

Selected Answers

Failures, repeated failures, are finger posts on the road to achievement. One fails forward toward success.

C. S. Lewis

For some exercises only partial answers are provided. Many of the proofs given below are merely sketches. In these cases, the student should supply the complete proof

Chapter 0

In short, if we adhere to the standard of perfection in all our endeavors, we are left with nothing but mathematics and the White Album.

DANIEL GILBERT, *Stumbling on Happiness*

1. $\{1, 2, 3, 4\}; \{1, 3, 5, 7\};$
 $\{1, 5, 7, 11\}; \{1, 3, 7, 9, 11, 13, 17, 19\};$
 $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16,$
 $17, 18, 19, 21, 22, 23, 24\}$
3. 12, 2, 2, 10, 1, 0, 4, 5
5. Let a be the least common multiple of every element of the set and b be any common multiple of every element of the set. Write $b = aq + r$ where $0 \leq r < a$. Then for any element c in the set we have that c divides $b - aq = r$. This means that r is common multiple of every element of the set and therefore is greater than or equal to a , which is a contradiction.
7. By using 0 as an exponent if necessary, we may write $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{n_1} \cdots p_k^{n_k}$, where the p 's are distinct primes and the m 's and n 's are nonnegative. Then $\text{lcm}(a, b) = p_1^{s_1} \cdots p_k^{s_k}$, where

$s_i = \max(m_i, n_i)$, and
 $\text{gcd}(a, b) = p_1^{t_1} \cdots p_k^{t_k}$, where
 $t_i = \min(m_i, n_i)$. Then
 $\text{lcm}(a, b) \cdot \text{gcd}(a, b) =$
 $p_1^{m_1+n_1} \cdots p_k^{m_k+n_k} = ab.$

9. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where $0 \leq r_1, r_2 < n$. We may assume that $r_1 \geq r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, where $r_1 - r_2 \geq 0$. If $a \bmod n = b \bmod n$, then $r_1 = r_2$ and n divides $a - b$. If n divides $a - b$, then by the uniqueness of the remainder, we have $r_1 - r_2 = 0$.
11. Use Exercise 9.
13. Use Theorem 0.2.
15. By Theorem 0.2 there are integers s and t such that $ms + nt = 1$. Then $m(sr) + n(tr) = r$.
17. Let p be a prime greater than 3. By the division algorithm, we can write p in the form $6n + r$, where r satisfies $0 \leq r < 6$. Now observe that $6n$, $6n + 2$, $6n + 3$, and $6n + 4$ are not prime.
19. Since st divides $a - b$, both s and t divide $a - b$. The converse is true when $\text{gcd}(s, t) = 1$.
21. Use Euclid's Lemma and the Fundamental Theorem of Arithmetic.

23. Use proof by contradiction.
25. x NAND y is 1 if and only if both inputs are 0; x XNOR y is 1 if and only if both inputs are the same.
27. Let S be a set with $n + 1$ elements and pick some a in S . By induction, S has 2^n subsets that do not contain a . But there is a one-to-one correspondence between the subsets of S that do not contain a and those that do. So, there are $2 \cdot 2^n = 2^{n+1}$ subsets in all.
29. Consider $n = 200! + 2$.
31. Say $p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, where the p 's and q 's are primes. By the Generalized Euclid's Lemma, p_1 divides some q_i , say q_1 (we may relabel the q 's if necessary). Then $p_1 = q_1$ and $p_2 \dots p_r = q_2 \dots q_s$. Repeating this argument at each step, we obtain $p_2 = q_2, \dots, p_r = q_r$ and $r = s$.
33. Suppose that S is a set that contains a and whenever $n \geq a$ belongs to S , then $n + 1 \in S$. We must prove that S contains all integers greater than or equal to a . Let T be the set of all integers greater than a that are not in S and suppose that T is not empty. Let b be the smallest integer in T (if T has no negative integers, b exists because of the Well Ordering Principle; if T has negative integers, it can have only a finite number of them so that there is a smallest one). Then $b - 1 \in S$, and therefore $b = (b - 1) + 1 \in S$.
35. For $n = 1$, observe that $1^3 + 2^3 + 3^3 = 36$. Assume that $n^3 + (n + 1)^3 + (n + 2)^3 = 9m$ for some integer m . We must prove that $(n + 1)^3 + (n + 2)^3 + (n + 3)^3$ is a multiple of 9. Using the induction hypothesis we have that $(n + 1)^3 + (n + 2)^3 + (n + 3)^3 = 9m - n^3 + (n + 3)^3 = 9m - n^3 + n^3 + 3 \cdot n^2 \cdot 3 + 3 \cdot n \cdot 9 + 3^3 = 9m + 9n^2 + 27n + 27$.
37. The statement is true for any divisor of $8^3 - 4 = 508$.
39. 6 P.M.
41. Observe that the number with the decimal representation $a_9 a_8 \dots a_1 a_0$ is $a_9 \cdot 10^9 + a_8 \cdot 10^8 + \dots + a_1 \cdot 10 + a_0$. Then use Exercise 9 and the fact that $a_i 10^i \bmod 9 = a_i \bmod 9$ to deduce that the check digit is $(a_9 + a_8 + \dots + a_1 + a_0) \bmod 9$.
43. For the case in which the check digit is not involved, see the answer to Exercise 41. If a transposition involving the check digit $c = (a_1 + a_2 + \dots + a_{10}) \bmod 9$ goes undetected, then $a_{10} = (a_1 + a_2 + \dots + a_9 + c) \bmod 9$. Substitution yields $2(a_1 + a_2 + \dots + a_9) \bmod 9 = 0$. Therefore, modulo 9, we have $10(a_1 + a_2 + \dots + a_9) = a_1 + a_2 + \dots + a_9 = 0$. It follows that $c = a_{10}$. In this case the transposition does not yield an error.
47. Cases where $(2a - b - c) \bmod 11 = 0$ are undetected.
49. No. $(1, 0) \in R$ and $(0, -1) \in R$, but $(1, -1) \notin R$.
51. a belongs to the same subset as a . If a and b belong to the subset A , then b and a also belong to A . If a and b belong to the subset A and b and c belong to the subset B , then $A = B$, since the distinct subsets of P are disjoint. So, a and c belong to A .

Chapter 1

If you are ready to learn from them, mistakes can be your friend.

FRANK WILCZEK

- Three rotations 0° , 120° , 240° —and three reflections across lines from vertices to midpoints of opposite sides. See the back inside cover for a picture.
- a.** V **b.** R_{270} **c.** R_0 **d.** $R_0, R_{180}, H, V, D, D'$ **e.** none
- D_n has n rotations of the form $k(360^\circ/n)$, where $k = 0, \dots, n - 1$. In addition, D_n has n reflections. When n is odd, the axes of reflection are the lines from the vertices to the midpoints of the opposite sides. When n is even, half of the axes of reflection

