choice of f_k.

9.3. Some Diophantine Equations

5. This exercise outlines a proof that the equation $x^4 + y^4 = z^2$ has no solution in $\mathbf{Z}^+$.

(a) Suppose that there is a positive triple x, y, z such that $x^4 + y^4 = z^2$. Show that we may assume that $(x, y) = 1$, and that $(x^2, y^2, z) = 1$.

Solution: If $(x, y) = d$, then $x = du$ and $y = dv$ for $u, v \in \mathbf{Z}$, and so $d^4u^4 + d^4v^4 = z^2$, where $(u, v) = 1$. Now $d^4 \mid z^2$, and so $d^2 \mid z$. Thus $z = d^2w$, for some $w \in \mathbf{Z}$, and hence $u^4 + v^4 = w^2$. Clearly $(u^2, v^2, w) = 1$.

(b) Show that there exists a least positive integer z such that $x^4 + y^4 = z^2$, with $(x, y) = 1$, $x > 0$, and $y > 0$.

Solution: Apply the well-ordering principle.

(c) Show that $x \not\equiv y \pmod 2$.

Solution: Since $(x, y) = 1$, the numbers x and y cannot both be even. If both x and y are odd, then $z^2 \equiv 2 \pmod 4$, a contradiction.

(d) Without loss of generality, suppose that x is even and y is odd. Show that there exist positive integers $r < s$, $(r, s) = 1$, $r \not\equiv s \pmod 2$ such that $x^2 = 2sr$, $y^2 = s^2 - r^2$, and $z = s^2 + r^2$.

Solution: Apply Exercise 30 of Section 1.2 to get $x^2 = 2sr$, $y^2 = s^2 - r^2$, $z = s^2 + r^2$, where $0 < r < s$ and $(r, s) = 1$. If $r \equiv s \pmod 2$, then y would be even, a contradiction.

(e) Show that r is even, and s is odd.

Solution: If s were even, then r would be odd, and so $y^2 \equiv -1 \pmod 4$, a contradiction.

(f) Say that $r = 2t$. Show that $(t, s) = 1$, and that both t and s are squares.

Solution: Since $(2t, s) = 1$, we have $(t, s) = 1$. Since $x^2 = 2sr = 4st$ and $(t, s) = 1$, we have that s and t are squares.

(g) Show that there exist integers m, n such that $0 < m < n$, $(m, n) = 1$, and $t = mn$, $y = n^2 - m^2$, and $s = n^2 + m^2$.

Solution: Since t is a square, there exists a positive integer h such that $t = h^2$. From $y^2 + r^2 = s^2$ we get $y^2 + (2h^2)^2 = s^2$. Applying Exercise 30 of Section 1.2 again, there exist integers m, n with $0 < m < n$, $(m, n) = 1$, such that $2h^2 = 2mn$, $y = n^2 - m^2$, and $s = m^2 + n^2$. Hence $t = mn$, $y = n^2 - m^2$, and $s = n^2 + m^2$.

(h) Show that both m and n are squares.

Solution: This follows since $h^2 = mn$ and $(m, n) = 1$.

(i) Say $m = a^2$ and $n = b^2$. Show that there exists $k \in \mathbf{Z}$ such that $a^4 + b^4 = k^2$, and obtain a contradiction to the choice of z in part (b) of this exercise.

Solution: Since s is a square, there exists $k \in \mathbf{Z}$ such that $x = k^2 = m^2 + n^2 = a^4 + b^4$, and since $s > r$ and $r > 0$ is even, we have $s > 1$, and so $k > 1$. Thus $0 < k < k^2 = s < s^2 + r^2 = z$. Therefore we have a solution (a^2, b^2, k) to $x^4 + y^4 = z^2$, which contradicts the choice of z.

6. **(a)** Show that the equation $x^4 + y^4 = z^4$ has no integer solution with $xyz \neq 0$.