- are obtained by joining opposite vertices; the other half, by joining midpoints of opposite sides.
7. A rotation followed by a rotation either fixes every point (and so is the identity) or fixes only the center of rotation. However, a reflection fixes a line.
 9. Observe that $1 \cdot 1 = 1$; $1(-1) = -1$; $(-1)1 = -1$; $(-1)(-1) = 1$. These relationships also hold when 1 is replaced by “rotation” and -1 is replaced by “reflection.”
 11. Thinking geometrically and observing that even powers of elements of a dihedral group do not change orientation, we note that each of a , b and c appears an even number of times in the expression. So, there is no change in orientation. Thus, the expression is a rotation.
 13. In D_4 , $HD = DV$ but $H \neq V$.
 15. R_0, R_{180}, H, V . Use the table in Chapter 1 to construct the Cayley table. Yes. Each has two rotations and two reflections.
 17. See answer for Exercise 15.
 19. In each case, the group is D_6 .
 21. First observe that squaring R_0, R_{180} or any reflection gives R_0 and squaring R_{90} or R_{270} gives R_{180} . Thus $X^2Y = Y$ or $X^2Y = R_{180}Y$. Since $Y \neq R_{90}$ we have $X^2Y = R_{180}Y$ and $X^2Y = R_{90}$. Thus $R_{180}Y = R_{90}$. Solving for Y gives $Y = R_{270}$.
 23. By Exercise 8 the elements listed are reflections. No two of these are equal for if so then multiplying by F on the right would yield equal rotations, which is not true.
 5. $7; 13; n - 1; \frac{3}{13} + \frac{2}{13}i$
 7. G_3 .
 9. If $5x = 3$ then multiply both sides by 4 we get $0 = 12$. If $3x = 5$ then multiply both sides by 7 we get $x = 15$. Checking we see that $3 \cdot 15 = 5 \pmod{20}$.
 11. One is Socks-Shoes-Boots.
 13. Under multiplication modulo 4, 2 does not have an inverse. Under multiplication modulo 5, each element has an inverse.
 15. a^{11}, a^6, a^4, a .
 17. **a.** $2a + 3b$ **b.** $-2a + 2(-b + c)$
c. $-3(a + 2b) + 2c = 0$
 19. Observe that $a^5 = e$ and $b^7 = e$ imply that $a^{-2} = a^3$ and $b^{-4} = b^3$. Thus, $a^{-2}b^{-4} = a^3b^3$. Moreover, $(a^2b^4)^{-2} = ((a^2b^4)^{-1})^2 = (b^{-4}a^{-2})^2 = (b^3a^3)^2 = b^3a^3b^3a^3$.
 21. Use $\det(AB) = (\det A)(\det B)$.
 23. 29
 25. For $n \geq 0$, use induction. For $n < 0$, note that $e = (ab)^0 = (ab)^n(ab)^{-n} = (ab)^na^{-n}b^{-n}$ so that $a^nb^n = (ab)^n$. In a non-Abelian group $(ab)^n$ need not equal a^nb^n .
 27. Use the Socks-Shoes Property.
 29. For the case $n > 0$, use induction. For $n < 0$, note that $e = (a^{-1}ba)^n(a^{-1}ba)^{-n} = (a^{-1}ba)^n(a^{-1}b^{-n}a)$ and solve for $(a^{-1}ba)^n$.
 31. $\{1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45\}$
 33. Suppose x appears in a row labeled with a twice; say, $x = ab$ and $x = ac$. Then cancellation yields $b = c$. But we use distinct elements to label the columns.
 35. Closure and associativity follow from the definition of multiplication; $a = b = c = 0$ gives the identity; we may find inverses by solving the equations $a + a' = 0$, $b' + ac' + b = 0$, $c' + c = 0$ for a', b', c' .
 37. Since e is one solution it suffices to show that nonidentity solutions come in distinct pairs. To this end note that if $x^n = e$ and $x \neq e$, then $(x^{-1})^n = e$

Chapter 2

There are no secrets to success. It is the result of preparation, hard work, and learning from failure.

COLIN POWELL

1. **c, d**
3. none

and $x \neq x^{-1}$. So if we can find one nonidentity solution we can find a second one. Now suppose that a and a^{-1} are nonidentity elements that satisfy $x^n = e$ and b is a nonidentity element such that $b \neq a$ and $b \neq a^{-1}$ and $b^n = e$. Then, as before, $(b^{-1})^n = e$ and $b \neq b^{-1}$. Moreover, $b^{-1} \neq a$ and $b^{-1} \neq a^{-1}$. Thus, finding a third nonidentity solution gives a fourth one. Continuing in this fashion we see that we always have an even number of nonidentity solutions to the equation $x^3 = e$.

To prove the second statement note that if $x^2 \neq e$, then $x^{-1} \neq x$ and $(x^{-1})^2 \neq e$. So, arguing as in the preceding case we see that solutions to $x^2 \neq e$ come in distinct pairs.

39. If $F_1 F_2 = R_0$, then $F_1 F_1 = F_1 F_2$ and by cancellation $F_1 = F_2$.
41. Since FR^k is a reflection we know that $(FR^k)(FR^k) = R_0$. So $R^k FR^k = F^{-1} = F$.
43. $R, R^{-1}F$
45. Since $a^2 = b^2 = (ab)^2 = e$, we have $aabb = abab$. Now cancel on the left and right.
47. The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $GL(2, Z_2)$ if and only if $ad \neq bc$. This happens when a and d are 1 and at least 1 of b and c is 0, and when b and c are 1 and at least 1 of a and d is 0. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ do not commute.
49. Use Exercise 33.
51. Let a be any element in G . Then for each b in G a appears exactly once in the row headed by b in the Cayley table for G .
53. $Z_{16}, D_8, U(17)$ and $U(32)$.

Chapter 3

Success is the ability to go from one failure to another with no loss of enthusiasm.

SIR WINSTON CHURCHILL

1. $|Z_{12}| = 12; |U(10)| = 4; |U(12)| = 4; |U(20)| = 8; |D_4| = 8$
In $Z_{12}, |0| = 1; |1| = |5| = |7| = |11| = 12; |2| = |10| = 6; |3| = |9| = 4; |4| = |8| = 3; |6| = 2$.
In $U(10), |1| = 1; |3| = |7| = 4; |9| = 2$.
In $U(12), |1| = 1; |5| = 2; |7| = 2; |11| = 2$. In $U(20), |1| = 1; |3| = |7| = |13| = |17| = 4; |9| = |11| = |19| = 2$.
In $D_4, |R_0| = 1; |R_{90}| = |R_{270}| = 4; |R_{180}| = |H| = |V| = |D| = |D'| = 2$.
In each case, notice that the order of the element divides the order of the group.
3. In $Q, |0| = 1$ and all other elements have infinite order. In $Q^*, |1| = 1, |-1| = 2$, and all other elements have infinite order.
5. Use Theorem 0.2.
7. Each is the inverse of the other.
9. $(a^4 c^{-2} b^4)^{-1} = b^{-4} c^2 a^{-4} = b^3 c^2 a^2$
11. $\{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\}$ where F is any reflection in D_6 .
13. $D_4; D_4$; it contains $\{R_0, R_{180}, H, V\}$
15. If n is a positive integer, the real solutions of $x^n = 1$ are 1 when n is odd and ± 1 when n is even. So, the only elements of finite order in R^* are ± 1 .
17. By Exercise 29 of Chapter 2 we have $e = (xax^{-1})^n = xa^n x^{-1}$ if and only if $a^n = e$.
19. Suppose $G = H \cup K$. Pick $h \in H$ with $h \notin k$. Pick $k \in K$ with $k \notin H$. Then, $hk \in G$ but $hk \notin H$ and $hk \notin K$.
 $U(8) = \{1, 3\} \cup \{1, 5\} \cup \{1, 7\}$.
21. $U_4(20) = \{1, 9, 13, 17\}; U_5(20) = \{1, 11\}; U_5(30) = \{1, 11\}; U_{10}(30) = \{1, 11\}$. To prove that $U_k(n)$ is a subgroup, it suffices to show that it is closed. Suppose that a and b belong to $U_k(n)$. We must show that in $U(n), ab \bmod k = 1$. That is, $(ab \bmod n) \bmod k = 1$. Let $n = kt$ and $ab = qn + r$ where $0 \leq r < n$. Then $(ab \bmod n) \bmod k = r \bmod k = (ab - qn) \bmod k = (ab - qkt) \bmod k = ab \bmod k = (a \bmod k)(b \bmod k) = 1 \cdot 1 = 1$. H is not a subgroup because $7 \in H$ but $7 \cdot 7 = 9$ is not $1 \bmod 3$.