Solution: If (r, s, t) is a solution to $x^4 + y^4 = z^4$ with $rst \neq 0$, then (r, s, t^2) is a solution to $x^4 + y^4 = z^2$ with $rst^2 \neq 0$, and this contradicts Exercise 5.

(b) In order to prove Fermat's last theorem, show this it *suffices* to prove that for any odd prime p, the equation $x^p + y^p = z^p$ has no integer solution with $xyz \neq 0$.

Solution: Fermat's last theorem states that $x^n + y^n = z^n$ has no solution with $xyz \neq 0$ when $n \geq 3$. Now if $p \,|\, n$, where p is an odd prime, then $n = mp$ for some m, and (x^m, y^m, z^m) is a solution to $x^p + y^p = z^p$ whenever (x, y, z) is a solution to $x^n + y^n = z^n$. If n has no odd prime divisor, then since $n \geq 3$ we have $4 \,|\, n$, so $n = 4k$ and (x^k, y^k, z^k) is a solution to $x^4 + y^4 = z^4$ whenever (x, y, z) is a solution to $x^n + y^n = z^n$.

10 GROUPS: SELECTED TOPICS

10.1. Nilpotent Groups

5. **(a)** Prove that D_n is solvable for all n.

Solution: Using the usual description $D_n = \{a^i b^j \mid 0 \leq i < n, 0 \leq j < 2\}$, with $ba = a^{-1}b$, we know that $\langle a \rangle$ is a normal subgroup of index 2, and since the factor group is also abelian, we have produced a series of normal subgroups of D_n that shows that it is solvable.

(b) Prove that D_n is nilpotent if and only if n is a power of 2.

Solution: It was shown in Exercise 22 of Section 3.6 that if n is odd, then the center of D_n is trivial, and if $n = 2m$ is even, then the center of D_n is $\{e, a^m\}$. We will show that D_n is nilpotent if and only if n is a power of 2, with the help of the following lemma.

Lemma: If $n = 2m$ is even, then $D_n / \langle a^m \rangle \cong D_m$.

Proof: Let $D_m = \{c^i d^j \mid 0 \leq i < m, 0 \leq j < 2\}$, and define $\phi : D_n \to D_m$ by setting $\phi(a^i b^j) = c^i d^j$, for $0 \leq i < n$ and $0 \leq j < 2$. It is clear that ϕ defines a group homomorphism from D_n onto D_m, and that $\ker(\phi) =$
$\{a^i \mid i \equiv 0 \pmod{m}\} = \langle a^m \rangle$. □

We now show that D_n is nilpotent if and only if n is a power of 2. First suppose that $n = 2^k$. Then $|D_n| = 2^{k+1}$, so D_n is a 2-group and therefore nilpotent.

Conversely, suppose that $n = 2^k m$, where m is an odd integer. Then in the ascending central series $Z_i(D_n)$, the first term is the center $\langle a^{2^{k-1}m} \rangle$. To calculate the next term, we note that the image of $\langle a^{2^{k-2}m} \rangle$ in $D_n / \langle a^{2^{k-1}m} \rangle$ is its center, so $Z_2(D_n) = \langle a^{2^{k-2}m} \rangle$, and $D_n / Z_2(D_n) \cong D_{2^{k-2}m}$. Continuing in this fashion, we arrive at $Z_k(D_n)$, with $D_n / Z_k(D_n) \cong D_m$. Since the center of this factor group is trivial, the series terminates, and therefore D_n is not nilpotent.

6. Use Theorem 10.1.7 to prove that any factor group of a finite nilpotent group is again nilpotent.

Solution: Let N be a normal subgroup of G, and suppose that H/N is a maximal subgroup of G/N. The correspondence between subgroups of G/N and subgroups of G that contain N shows that H is a maximal subgroup of G, and so it is normal in G by Theorem 10.1.7. It follows that H/N is a normal subgroup of G/N, and thus Theorem 10.1.7 implies that G/N is nilpotent.

10.2. Internal Semidirect Products of Groups

5. Let G be the subgroup of $\mathrm{GL}_3(\mathrm{GF}(2))$ generated by the following matrices:
$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

(a) List the elements of G.

Solution: The following matrices form the smallest subgroup N of $GL_3(\mathrm{GF}(2))$ containing the first two of the given matrices:
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$
Note that each nonidentity element has order two.

Multiplying these matrices on the left by the third matrix interchanges the bottom two rows; multiplying on the right by the third matrix interchanges the two right hand columns. Either calculation produces the four additional matrices that make up the required subgroup G:
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

(b) Find elements $a, b \in G$ with $o(a) = 4$, $o(b) = 2$, $ba = a^3b$, and conclude that G is isomorphic to D_4. Identify the subgroups that show that it is an internal semidirect product of a cyclic subgroup of order 4 by a subgroup of order 2.

Solution: We need to find an element of order 4, and setting $a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ provides one, with $a^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ and $a^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. We can let b be any element not in this subgroup, say $b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$. Then
$$ba = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \text{ and}$$
$$a^3b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$
showing that $G \cong D_4$, and it is the internal semidirect product of the normal

subgroup $\langle a \rangle = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \right\}$
by the subgroup $\langle b \rangle = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\}$.

(c) Show that G is the internal semidirect product of a normal subgroup N isomorphic to the Klein four-group V by a subgroup of order 2.

Solution: Let $N = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right\}$, the elements of the form $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$, and let $K = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\}$. Then $N \cap K = \{I\}$, and so a counting argument shows that $NK = G$. Since N has index 2 in G, it is normal, and thus $G = N \rtimes K$. A short calculation shows that each element in N has order 2, and therefore N is isomorphic to the Klein four-group.

7. Let $n = 2m$, where m is an odd integer ≥ 3. Show that the dihedral group D_n is the internal semidirect product of a cyclic group of order m by a subgroup isomorphic to the Klein four-group.

Solution: Let $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$, where $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$. Let $N = \langle a^2 \rangle$ and $K = \{e, a^m, b, a^m b\}$. It is easily checked that K is a subgroup, and since each nontrivial element has order 2, it is isomorphic to the Klein four-group. If $a^i \in N$, where i is even, then $ba^i b^{-1} = a^{-i} \in N$, so N is a normal subgroup. Since every power of a^2 is even, we have $N \cap K = \{e\}$, and then it is clear that $NK = D_n$, completing the proof.

8. Let m, n be positive integers. Show that the direct product $\mathbf{Z}_m \times D_n$ is the internal semidirect product of a normal subgroup isomorpic to $\mathbf{Z}_m \oplus \mathbf{Z}_n$ by a subgroup of order 2.

Solution: Let $D_n = \{a^i b^j \mid 0 \leq i < n,\ 0 \leq j < 2\}$, where $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$. Let $N = \{(x, a^i) \mid x \in \mathbf{Z}_m,\ 0 \leq i < n\}$ and let $K = \langle (0, b) \rangle$. Then N is a subgroup of $\mathbf{Z}_m \times D_n$ by Exercise 11 of Section 3.3, it is normal since it has index 2, and it is clear that $NK = \mathbf{Z}_m \times D_n$. Thus $\mathbf{Z}_m \times D_n = N \rtimes K$, and it is easy to check that $N \cong \mathbf{Z}_m \oplus \mathbf{Z}_n$.

10.3. External Semidirect Products of Groups

6. Let C_4 be the cyclic group of order 4, written multiplicatively, and let α be the only nontrivial group homomorphism from C_4 into $\mathrm{Aut}(\mathbf{Z}_3) \cong C_2$. Find elements a of order 6 and b of order 4 with $b^2 = a^3$ and $ba = a^{-1}b$ such that $\mathbf{Z}_3 \rtimes_\alpha C_4$ can be described as $\{a^i b^j \mid 0 \leq i < 6,\ 0 \leq j < 2\}$.