23. Suppose that $m < n$ and $a^m = a^n$. Then $e = a^n a^{-m} = a^{n-m}$. This contradicts the assumption that a has infinite order.
25. $\det A = \pm 1$
27. $\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 9, 13, 11, 5, 1\} = U(14)$. $\langle 5 \rangle = \{5, 5^2, 5^3, 5^4, 5^5, 5^6\} = \{5, 11, 13, 9, 3, 1\} = U(14)$. $\langle 11 \rangle = \{11, 9, 1\} \neq U(14)$. Since $|U(20)| = 8$, for $U(20) = \langle k \rangle$ for some k it must be the case that $|k| = 8$. But $1^1 = 1$, $3^4 = 1$, $7^4 = 1$, $9^2 = 1$, $11^2 = 1$, $13^4 = 1$, $17^4 = 1$, and $19^2 = 1$. So, the maximum order of any element is 4.
29. By Exercise 28, either every element of H is even or exactly half are even. Since H has odd order the latter cannot occur.
31. By Exercise 30, either every element of H is a rotation or exactly half are rotations. Since H has odd order the latter cannot occur.
33. Since n is even, D_n contains R_{180} . Let F be any reflection in D_n . Then the set $\{R_0, R_{180}, F, R_{180}F\}$ is closed and therefore is a subgroup of D_n .
35. $\langle 2 \rangle, \langle 3 \rangle, \langle 6 \rangle$
37. Suppose that H is a subgroup of D_3 of order 4. Since D_3 has only two elements of order 2, H must contain R_{120} or R_{240} . By closure, it follows that H must contain R_0 , R_{120} , and R_{240} as well as some reflection F . But then H must also contain the reflection $R_{120}F$.
39. $\{R_0, R_{180}\}$
41. If $x \in Z(G)$, then $x \in C(a)$ for all a , so $x \in \bigcap_{a \in G} C(a)$. If $x \in \bigcap_{a \in G} C(a)$, then $xa = ax$ for all a in G , so $x \in Z(G)$.
43. The case that $k = 0$ is trivial. Let $x \in C(a)$. If k is positive, then by induction on k , $xa^{k+1} = xaa^k = axa^k = aa^kx = a^{k+1}x$. The case where k is negative now follows from Exercise 34. In a group, if x commutes with a , then x commutes with all powers of a . If x commutes with a^k for some k , then x need not commute with a .
45. a. First observe that because $\langle S \rangle$ is a subgroup of G containing S , it is a member of the intersection. So, $H \subseteq \langle S \rangle$. On the other hand, since H is a subgroup of G and H contains S , by definition $\langle S \rangle \subseteq H$.
- b. Let $K = \{s_1^{n_1} s_2^{n_2} \dots s_m^{n_m} \mid m \geq 1, s_i \in S, n_i \in \mathbb{Z}\}$. Then because K satisfies the subgroup test and contains S , we have $\langle S \rangle \subseteq K$. On the other hand, if L is any subgroup of G that contains S , then L also contains K by closure. Thus, by part a, $H = \langle S \rangle$ contains K .
47. Mimic the proof of Theorem 3.5.
49. No. In D_4 , $C(R_{180}) = D_4$. Yes. Elements in the center commute with all elements.
51. For the first part, see Example 4. For the second part, use D_4 .
53. Note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.
55. First observe that $(a^d)^{n/d} = a^n = e$, so $|a^d|$ is at most n/d . Moreover, there is no positive integer $t < n/d$ such that $(a^d)^t = a^{dt} = e$, for otherwise $|a| \neq n$.
57. Let G be a group of even order. Observe that for each element x of order greater than 2 x and x^{-1} are distinct elements of the same order. So, because elements of order greater than 2 come in pairs, there is an even number of elements of order greater than 2 (possibly 0). This means that the number of elements of order 1 or 2 is even. Since the identity is the unique element of order 1, it follows that the number of order 2 is odd.
59. For any positive integer n , a rotation of $360^\circ/n$ has order n . A rotation of $\sqrt{2}$ degrees has infinite order.
61. Inscribe a regular n -gon in a circle. Then every element of D_n is a symmetry of the circle.
63. Let $|g| = m$ and write $m = nq + r$, where $0 \leq r < n$. Then $g^r = g^{m-nq} = g^m(g^n)^{-q} = (g^n)^{-q}$ belongs to H . So, $r = 0$.
65. $1 \in H$. Let $a, b \in H$. Then $(ab^{-1})^2 = a^2(b^2)^{-1}$, which is the product of two rationals. 2 can be

- replaced by any positive integer.
67. Let $|a| = n$ and $m = nq = r$ where $0 \leq r < n$. Then $a^r = a^{m-nq} = a^m(a^{-q})^n = ee = e$. So, $r = 0$.
69. In Z_6 , $H = \{0, 1, 3, 5\}$ is not closed.
71. a. Let xh_1x^{-1} and xh_2x^{-1} belong to xHx^{-1} . Then $(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$ also.
 b. Let $\langle h \rangle = H$. Then $\langle xhx^{-1} \rangle = xHx^{-1}$.
 c. $(xh_1x^{-1})(xh_2x^{-1}) = xh_1h_2x^{-1} = xh_2h_1x^{-1} = (xh_2x^{-1})(xh_1x^{-1})$.
73. Let a/b and c/d belong to the set. By observation ac/bd and b/a have odd numerators and denominators. If ac/bd reduces lowest terms to x/y then x divides ac and y divides bd . So they are odd.
75. If 2^a and $2^b \in K$, then $2^a(2^b)^{-1} = 2^{a-b} \in K$, since $a - b \in H$.
77. $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & n \\ 0 & \frac{1}{2} \end{bmatrix}$ is not in H .
79. If $a + bi$ and $c + di \in H$, then $(a + bi)(c + di)^{-1} = (ac + bd) + (bc - ad)i$ and $(ac + bd)^2 + (bc - ad)^2 = 1$, so that H is a subgroup. H is the unit circle in the complex plane.
81. $\{1, 2n - 1, 2n + 1, 4n - 1\}$
83. In D_{10} let a be any reflection and $b = R_{36}$.
85. First observe that $2^n - 1$ and $2^{n-2} \pm 1$ are in $U(2^n)$ and satisfy $x^2 = 1$. Now suppose that $x \in U(2^n)$, $x \neq 1$, and $x^2 = 1 \pmod{2^n}$. From $x^2 = 1 \pmod{2^n}$ we have that $x^2 - 1 = (x - 1)(x + 1)$ is divisible by 2^n . Since $x - 1$ and $x + 1$ are even and $n \geq 3$, we know that at least one of $x - 1$ and $x + 1$ is divisible by 4. Moreover, it cannot be the case that both $x - 1$ and $x + 1$ are divisible by 4 for then so would $(x + 1) - (x - 1) = 2$. If $x - 1$ is not divisible by 4, then $x + 1$ is divisible by 2^{n-1} . Thus $x + 1 = k2^{n-1}$ for some integer k and $k2^{n-1} = x + 1 \leq 2^n$. So, $k = 1$ or $k = 2$. For $k = 1$, we have $x = 2^{n-1} - 1$. For $k = 2$, we have $x = 2^n - 1$. If $x + 1$ is not divisible by 4, then $x - 1$ is divisible by 2^{n-1} .
- Thus $x - 1 = k2^{n-1}$ for some integer k and $k2^{n-1} = x - 1 < 2^n$. So, $k = 1$ and $x = 2^{n-1} + 1$.
87. Since $ee = e$ is in $HZ(G)$, it is nonempty. Let h_1z_1 and h_2z_2 belong to $HZ(G)$. Then $h_1z_1(h_2z_2)^{-1} = h_1z_1z_2^{-1}h_2^{-1} = h_1h_2^{-1}z_1z_2^{-1} \in HZ(G)$.
89. Use Exercise 88.
91. In a finite group G , $|C(x)|/|G|$ is the probability that x commutes with every element of G . Let x be any element in D_4 . If $x = R_0$ or R_{180} the probability that x commutes with every element is 1. If $x = R_{90}$ or R_{270} the probability that x commutes with every element is .5. If x is a reflection the probability that x commutes with every element is .5 (x commutes with R_0, R_{180}, x , and $R_{180}x$). So, the probability that any two elements commute exceeds .5 (the exact probability is 5/8). For D_3 , the probability is .5.

Chapter 4

A mistake is to commit a misunderstanding.

BOB DYLAN

- For Z_6 , generators are 1 and 5; for Z_8 , generators are 1, 3, 5, and 7; for Z_{20} , generators are 1, 3, 7, 9, 11, 13, 17, and 19.
- $\langle 20 \rangle = \{20, 10, 0\}$; $\langle 10 \rangle = \{10, 20, 0\}$; $\langle a^{20} \rangle = \{a^{20}, a^{10}, a^0\}$; $\langle a^{10} \rangle = \{a^{10}, a^{20}, a^0\}$
- $\langle 3 \rangle = \{3, 9, 7, 1\}$; $\langle 7 \rangle = \{7, 9, 3, 1\}$
- $U(8)$ or D_3
- Six subgroups; generators are the divisors of 20. Six subgroups; generators are a^k , where k is a divisor of 20.
- By definition, $a^{-1} \in \langle a \rangle$. So, $\langle a^{-1} \rangle \subseteq \langle a \rangle$. By definition, $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$. So, $\langle a \rangle \subseteq \langle a^{-1} \rangle$.
- In Z_k , $\langle m \rangle \cap \langle n \rangle = \text{lcm}(m, n)$. In Z_k , $\langle m \rangle \cap \langle n \rangle = \text{lcm}(m, n) \pmod k$. If $|a| = \infty$, $\langle a^m \rangle \cap \langle a^n \rangle = a^{\text{lcm}(m, n)}$. If