Solution: We will use the given subgroups $C_4 = \{\pm 1, \pm i\}$ and $C_2 = \{\pm 1\}$ of $\mathbf{C}^\times$. Since $\mathrm{Aut}(\mathbf{Z}_3) \cong C_2$, the only nontrivial homomorphism $\alpha : C_4 \to C_2$ is defined by $\alpha(i) = -1$, and then $\alpha(-1) = 1$ and $\alpha(-i) = -1$. Thus α_{-1} is the identity automorphism, while α_i and α_{-i} represent a change of sign.

Let $a = (1, -1)$ and $b = (0, i)$ in $\mathbf{Z}_3 \rtimes_\alpha C_4$. We have
$a^2 = (1,-1) \cdot (1,-1) = (1 + \alpha_{-1}(1), (-1)(-1)) = (1 + 1, 1) = (2, 1)$,
$a^3 = (1,-1) \cdot (2, 1) = (1 + \alpha_{-1}(2), (-1)(1)) = (1 + 2, -1) = (0, -1)$,
$a^4 = (1,-1) \cdot (0,-1) = (1 + \alpha_{-1}(0), (-1)(-1)) = (1 + 0, 1) = (1, 1)$,
$a^5 = (1,-1) \cdot (1, 1) = (1 + \alpha_{-1}(1), (-1)(1)) = (1 + 1, -1) = (2, -1)$,
$a^6 = (1,-1) \cdot (2,-1) = (1 + \alpha_{-1}(2), (-1)(-1)) = (1 + 2, 1) = (0, 1)$,
and so $o(a) = 6$. In general, $(x, y) \cdot (0, z) = (x + \alpha_y(0), yz) = (x, yz)$, so $b^2 = (0, -1)$, $b^3 = (0, -i)$, and $b^4 = (0, 1)$, and thus b has order 4. From the above list of powers of a, it is clear that each element of $\mathbf{Z}_3 \rtimes_\alpha C_4$ has the form a^i or $a^i b$, for $0 \leq i < 6$.

From the above calculations, $b^2 = (0, -1) = a^3$, and $ba = (0, i) \cdot (1, -1) = (0 + \alpha_i(1), (i)(-1)) = (0 - 1, -i) = (2, -i)$ while $a^{-1}b = a^5 b = (2, -1) \cdot (0, i) = (2, -i)$, and so $ba = a^{-1}b$.

Comment: Since $b^2 = a^3$, we have $a^2 b^2 = a^5$, $a^4 b^2 = a$, $b^3 = a^3 b$, $a^2 b^3 = a^5 b$, and $a^4 b^3 = ab$. Thus can also write
$\mathbf{Z}_3 \rtimes_\alpha C_4 = \{a^{2i} b^j \mid 0 \leq i < 3,\ 0 \leq j < 4\}$.

7. Let V be the Klein four-group, written multiplicatively, and let $\alpha : V \to \mathrm{Aut}(\mathbf{Z}_3)$ be any nontrivial group homomorphism. Show that $\mathbf{Z}_3 \rtimes_\alpha V \cong D_6$.

Solution: By Example 10.3.3 we are free to consider any linear action of V on a cyclic group of order 3, written additively. Since each nontrivial element of $\mathbf{Z}_{12}^\times$ has order 2, it is isomorphic to V, and since $\mathbf{Z}_{12}^\times = \mathrm{Aut}(\mathbf{Z}_{12})$, it acts linearly on $\mathbf{Z}_{12}$. As in Example 10.3.4, we will make use of a subgroup of the holomorph $\mathcal{H}_{12}$ of $\mathbf{Z}_{12}$.

We can identity $\mathbf{Z}_{12}^\times = \{\pm 1, \pm 5\}$ with V, and we can identity the cyclic subgroup $N = \{0, 4, 8\} \subseteq \mathbf{Z}_{12}$ with $\mathbf{Z}_3$. Since this subgroup is also an ideal of the ring $\mathbf{Z}_{12}$, each element of $\mathrm{Aut}(\mathbf{Z}_{12})$ maps N to N. We conclude that multiplication in $\mathbf{Z}_{12}$ defines a linear action of $\mathbf{Z}_{12}^\times$ on N.

In the semidirect product $N \rtimes_\alpha \mathbf{Z}_{12}^\times$, let $a = (4, -5)$ and let $b = (0, -1)$. Then $(0, -1) \cdot (0, -1) = (0 + (-1)(0), (-1)(-1)) = (0, 1)$, and so b has order 2. We also have
$a^2 = (4,-5) \cdot (4,-5) = (4 + (-5)(4), (-5)(-5)) = (8, 1)$,

$a^3 = (4,-5)\cdot(8,1) = (4+(-5)(8),(-5)(1)) = (0,-5)$,
$a^4 = (4,-5)\cdot(0,-5) = (4+(-5)(0),(-5)(-5)) = (4,1)$,
$a^5 = (4,-5)\cdot(4,1) = (4+(-5)(4),(-5)(1)) = (8,-5)$,
$a^6 = (4,-5)\cdot(8,-5) = (4+(-5)(8),(-5)(-5)) = (0,1)$,
and so $o(a) = 6$. Since $(x,y)(0,-1) = (x,-y)$, it follows easily from the above list of powers of a that each element of $N \rtimes_\alpha \mathbf{Z}_{12}^\times$ has the form a^i or $a^i b$, for $0 \le i < 6$. Furthermore, $ba = (0,-1)\cdot(4,-5) = (0+(-1)(4),(-1)(-5)) = (8,5)$ and $a^5 b = (8,-5)\cdot(0,-1) = (8+(-5)(0),(-5)(-1)) = (8,5)$, and so we conclude that $\mathbf{Z}_3 \rtimes_\alpha V \cong N \rtimes_\alpha \mathbf{Z}_{12}^\times$ is isomorphic to the dihedral group D_6.

8. Using the isomorphism between $\mathbf{Z}_5^\times$ and $\mathrm{Aut}(\mathbf{Z}_5)$, define an action $\mu : \mathbf{Z}_5^\times \to \mathbf{Z}_5^\times$ of $\mathbf{Z}_5^\times$ on $\mathbf{Z}_5$ by $\mu(x) = x^2$, for all $x \in \mathbf{Z}_5^\times$.

(a) Find elements a of order 10 and b of order 4 with $b^2 = a^5$ and $ba = a^{-1}b$ such that $\mathbf{Z}_5 \rtimes_\mu \mathbf{Z}_5^\times$ can be described as $\{a^i b^j \mid 0 \le i < 10,\ 0 \le j < 2\}$.

Solution: Let $\mathbf{Z}_5^\times = \{\pm 1, \pm 2\}$ and $\mathbf{Z}_5 = \{0,1,2,3,4\}$. Since $\mathrm{Aut}(\mathbf{Z}_5) \cong \mathbf{Z}_5^\times$, the homomorphism μ defines a linear action of $\mathbf{Z}_5^\times$ on $\mathbf{Z}_5$ in which $\mu_k(n) = \mu(k)\cdot n = k^2 n$, for $k \in \mathbf{Z}_5^\times$, $n \in \mathbf{Z}_5$. Let $a = (1,-1)$ and $b = (0,2)$. For $(n_1,k_1),(n_2,k_2) \in \mathbf{Z}_5 \rtimes_\mu \mathbf{Z}_5^\times$ we have $(n_1,k_1)\cdot(n_2,k_2) = (n_1 + (k_1)^2 n_2, k_1 k_2)$, so in particular $(1,-1)\cdot(n,k) = (1+n,-k)$ and $(0,k_1)\cdot(0,k_2) = (0,k_1k_2)$. It follows that $\langle a\rangle = \{(0,1),(1,-1),(2,1),(3,-1),(4,1),(0,-1),(1,1),(2,-1),(3,1),(4,-1)\}$ and $\langle b\rangle = \{(0,1),(0,2),(0,-1),(0,-2)\}$. Thus $b^2 = a^5$, and $bab^{-1} = (0,2)\cdot(1,-1)\cdot(0,-2) = (0+4\cdot 1,-2)\cdot(0,-2) = (4,-2)\cdot(0,-2) = (4+4\cdot 0,-1) = (4,-1) = a^9$, and so $ba = a^{-1}b$. Furthermore, $(n,1)\cdot(0,2) = (n,2)$ and $(n,-1)\cdot(0,2) = (n,-2)$ so it is clear that $G = \{a^i b^j \mid 0 \le i < 10,\ 0 \le j < 2\}$.