- $|a| = k$, $\langle a^m \rangle \cap \langle a^n \rangle = a^{\text{lcm}(m,n)} \pmod k$.
15. $|g|$ divides 12 is equivalent to $g^{12} = e$. So, if $a^{12} = e$ and $b^{12} = e$, then $(ab^{-1})^{12} = a^{12}(b^{12})^{-1} = ee^{-1} = e$. The same argument works when 12 is replaced by any integer (see Exercise 51 of Chapter 3).
 17. By Theorem 4.2 we have $|\langle a^6 \rangle| = n/\gcd(n, 6)$. Since n is odd and $\langle a^6 \rangle$ is a proper subgroup we have $\gcd(n, 6) = 3$. So, $|\langle a^6 \rangle| = n/3$.
 19. If $|a^2| = 3$, $|a|$ is 3 or 6. If $|a^2| = 4$, $|a| = 8$.
 21. For every a and b we have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.
 23. Let $|a| = m$, $|b| = n$, $|ab| = k$ and $\gcd(m, n) = d$. Then $\text{lcm}(m, n) = mn/d$ and $(ab)^{mn/d} = (a^m)^{n/d}(b^{n/d})^m = ee = e$ so k divides $\text{lcm}(m, n)$. So, if $d > 1$, then $k < mn$. If $d = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$ because $|\langle a \rangle \cap \langle b \rangle|$ divides both $|\langle a \rangle|$ and $|\langle b \rangle|$. We also have $e = (ab)^k = a^k b^k$ and therefore $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = \{e\}$.
 25. Exercise 31 in Chapter 3 tells us that H is a subgroup of the cyclic group of n rotations in D_n . So, by Theorem 4.3, H is cyclic.
 27. one
 29. **a.** $|a|$ divides 12. **b.** $|a|$ divides m . **c.** By Theorem 4.3, $|a| = 1, 2, 3, 4, 6, 8, 12$, or 24. If $|a| = 2$, then $a^8 = (a^2)^4 = e^4 = e$. A similar argument eliminates all other possibilities except 24.
 31. Yes, by Theorem 4.3. The subgroups of Z are of the form $\langle n \rangle = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$, $n = 0, 1, 2, 3, \dots$. The subgroups of $\langle a \rangle$ are of the form $\langle a^n \rangle$ for $n = 0, 1, 2, 3, \dots$.
 33. For the first part, apply Theorem 4.3 to the subgroup of rotations; D_n has n elements of order 2 when n is odd and $n + 1$ elements of order 2 when n is even.
 35. See Example 16 of Chapter 2.
 37. 1000000, 3000000, 5000000, 7000000;
- by Theorem 4.3, $\langle 1000000 \rangle$ is the unique subgroup of order 8, and only those on the list are generators. $a^{1000000}, a^{3000000}, a^{5000000}, a^{7000000}$; by Theorem 4.3, $\langle a^{1000000} \rangle$ is the unique subgroup of order 8, and only those on the list are generators.
39. Let $G = \{a_1, a_2, \dots, a_k\}$. Now let $|a_i| = n_i$. Consider $n = n_1 n_2 \cdots n_k$.
 41. The lattice is a vertical line with successive terms from top to bottom $\langle p^0 \rangle, \langle p^1 \rangle, \langle p^3 \rangle, \dots, \langle p^{n-1} \rangle, \langle 0 \rangle$.
 43. Suppose that a/b generates e positive rationals under multiplication. Because $\langle a/b \rangle = \langle (a/b)^{-1} \rangle = \langle b/a \rangle$ we may assume that $1 < a/b$. Then from $1 < a/b < (a/b)^2 < (a/b)^3 < \dots$, we see that $\langle a/b \rangle$ does not contain any rational number k strictly between 1 and ab .
 45. For 7, use Z_{2^6} . For n , use $Z_{2^{n-1}}$.
 47. Suppose that $|ab| = n$. Then $(ab)^n = e$ implies that $b^n = a^{-n} \in \langle a \rangle$, which is finite. Thus $b^n = e$.
 49. 50; 10
 51. All divisors of 60
 53. The argument given in the proof of the corollary to Theorem 4.4 shows that in an infinite group, the number of elements of finite order n is a multiple of $\phi(n)$ or there is an infinite number of elements of order n .
 55. It follows from Example 16 in Chapter 2 and Example 15 in Chapter 0 that the group $H = \langle \cos(360^\circ/n) + i \sin(360^\circ/n) \rangle$ is a cyclic group of order n and every member of this group satisfies $x^n - 1 = 0$. Moreover, since every element of order n satisfies $x^n - 1 = 0$ and there can be at most n such elements, all complex numbers of order n are in H . Thus, by Theorem 4.4, $\mathbf{C}^*$ has exactly $\phi(n)$ elements of order n .
 57. Let $x \in Z(G)$ and $|x| = p$ where p is prime. Say $y \in G$ with $|y| = q$ where q is prime. Then $(xy)^{pq} = e$ and therefore $|xy| = 1, p$, or q . If $|xy| = 1$, then $p = q$. If $|xy| = p$, then $e = (xy)^p = y^p$ and q divides p . Thus,

- $q = p$. A similar argument applies if $|xy| = q$.
59. An infinite cyclic group does not have an element of prime order. A finite cyclic group can have only one subgroup for each divisor of its order. A subgroup of order p has exactly $p - 1$ elements of order p . Another element of order p would give another subgroup of order p .
61. $1 \cdot 4, 3 \cdot 4, 7 \cdot 4, 9 \cdot 4; x^4, (x^4)^3, (x^4)^7, (x^4)^9$
63. 1 of order 1; 33 of order 2; 2 of order 3; 10 of order 11; 20 of order 33
65. 1, 2, 10, 20. In general, if an Abelian group contains cyclic subgroups of order m and n where m and n are relatively prime, then it contains subgroups of order d for each divisor d of mn .
67. Say a and b are distinct elements of order 2. If a and b commute, then ab is a third element of order 2. If a and b do not commute, then aba is a third element of order 2.
69. Use Exercise 38 of Chapter 3 and Theorem 4.3.
71. 1 and 2.
73. Suppose that G has 14 elements of order 3. Let $a \in G$ and $a \neq e$. Let $b \in G$ and $b \notin \langle a \rangle$. Then, by cancellation,
 $H = \{a^i b^j \mid i, j \text{ are } 0, 1, 2\}$ has exactly nine elements and is closed and therefore is a subgroup of G . Let $c \in G$ and $c \notin H$. Then, by cancellation, the nine expressions of the form $a^i b^j c$ where i, j are 0, 1, 2 are distinct and have no overlap with the nine elements of H . But that gives 18 elements in G .
75. 12 or 60; 48
77. 3; 2; 6
79. Since $|e| = 1$, H is nonempty. Assume $a, b \in H$ and let $|a| = m$ and $|b| = n$. Then $(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = ee = e$. So, $|ab|$ divides mn . Since mn is odd, so is $|ab|$.
81. See Example 7 in Chapter 3.
83. Observe that $n^2 - 1 = -1$ and n are in $U(n^2 - 1)$ and have order 2. (It follows from the Corollary of Theorem 0.2 in Chapter 0 that n is relatively prime to both $n - 1$ and $n + 1$) Thus $\{\pm 1, \pm n\}$ is closed and therefore is a subgroup.
85. Observe that among the integers from 1 to p^n , the p^{n-1} integers $p, 2p, 3p, \dots, p^{n-1}p$ are exactly the ones that are not relatively prime to p .
87. Let $d_1, d_2, \dots, d_k$ be the distinct positive divisors of n and for each i from 1 to k let $D_i = \{x \in Z_n \mid |x| = d_i\}$. By Theorem 4.3 and the definition of order each element of Z_n is in exactly one D_i . So, $n = |D_1| + |D_2| + \dots + |D_k|$ and by Theorem 4.4 $|D_i| = \phi(d_i)$.
89. First note that $x \neq e$. If $x^3 = x^5$, then $x^2 = e$. By Corollary 2 Theorem 4.1 and Theorem 4.3 we then have $|x|$ divides both 2 and 15. Thus $|x| = 1$ and $x = e$. If $x^3 = x^9$, then $x^6 = e$ and therefore $|x|$ divides 6 and 15. This implies that $|x| = 3$. Then $|x^{13}| = |x(x^3)^4| = |x| = 3$. If $x^5 = x^9$, then $x^4 = e$ and $|x|$ divides both 4 and 15, and therefore $x = e$.

Chapter 5

Mistakes are often the best teachers.

JAMES A. FROUDE

- $\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$
 - $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}$
 - $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}$
- a. (15)(234) b. (124)(35)(6) c. (1423)
- a. 3 b. 12 c. 6 d. 6 e. 12 f. 2
- 12
- $((14562)(2345)(136)(235))^{10} = ((153)(46))^{10} = (135)^{10}(46)^{10} = (153)$.
- even; odd
- Say $S = \{s_1, \dots, s_n\}$ and ϕ is one-to-one from S to S . Then $\phi(s_1), \dots, \phi(s_n)$ are all distinct and all in S so $\phi(S) = S$. On the other hand, if $\phi(s_i) = \phi(s_j)$ for some $i \neq j$, then $\phi(S)$ has at most $n - 1$ members. The

- mapping from Z to Z that takes x to $2x$ is one-to-one but not onto.
15. Suppose that α can be written as a product of m 2-cycles and β can be written as a product of n 2-cycles. Then $\alpha\beta$ can be written as a product of $m+n$ 2-cycles. Now observe that $m+n$ is even if and only if m and n are both even or both odd.
 17. n is odd.
 19. If α is the product of m 2-cycles and β is the product of n 2-cycles then $\alpha^{-5}\beta\alpha^3$ is the product of $8m+n$ and $8m+n$ is odd if and only if n is odd.
 21. even.
 23. For S_6 , the possible orders are 1, 2, 3, 4, 5, 6; for A_6 , 1, 2, 3, 4, 5; for A_7 , 1, 2, 3, 4, 5, 6, 7.
 25. Since $|\beta| = 21$, we have $n = 16$.
 27. Suppose H contains at least one odd permutation, σ . Imitate the proof of Theorem 5.7 with σ in place of (12).
 29. The identity is even; the set is not closed.
 31. $(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)/(2 \cdot 2 \cdot 2 \cdot 2 \cdot 4!)$
 33. In A_6 elements of order 2 in disjoint cycle form must be the product of two 2-cycles. So the number of elements of order 2 is $6 \cdot 5 \cdot 4 \cdot 3/(2 \cdot 2 \cdot 2)$.
 35. Since $|x^5| = 5$, we know $|x| = 25$. One solution is (1, 6, 7, 8, 9, 2, 10, 11, 13, 3, 14, 15, 16, 17, 4, 18, 19, 20, 21, 5, 22, 23, 24, 25). The number of solutions is $20!$.
 37. 180; 75
 39. In S_7 , $\beta = (2457136)$. In S_9 , $\beta = (2457136)$ or $\beta = (2457136)(89)$.
 41. Since $|(a_1a_2a_3a_4)(a_5a_6)| = 4$ such an x would have order 8. But the elements in S_{10} of order 8 are 8-cycles or the disjoint product of 8-cycle and a 2-cycle. In both cases the square of such an element is the product of two 4-cycles.
 43. Let $\alpha, \beta \in \text{stab}(a)$. Then $\alpha\beta(a) = \alpha(\beta(a)) = \alpha(a) = a$. Also, $\alpha(a) = a$ implies $\alpha^{-1}(\alpha(a)) = \alpha^{-1}(a)$ or $a = \alpha^{-1}(a)$.
 45. The Finite Subgroup Test shows that H is a subgroup. $|H| = 2(n-2)!$.
 47. The first part follows directly from Corollary 3 of Theorem 4.2. For the second part look at (123456).
 49. Let $\alpha = (123)$ and $\beta = (145)$.
 51. $(123)(12) \neq (12)(123)$ in S_n ($n \geq 3$).
 53. An even number of 2-cycles followed by an even number of 2-cycles gives an even number of 2-cycles in all. So the Finite Subgroup Test is verified.
 55. $\langle (1234); \{(1), (12), (34), (12)(34)\} \rangle$.
 57. R_0, R_{180}, H, V
 59. The permutation corresponding to the rotation of $360/n$ degrees, $(1, 2, \dots, n)$, is an even permutation so all rotations are even. Labeling consecutive vertices of a regular 5-gon 1, 2, 3, 4, 5 the even permutation $(14)(23)(5)$ is the reflection that fixes 5 and switches vertices 1 and 4 and 2 and 3. Multiplying the n rotations by this reflection yields all n reflections. There is no reflection in D_7 since their disjoint cycle form is a 1-cycle and three 2-cycles, which is an odd permutation.
 61. Since $(1234)^2$ is in B_n it is non-empty. If $\alpha = \alpha_1\alpha_2 \cdots \alpha_i$ and $\beta = \beta_1\beta_2 \cdots \beta_j$ where i and j are even and all the α 's and β 's are 4-cycles, then $\alpha\beta = \alpha_1\alpha_2 \cdots \alpha_i\beta_1\beta_2 \cdots \beta_j$ is the product of $i+j$ 4-cycles and $i+j$ is even. So, by the Finite Subgroup Test B_n is a subgroup. To show that B_n is a subgroup of A_n note that 4-cycles are odd permutations and the product of any two odd permutations is even. So, for the product of any even number of 4-cycles the product of the first two 4-cycles is even, then the product of the next two 4-cycles is even, and so on. This proves that B_n is a subgroup of A_n .
 63. By the previous exercise B_n contains all 3-cycles in A_n . By Exercise 60 every element of A_n is a 3-cycle or a product of 3-cycles. Since 3-cycles are even permutations any product of them is an even permutation.
 65. Cycle decomposition shows that any nonidentity element of A_5 is a 5-cycle,

- a 3-cycle, or a product of a pair of disjoint 2-cycles. Then, observe that there are $(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)/5 = 24$ group elements of the form $(abcde)$, $(5 \cdot 4 \cdot 3)/3 = 20$ group elements of the form (abc) , and $(5 \cdot 4 \cdot 3 \cdot 2)/(2 \cdot 2 \cdot 2) = 15$ group elements of the form $(ab)(cd)$.
67. If α has odd order k and α is an odd permutation, then $\epsilon = \alpha^k$ would be odd.
 69. The product is the n -cycle $(1, n, 2, n-1, 3, n-2, \dots, (n-1)/2, (n+3)/2, (n+1)/2)$. Labeling the vertices of a regular n -gon in consecutive order 1 through n counterclockwise we can think of $(12 \cdots n)$ as a $360/n$ degree rotation and $(2, n)(3, n-1) \cdots ((n+1)/2, (n+3)/2)$ as reflection through the vertex labeled 1 to the midpoint of the opposite edge.
 71. Verifying that $a * \sigma(b) \neq b * \sigma(a)$ is done by examining all cases. To prove the general case, observe that $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ can be written in the form $\sigma^i(a) * \sigma(\sigma^i(b)) \neq \sigma^i(b) * \sigma(\sigma^i(a))$, which is the case already done. If a transposition were not detected, then $\sigma(a_1) * \cdots * \sigma^i(a_i) * \sigma^{i+1}(a_{i+1}) * \cdots * \sigma^n(a_n) = \sigma(a_1) * \cdots * \sigma^i(a_{i+1}) * \sigma^{i+1}(a_i) * \cdots * \sigma^n(a_n)$, which implies $\sigma^i(a_i) * \sigma^{i+1}(a_{i+1}) = \sigma^i(a_{i+1}) * \sigma^{i+1}(a_i)$.
 73. By Theorem 5.4 it is enough to prove that every 2-cycle can be expressed as a product of elements of the form $(1k)$. To this end, observe that if $a \neq 1, b \neq 1$, then $(ab) = (1a)(1b)(1a)$.
 75. By case-by-case analysis, H is a subgroup for $n = 1, 2, 3$, and 4. For $n \geq 5$, observe that $(12)(34)$ and $(12)(35)$ belong to H but their product does not.
 77. The product of an element of $Z(A_4)$ of order 2 and an element of A_4 of order 3 would have order 6. But A_4 has no element of order 6.
 79. TAAKTPKSTOOPEDN

Chapter 6

Think and you won't sink.