(b) Show that the Frobenius group F_{20} has no element of order 10. Conclude that $\mathbf{Z}_5 \rtimes_\mu \mathbf{Z}_5^\times$ is not isomorphic to $\mathbf{Z}_5 \rtimes_\iota \mathbf{Z}_5^\times \cong F_{20}$.

Solution: In F_{20} an element of the form $\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$ has order 5 if $x \neq 0$. Since $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ y & a^4 \end{bmatrix}$, where $y = x(1+a+a^2+a^3)$, it follows that $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$ has order 4 for $a = 2,3,4$. (A routine calculation shows that $1 + a + a^2 + a^3 = 0$ for $a = 2,3,4$.) Therefore F_{20} has no element of order 10.

10. Let N and K be groups, let $\alpha, \beta : K \to \mathrm{Aut}(N)$ be group homomorphisms, let $\gamma \in \mathrm{Aut}(N)$, and define $\phi : N \rtimes_\alpha K \to N \rtimes_\beta K$ by setting $\phi((n,k)) = (\gamma(n),k)$, for all $n \in N$, $k \in K$. Show that ϕ is an isomorphism if and only if $\beta = i_\gamma \alpha$, where i_γ is the inner automorphism of $\mathrm{Aut}(N)$ determined by γ.

Solution: We have defined ϕ by setting $\phi((n,k)) = (\gamma(n),k)$, for all $n \in N$, $k \in K$, so it is clear that ϕ is one-to-one and onto since γ is an automorphism.

For $n_1, n_2 \in N$ and $k_1, k_2 \in K$, we have

$$\begin{aligned} \phi((n_1,k_1)(n_2,k_2)) &= \phi((n_1\alpha_{k_1}(n_2), k_1k_2)) \\ &= (\gamma(n_1\alpha_{k_1}(n_2)), k_1k_2) \\ &= (\gamma(n_1)\gamma(\alpha_{k_1}(n_2)), k_1k_2) \end{aligned}$$

$$\begin{aligned} \phi((n_1,k_1))\phi((n_2,k_2)) &= (\gamma(n_1),k_1)(\gamma(n_2),k_2) \\ &= (\gamma(n_1)\beta_{k_1}(\gamma(n_2)), k_1k_2) \end{aligned}$$

Thus ϕ preserves the respective multiplications if and only if $\gamma(\alpha_k(n)) = \beta_k(\gamma(n))$ for all $n \in N$ and $k \in K$. We can write this as $\gamma\alpha_k = \beta_k\gamma$, for all $k \in K$, and so $\beta_k = \gamma\alpha_k\gamma^{-1}$, for all $k \in K$. Therefore $\beta(k) = i_\gamma\alpha(k)$, for all $k \in K$.

10.4. Classification of Groups of Small Order

6. Show that the holomorph $\mathcal{H}_n = \mathbf{Z}_n \rtimes_\alpha \mathbf{Z}_n^\times$ of $\mathbf{Z}_n$ can be represented as the set of matrices of the form $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$, where $x \in \mathbf{Z}_n$ and $a \in \mathbf{Z}_n^\times$.