B. C. FORBES, *Epigrams*

1. Try $n \rightarrow 2n$.
3. $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$.
5. The mapping $\phi(x) = (3/2)x$ is an isomorphism from G onto H . Multiplication is not preserved since $\phi(4) = 6$ but $\phi(2)\phi(2) = 3 \cdot 3 = 9$. When $G = \langle m \rangle$ and $H = \langle n \rangle$ the mapping $\phi(x) = (n/m)x$ is an isomorphism from G onto H .
7. D_{12} has an element of order 12 and S_4 does not; D_{12} has an element of order 6 and S_4 does not; D_{12} has exactly 2 elements of order 4 and S_4 has more than 2; $|Z(D_6)| = 2$ whereas $|Z(S_4)| = 1$.
9. Since $T_e(x) = ex = x$ for all x , T_e is the identity. For the second part, observe that $T_g \circ (T_g)^{-1} = T_e = T_{gg^{-1}} = T_g \circ T_{g^{-1}}$ and cancel.
11. $3\bar{a} - 2\bar{b}$.
13. For any x in the group, we have $(\phi_g \phi_h)(x) = \phi_g(\phi_h(x)) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x)$.
15. $\phi_{R_{90}}$ and ϕ_{R_0} disagree on H ; $\phi_{R_{90}}$ and ϕ_H disagree on R_{90} ; $\phi_{R_{90}}$ and ϕ_D disagree on R_{90} . The remaining cases are similar.
17. Let $\alpha \in \text{Aut}(G)$. We show that α^{-1} is operation-preserving: $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$ if and only if $\alpha(\alpha^{-1}(xy)) = \alpha(\alpha^{-1}(x)\alpha^{-1}(y))$, that is, if and only if $xy = \alpha(\alpha^{-1}(x))\alpha(\alpha^{-1}(y)) = xy$. So α^{-1} is operation-preserving. That $\text{Inn}(G)$ is a group follows from the equation $\phi_g \phi_h = \phi_{gh}$.
19. Note that for $n > 1$, $(\phi_a)^n = (\phi_a)^{n-1}\phi_a$ so an induction argument gives $(\phi_a)^n = (\phi_a)^{n-1}\phi_a = \phi_{a^{n-1}}\phi_a$. Thus $(\phi_{a^{n-1}}\phi_a)(x) = \phi_{a^{n-1}}(\phi_a(x)) = \phi_{a^{n-1}}(axa^{-1}) = a^{n-1}(axa^{-1})(a^{n-1})^{-1} =$

- $a^{n-1}(axa^{-1})(a^{-n+1}) = a^n xa^{-n} = \phi_{a^n}(x)$. To handle the case where n is negative we note that $\phi_e = \phi_{a^n a^{-n}} = \phi_{a^n} \phi_{a^{-n}} = \phi_{a^n} (\phi_a)^{-n}$ (because $-n$ is positive). Solving for ϕ_{a^n} we obtain $\phi_{a^n} = (\phi_a)^n$.
21. Since $b = \phi(a) = a\phi(1)$, it follows that $\phi(1) = a^{-1}b$ and therefore $\phi(x) = a^{-1}bx$. [Here a^{-1} is the multiplicative inverse of $a \bmod n$, which exists because $a \in U(n)$.]
 23. Note that both H and K are isomorphic to the group of all permutations on four symbols, which is isomorphic to S_4 . The same is true when 5 is replaced by n , since both H and K are isomorphic to S_{n-1} .
 25. Recall that, when n is even, $Z(D_n) = \{R_0, R_{180}\}$. Since R_{180} and $\phi(R_{180})$ are not the identity and belong to $Z(D_n)$, they must be equal.
 27. $Z_{60}; D_{60}$
 29. See Example 16 of Chapter 2.
 31. That α is one-to-one follows from the fact that r^{-1} exists modulo n . The operation-preserving condition is Exercise 11 in Chapter 0.
 33. By Part 1 of Theorem 6.2, we have $\phi(a^n) = \phi(a)^n = \gamma(a)^n = \gamma(a^n)$ thus ϕ and γ agree on all elements of $\langle a \rangle$.
 35. First observe that because $2^5 = 10 = -1$ we have $|2| = 10$. So, by parts 4 and 2 of Theorem 6.1, the mapping that takes $\phi(x) = 2^x$ is an isomorphism.
 37. $T_g(x) = T_g(y)$ if and only if $gx = gy$ or $x = y$. This shows that T_g is a one-to-one function. Let $y \in G$. Then $T_g(g^{-1}y) = y$, so that T_g is onto.
 39. Apply the appropriate definitions.
 41. See Exercise 43 in Chapter 4.
 43. Try $a + bi \rightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.
 45. Yes, by Cayley's Theorem.
 47. Observe that $\phi_g(y) = gyg^{-1}$ and $\phi_{zg}(y) = zgy(zg)^{-1} = zgyg^{-1}z^{-1} = gyg^{-1}$ since $z \in Z(G)$. So, $\phi_g = \phi_{zg}$.
 49. $\phi_g = \phi_h$ implies $g x g^{-1} = h x h^{-1}$ for all x . This implies $h^{-1} g x (h^{-1} g)^{-1} = x$, and therefore $h^{-1} g \in Z(G)$.
 51. By Exercise 49 $\phi_\alpha = \phi_\beta$ implies $\beta^{-1} \alpha$ is in $Z(S_n)$ and by Exercise 70 in Chapter 5, $Z(S_n) = \{\epsilon\}$.
 53. Since both ϕ and γ take e to itself, H is not empty. Assume a and b belong to H . Then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = \gamma(a)\gamma(b)^{-1} = \gamma(a)\gamma(b^{-1}) = \gamma(ab^{-1})$. Thus, ab^{-1} is in H .
 55. Two of many are $(12)H(12) = \{(1), (235), (253), (16)(35), (16)(23), (16)(25)\}$; $(123)H(123)^{-1} = \{(1), (152), (125), (15)(36), (25)(36), (12)(36)\}$.
 57. Since -1 is the unique element of $\mathbf{C}^*$ of order 2, $\phi(-1) = -1$. Since i and $-i$ are the only elements of $\mathbf{C}^*$ of order 4, $\phi(i) = i$ or $-i$.
 59. Z_{120}, D_{60}, S_5 . Z_{120} is Abelian, the other two are not. D_{60} has an element of order 60 and S_5 does not.
 61. For the first part use $D = R_{90}V$ and $H = R_{90}D$. For the second part use $H = R_{180}V$.
 63. $T_{R_{90}} = (R_0 R_{90} R_{180} R_{270})(H D' V D)$.
 65. The first statement follows from the fact that every element of D_n has the form $(R_{360/n})^i$ or $(R_{360/n})^i F$. Because α must map an element of order n to an element of order n $R_{360/n}$ must map to $(R_{360/n})^i$ where $i \in U(n)$. Moreover, F must map to a reflection (see Exercise 20). Thus we have at most $n|U(n)|$ choices.
 67. In both cases H is isomorphic to the set of all even permutations of the set of four integers so it is isomorphic to A_4 .
 69. Consider the mapping $\phi(x) = x^2$ and note that 2 is not in the image.
 71. Use the fact that if $a > 0$, then $a = \sqrt{a}\sqrt{a}$. For the second part, use the first part together with the fact that the inverse of an automorphism is an automorphism.
 73. Say ϕ is an isomorphism from Q to R^+ and ϕ takes 1 to a . It follows that the integer r maps to a^r . Then $a = \phi(1) = \phi(s \frac{1}{s}) = \phi(\frac{1}{s} + \cdots + \frac{1}{s}) = \phi(\frac{1}{s})^s$

and therefore $a^{\frac{1}{s}} = \phi(\frac{1}{s})$. Thus the rational r/s maps to $a^{r/s}$. But $a^{r/s} \neq a^\pi$ for any rational number r/s .

75. Send each even permutation in S_n to itself. Send each odd permutation α in S_n to $(n+1, n+2)\alpha$. This does not contradict Theorem 5.5 because the subgroup is merely isomorphic to A_{n+2} , not the same as A_{n+2} . In particular, this example shows that an isomorphism from one permutation group to another permutation group need not preserve oddness.

Chapter 7

Use missteps as stepping stones to deeper understanding and greater achievement.