Solution: The first issue is that up to this point we have only considered matrices with entries in a field, and these matrices have entries in a commutative ring $\mathbf{Z}_n$. The standard proof that multiplication of matrices is associative (when the entries are from a field) remains valid when the entries come from a commutative ring R, and it is clear that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is a multiplicative identity element. If $a, b, c, d \in R$, then $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (ad - bc)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ since R is commutative, and so the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible if and only if its determinant $ad - bc$ is a unit of R. These observations show that the matrices we are considering are invertible. In fact, $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ -a^{-1}x & a^{-1} \end{bmatrix}$, since a is a unit of $\mathbf{Z}_n$.

For $(x, a) \in \mathbf{Z}_n \rtimes_\alpha \mathbf{Z}_n^\times$, define $\phi((x,a)) = \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$. Then ϕ is a group homomorphism since $\phi((x_1,a_1)(x_2,a_2)) = \phi((x_1 + a_1x_2, a_1a_2)) = \begin{bmatrix} 1 & 0 \\ x_1 + a_1x_2 & a_1a_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ x_1 & a_1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ x_2 & a_2 \end{bmatrix} = \phi((x_1,a_1))\phi((x_2,a_2))$. It is clear that ϕ is one-to-one and onto, and so ϕ is an isomorphism.

9. Consider the holomorph $\mathcal{H}_{15} = \mathbf{Z}_{15} \rtimes \mathbf{Z}_{15}^{\times}$ of $\mathbf{Z}_{15}$, using its representation from Exercise 6 as matrices of the form $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$, where $x \in \mathbf{Z}_{15}$ and $a \in \mathbf{Z}_{15}^{\times}$. Note that $\mathbf{Z}_{15}^{\times}$ has three cyclic subgroups of order 2: $\langle -1 \rangle$, $\langle 4 \rangle$, and $\langle -4 \rangle$.

(a) Let G_1 be the subgroup of $\mathcal{H}_{15}$ with $a \in \langle -1 \rangle$. Show that $G_1 \cong D_{15}$.

Solution: Let $c = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and $d = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Then $o(c) = 15$, $o(d) = 2$, and $dc = c^{-1}d$ since the action of $\langle -1 \rangle$ on $\mathbf{Z}_{15}$ changes the sign. Thus $G_1 \cong D_{15}$.

(b) Let G_2 be the subgroup of $\mathcal{H}_{15}$ with $a \in \langle 4 \rangle$. Show that $G_2 \cong \mathbf{Z}_3 \times D_5$.

Solution: Let $b = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$. We have $\mathbf{Z}_{15} = 5\mathbf{Z}_{15} \oplus 3\mathbf{Z}_{15} \cong \mathbf{Z}_3 \oplus \mathbf{Z}_5$. Since $4 \cdot 5 = 20 \equiv 5 \pmod{15}$ and $4 \cdot 3 = 12 \equiv -3 \pmod{15}$, the element b acts as the identity on $5\mathbf{Z}_{15}$ and changes the sign on $3\mathbf{Z}_{15}$. Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \middle| x \in 5\mathbf{Z}_{15}, a = 1 \right\}$, $K = \left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \middle| x \in 3\mathbf{Z}_{15}, a \in \langle 4 \rangle \right\}$.

Then H is cyclic of order 3, so $H \cong \mathbf{Z}_3$, and $K \cong D_5$ since it is a nonabelian group of order 10. We have $H \cap K = \{I\}$, so $HK = G_2$. To show that G_2 is the internal direct product of H and K we will show that elements of H and K commute. Let $\begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \in H$ and let $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \in K$. Then $\begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ y + x & a \end{bmatrix}$, while $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ x + ay & a \end{bmatrix}$. But (as shown above) since $a = 1$ or $a = 4$ and $y = 0, 5, 10$, we have $ay \equiv y \pmod{15}$, and so the elements commute.