SUSAN TAYLOR

- For the general case the distinct left cosets are $H, 1+H, 2+H$, an eclipses $n-1+H$.
- a.** yes **b.** yes **c.** no
- For $\langle a^5 \rangle$ there are 5: $\langle a^5 \rangle, a\langle a^5 \rangle, a^2\langle a^5 \rangle, a^3\langle a^5 \rangle, a^4\langle a^5 \rangle$. By Corollary 2 of Theorem 4.2, for $\langle a^4 \rangle = \langle a^2 \rangle$ there are two left cosets: $\langle a^2 \rangle, a\langle a^2 \rangle$.
- Suppose that $H \neq \langle 3 \rangle$. Let $a \in H$ but a not in $\langle 3 \rangle$. Then $a + \langle 3 \rangle = 1 + \langle 3 \rangle$ or $a + \langle 3 \rangle = 2 + \langle 3 \rangle$. If $a + \langle 3 \rangle = 1 + \langle 3 \rangle$ then $1 \in H$ and $H = Z$. If $a + \langle 3 \rangle = 2 + \langle 3 \rangle$ then both 2 and 3 belong to H and therefore $3-2=1$ belongs to H .
- Let ga belong to $g(H \cap K)$, where a is in $H \cap K$. Then by definition ga is in $gH \cap gK$. Now let $x \in gH \cap gK$. Then $x = gh$ for some $h \in H$, and $x = gk$ for some $k \in K$. Cancellation then gives $h = k$. Thus, $x \in g(H \cap K)$.
- Suppose that $h \in H$ and $h < 0$. Then $h\mathbf{R}^+ \subseteq hH = H$. But $h\mathbf{R}^+$ is the set of all negative real numbers. Thus, $H = \mathbf{R}^*$.
- 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60
- Use Lagrange's Theorem (Theorem 7.1) and Corollary 3.
- By Exercise 16, we have $5^6 \bmod 7 = 1$. So, using mod 7, we have $5^{15} = 5^6 \cdot 5^6 \cdot 5^2 \cdot 5 = 1 \cdot 1 \cdot 4 \cdot 5 = 6$; $7^{13} \bmod 11 = 2$.
- Use Corollary 4 of Lagrange's Theorem (Theorem 7.1) together with Theorem 0.2.
- First observe that for all $n \geq 3$ the subgroup of rotations of D_n is isomorphic to Z_n . If n is even let F be any reflection in D_n . Then the set $\{R_0, R_{180}, F, FR_{180}\}$ is closed and therefore a subgroup of order 4. Now suppose that D_n has a subgroup K of order 4. By Lagrange, $|D_n| = 2n = 4k$ and therefore $n = 2k$.
- Since G has odd order, no element can have order 2. Thus, for each $x \neq e$, we know that $x \neq x^{-1}$. So, we can write the product of all the elements in the form $ea_1a_1^{-1}a_2a_2^{-1}\cdots a_na_n^{-1} = e$.
- Let $e \neq g \in G$. Then $|g| = 5$ or 25. If $|g| = 25$ for some g , then G is cyclic. If there is no such g , then $|g| = 1$ or 5 for all g .
- 1, 3, 11, 33. If some x has order 33, then $|x^{11}| = 3$. Otherwise, use the Corollary to Theorem 4.4.
- If the group is cyclic Theorem 4.3 says that it has exactly one subgroup of order 5. So, assume the group is not cyclic. Not all of the 54 nonidentity elements can have order 5 because the number of elements of order 5 is a multiple of $\phi(5) = 4$. So the group has an element of order 11. Also since $\phi(11) = 10$ the number of elements of order 11 is a multiple of 10. If there were more than 10 the group would have distinct subgroups H and K of order 11. But then $|HK| = |H||K|/|H \cap K| = 121$. So, excluding the subgroup of order 11, there are 44 elements remaining and each has order 5. That gives us exactly 11 subgroups of order 5.
- By Lagrange's Theorem every element in G has an order that is a divisor of n . So, we can partition the n elements of G according to their orders. For

- each divisor d of n let m_d be the number elements in G of order d . By our assumption m_d is $\phi(d)$ where ϕ is the Euler phi function. (If there were more than $\phi(d)$ elements of order d in G then G would have at least 2 subgroups of order d .) So $n = \sum m_d$ where d ranges over all divisors d of n . We also have from Exercise 87 of Chapter 4 that $n = \sum \phi(d)$ where d ranges over all divisors d of n . This proves that each $n_d = \phi(d)$. In particular, $m_n \neq 0$.
33. Suppose that H and K are distinct subgroups of order m . Then $|HK| = |H||K| = \frac{m \cdot m}{|H \cap K|} \leq 2m$ and therefore $\frac{m}{2} \leq |H \cap K|$. Since m is odd and H and K are distinct we know that $\frac{m}{2} < |H \cap K| < m$ and that $|H \cap K|$ divides m . This is impossible.
35. Observe that $|G : H| = |G|/|H|$, $|G : K| = |G|/|K|$, and $|K : H| = |K|/|H|$.
37. Since the reflections in a dihedral group have order 2, the generators of the subgroups of orders 12 and 20 must be rotations. The smallest rotation subgroup of a dihedral group that contains rotations of orders 12 and 20 must have order divisible by 12 and 20 and therefore must be a multiple of 60. So, D_{60} is the smallest such dihedral group.
39. Let a have order 3 and b be an element of order 3 not in $\langle a \rangle$. Then $\langle a \rangle \langle b \rangle$ is a subgroup of G of order 9. Now use Lagrange's Theorem.
41. By Corollary 5 of Theorem 7.1, the statement is true for $n = 1$. For the sake of induction assume that $a^{p^k} = a$. Then $a^{p^{k+1}} = a^{p^k} a^p = a^p = a$.
43. Let $a \in G$ and $|a| = 5$. Then the set $\langle a \rangle H$ has exactly $5 \cdot |H|/|\langle a \rangle \cap H|$ elements and $|\langle a \rangle \cap H|$ divides $|\langle a \rangle| = 5$. It follows that $|\langle a \rangle \cap H| = 5$ and therefore $\langle a \rangle \cap H = \langle a \rangle$.
45. First observe that by Corollary 2 of Lagrange's Theorem every positive integer k with the property that $x^k = e$ for all x in G is a common multiple of orders of all the elements in G . So, d is the least common multiple of the orders of the elements of G . Since $|G|$ is a common multiple of the orders of all the elements of G it follows directly from the division algorithm (Theorem 0.1) that $|G|$ is divisible by d .
47. Let G be a finite Abelian group. The case G has 0 or 1 element of order 2 corresponds to the cases $n = 0$ and $n = 1$. Let $H = \{x \in G \mid x^2 = e\}$. Then H is a subgroup of G that consists of the identity and all elements of order 2. It suffices to prove $|H| = 2^n$. If G has at least two elements of order 2, say a_1 and b . Then $H_1 = \{e, a_1, b, a_1 b\}$ is a subgroup of order 2^2 . If $H_1 = H$, we are done. If not, let $a_2 \in H$ but not in H_1 . Then $H_2 = H_1 \cup \langle a_2 \rangle H_1$ is a subgroup of H of order $2|H_1| = 2^3$. If $H_2 = H$ we are done. If not, let $a_3 \in H$ but not in H_2 and let $H_3 = H_2 \cup \langle a_3 \rangle H_2$. We can continue this argument until we reach H .
49. Consider the mapping from G to G defined by $\phi(x) = x^2$ and let $|G| = 2k + 1$. Use the observation that $x = xe = xx^{2k+1} = x^{2k+2} = (x^2)^{k+1}$ to prove that ϕ is one-to-one and Exercise 13 of Chapter 5 to show that ϕ is onto.
51. If H and K are distinct subgroups of order p^m then $np^m = |G| \geq |HK| = |H||K|/|H \cap K| \geq p^m p^m / p^{m-1} = pp^m$, which is obviously false.
53. Let G be the group and H the unique subgroup of order q . We must show that G has an element of order pq . Let a belong to G but not in H . By Lagrange, $|a| = p$ or pq . If $|a| = pq$ we are done. So, we may assume that a has order p and we let $K = \langle a \rangle$. Then $H \cup K$ accounts for $q + p - 1$ elements (the identity appears twice). Pick $b \in G$ but b not one of the elements in $H \cup K$. Then $L = \langle b \rangle$ is a subgroup of G of order p different than K . Then $K \cap L = \{e\}$ because $|K \cap L|$ must