(c) Let G_3 be the subgroup of $\mathcal{H}_{15}$ with $a \in \langle -4 \rangle$. Show that $G_3 \cong \mathbf{Z}_5 \times D_3$.

Solution: Let $b = \begin{bmatrix} 1 & 0 \\ 0 & -4 \end{bmatrix}$. We have $\mathbf{Z}_{15} = 3\mathbf{Z}_{15} \oplus 5\mathbf{Z}_{15} \cong \mathbf{Z}_5 \oplus \mathbf{Z}_3$. Since $-4 \cdot 3 = -12 \equiv 3 \pmod{15}$ and $-4 \cdot 5 = -20 \equiv -5 \pmod{15}$, the element b acts as the identity on $3\mathbf{Z}_{15}$ and changes the sign on $5\mathbf{Z}_{15}$. As in part (b), it can be checked that G_3 is the internal direct product of H and K, for $H = \left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \middle| x \in 3\mathbf{Z}_{15}, a = 1 \right\}$, $K = \left\{ \begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix} \middle| x \in 5\mathbf{Z}_{15}, a \in \langle -4 \rangle \right\}$. Furthermore, $H \cong \mathbf{Z}_5$ and $K \cong D_3$, as required.

(d) Show that the groups G_1, G_2, G_3 represent three distinct isomorphism classes.

Solution: We can distinguish between the groups by looking at their centers. Exercise 22 of Section 3.6 shows that the center of D_n is trivial if n is odd. It is easy to check that the center of a direct product is the direct product of the centers. Thus

the center of G_1 is trivial, the center of G_2 is its Sylow 3-subgroup, and the center of G_3 is its Sylow 5-subgroup.

10. Show that any nonabelian group of order 30 is isomorphic to D_{15}, $\mathbf{Z}_3 \times D_5$, or $\mathbf{Z}_5 \times D_3$.

Solution: Let G be a group of order $30 = 2 \cdot 3 \cdot 5$. By Theorem 7.4.4 the number of Sylow 5-subgroups is 1 or 6, and the number of Sylow 3-subgroups is 1 or 10. If neither of these Sylow subgroups were normal, then G would contain $6 \cdot 4 = 24$ elements of order 5 and and $10 \cdot 2 = 20$ elements of order 3, which is impossible. We conclude that either the Sylow 5-sybgroup or the Sylow 3-subgroup is normal.

Suppose that the Sylow 5-subgroup P_5 is normal. Then $|G/P_5| = 6$ has a subgroup of index 2 since G/P_5 is isomorphic to $\mathbf{Z}_6$ or S_3. Proposition 3.8.7 shows that G has a corresponding subgroup of index 2, which must be normal. If the Sylow 3-subgroup P_3 is normal, then $|G/P_3| = 10$, and again G has a normal subgroup of index 2 since the same is true for G/P_3, which isomorphic to $\mathbf{Z}_{10}$ or D_5.

Since a subgroup of order 15 is isomorphic to $\mathbf{Z}_{15}$, we conclude that G is the internal semidirect product of a normal cyclic group of order 15 by a subgroup of order 2. By Theorem 10.4.4, we can consider the possible external semidirect products. These are determined by a group homomorphism $\alpha : C_2 \to \mathbf{Z}_{15}^\times$. Let $\mathbf{Z}_{15}^\times = \{\pm 1, \pm 2, \pm 4, \pm 8\}$. The image of α in $\mathbf{Z}_{15}^\times$ is $\{1\}$ or one of three cyclic subgroups of order 2: $\langle -1 \rangle$, $\langle 4 \rangle$, and $\langle -4 \rangle$. Thus there are at most 3 isomorphism classes of nonabelian external semidirect products $\mathbf{Z}_{15} \rtimes_\alpha C_2$. The desired conclusion, that G is belongs to one of the isomorphism classes represented by D_{15}, $\mathbf{Z}_3 \times D_5$, or $\mathbf{Z}_5 \times D_3$, now follows from Exercise 9.