- divide p and is not p . By Theorem 7.2 $|KL| = |K||L|/|K \cap L| = (p \cdot p)/1 = p^2$. But a group of order pq with $q < p$ cannot have p^2 elements. This shows that b cannot have order p . So $|b| = pq$.
55. Use Theorem 7.2.
57. 50
59. Let K be the set of all even permutations in H . Since K is closed it is a subgroup of H . If $K = H$, we are done. If not, let α be an element in H that is odd. Then αK must be the set of all odd permutations in H , for if β is any odd permutation in H , we have $\alpha^{-1}\beta \in H$, which means $\beta \in H$. Thus $|H| = |K \cup \alpha K| = 2|K|$.
61. Suppose that H is a subgroup of A_5 of order 30. We claim that H contains all 20 elements of A_5 that have order 3. To verify this, assume that there is some α in A_5 of order 3 that is not in H . Then $A_5 = H \cup \alpha H$. It follows that $\alpha^2 H = H$ or $\alpha^2 = \alpha H$. Since the latter implies that $\alpha \in H$, we have that $\alpha^2 H = H$, which implies that $\alpha^2 \in H$. But then $\langle \alpha \rangle = \langle \alpha^2 \rangle \subseteq H$, which is a contradiction of our assumption that α is not in H . The same argument, shows that H must contain all 24 elements of order 5. Since $|H| = 30$, we have a contradiction.
63. Say H is a subgroup of order 30. By Exercise 61 H is not a subgroup of A_5 and by Exercise 59 $H \cap A_5$ is a subgroup of A_5 of order 15. But this contradicts Exercise 62.
65. If H is a subgroup of S_5 of order 60 other than A_5 , then it follows from Theorem 7.2 that $|A_5 \cap H| = 30$, which contradicts Exercise 61.
67. Certainly, $a \in \text{orb}_G(a)$. Now suppose that $c \in \text{orb}_G(a) \cap \text{orb}_G(b)$. Then $c = \alpha(a)$ and $c = \beta(b)$ for some α and β , and therefore $(\beta^{-1}\alpha)(a) = b$. So, if $x \in \text{orb}_G(b)$, then $x = \gamma(b) = (\gamma\beta^{-1}\alpha)(a)$ for some γ . This proves that $\text{orb}_G(b) \subseteq \text{orb}_G(a)$. By symmetry, $\text{orb}_G(a) \subseteq \text{orb}_G(b)$.
69. **a.** $\text{stab}_G(1) = \{(1), (24)(56)\}; \text{orb}_G(1) = \{1, 2, 3, 4\}$
- b.** $\text{stab}_G(3) = \{(1), (24)(56)\}; \text{orb}_G(3) = \{3, 4, 1, 2\}$
- c.** $\text{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\}; \text{orb}_G(5) = \{5, 6\}$
71. Suppose that $B \in G$ and $\det(B) = 2$. Then $\det(A^{-1}B) = 1$, so that $A^{-1}B \in H$ and therefore $B \in AH$. Conversely, for any $Ah \in AH$ we have $\det(Ah) = (\det(A))(\det(B)) = 2 \cdot 1 = 2$.
73. It is the set of all permutations that carry face 2 to face 1.
75. $aH = bH$ if and only if $\det(a) = \pm \det(b)$.
77. Closure of the set follows from using $\alpha\beta^2 = \beta^2\beta^3$.

Chapter 8

Practice isn't the thing you do when you're good. It's the thing you do that makes you good.

MALCOLM GLADWELL

- Closure and associativity in the product follow from the closure and associativity in each component. The identity in the product is the n -tuple with the identity in each component. The inverse of $(g_1, g_2, \dots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.
- Use $g \rightarrow (g, e_H)$ and $h \rightarrow (e_G, h)$.
- To show that $Z \oplus Z$ is not cyclic, note that $(a, b+1) \notin \langle (a, b) \rangle$.
- Use $(g_1, g_2) \rightarrow (g_2, g_1)$. In general, $G_1 \oplus G_2 \cdots \oplus G_n$ is isomorphic to the external direct product of any rearrangement of $G_1, G_2, \dots, G_n$.
- In $Z_6 \oplus Z_2$ take $\langle (1, 0) \rangle$ and $\langle (2, 1) \rangle$. In $Z_{pm} \oplus Z_p$ take $\langle (1, 0) \rangle$ and $\langle (p, 1) \rangle$.
- There are 12 elements of order 4. Observe by Theorem 4.4 that as long as d divides n , the number of elements of order d in a cyclic group depends only on d . So, in both $Z_{8000000}$ and Z_4 there are $\phi(4) = 2$ elements of order 4 and $\phi(2) = 1$ element of order 2. Similarly for $Z_m \oplus Z_n$.
- Z_{n^2} and $Z_n \oplus Z_n$.
- Try $a + bi \rightarrow (a, b)$.

17. Use Exercise 3 and Theorem 4.3.
19. $\langle m/r \rangle \oplus \langle n/s \rangle$
21. Since $\langle \langle g, h \rangle \rangle \subseteq \langle g \rangle \oplus \langle h \rangle$, a necessary and sufficient condition for equality is that $\text{lcm}(|g|, |h|) = |\langle g, h \rangle| = |\langle g \rangle \oplus \langle h \rangle| = |g||h|$. This is equivalent to $\text{gcd}(|g|, |h|) = 1$.
23. $(m+2)(n+1) - 1$ of order 2; $2(n+1)$ of order 4.
25. Map $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to (a, b, c, d) . Let $\mathbf{R}^k$ denote $\mathbf{R} \oplus \mathbf{R} \oplus \cdots \oplus \mathbf{R}$ (k factors). Then the group of $m \times n$ matrices under addition is isomorphic to $\mathbf{R}^{mn}$.
27. $(g, g)(h, h)^{-1} = (gh^{-1}, gh^{-1})$. When $G = \mathbf{R}$, $G \oplus G$ is the plane and H is the line $y = x$.
29. $\langle \langle 3, 0 \rangle \rangle, \langle \langle 3, 1 \rangle \rangle, \langle \langle 3, 2 \rangle \rangle, \langle \langle 0, 1 \rangle \rangle$
31. $\text{lcm}(6, 10, 15) = 30$; $\text{lcm}(n_1, n_2, \dots, n_k)$.
33. Observe that $Z_4 \oplus Z_3 \oplus Z_2 \approx Z_4 \oplus Z_6 \approx \langle 25 \rangle \oplus \langle 10 \rangle$. Also $Z_4 \oplus Z_3 \oplus Z_2 \approx Z_2 \oplus Z_{12} \approx \langle 50 \rangle \oplus \langle 5 \rangle$.
35. Let F be a reflection in D_3 . $\{R_0, F\} \oplus \{R_0, R_{180}, H, V\}$.
37. Compare the number of elements of order 2 in each group.
39. The mapping $\phi(3^m 6^n) = (m, n)$ is an isomorphism. The mapping $\phi(3^m 9^n) = (m, n)$ is not well-defined, since $\phi(3^2 9^0) \neq \phi(3^0 9^1)$.
41. In both cases they are the same.
43. $\mathbf{C}^*$ has only one element of order 2 whereas $Z_m \oplus Z_n$ has exactly one element of order 2 if and only if it is cyclic, which is true if and only if $\text{gcd}(m, n) = 1$.
45. 12
47. $\text{Aut}(U(25)) \approx \text{Aut}(Z_{20}) \approx U(20) \approx U(4) \oplus U(5) \approx Z_2 \oplus Z_4$
49. $2^k - 1$; $2^t - 1$, where t is the number of the integers $n_1, n_2, \dots, n_k$ that are even.
51. For part **a**, there are $\phi(18) = 6$. Two are $\phi(x) = (x, x)$ and $\phi(x) = (x, 2x)$. For part **b**, there are none because $Z_2 \oplus Z_3 \oplus Z_3$ is not cyclic.
53. Since $(2, 0)$ has order 2, it must map to an element in Z_{12} of order 2. The only such element in Z_{12} is 6. The isomorphism defined by $(1, 1) x \rightarrow 5x$ with $x = 6$ takes $(2, 0)$ to 6. Since $(1, 0)$ has order 4, it must map to an element in Z_{12} of order 4. The only such elements in Z_{12} are 3 and 9. The first case occurs for the isomorphism defined by $(1, 1) x \rightarrow 7x$ with $x = 9$ [recall that $(1, 1)$ is a generator of $Z_4 \oplus Z_3$]; the second case occurs for the isomorphism defined by $(1, 1) x \rightarrow 5x$ with $x = 9$.
55. Since $a \in Z_m$ and $b \in Z_n$, we know that $|a|$ divides m and $|b|$ divides n . So, $|(a, b)| = \text{lcm}(|a|, |b|)$ divides $\text{lcm}(m, n)$.
57. Z, Z_3, Z_4, Z_6
59. Observe that every nonidentity element of $Z_p \oplus Z_p$ has order p and each subgroup of order p contains $p - 1$ of them. So, there are exactly $(p^2 - 1)/(p - 1) = p + 1$ subgroups of order p .
61. Look at $Z \oplus Z_2$.
63. $U(165) \approx U(11) \oplus U(15) \approx U(5) \oplus U(33) \approx U(3) \oplus U(55) \approx U(3) \oplus U(5) \oplus U(11)$
65. $U(2n) \approx U(2) \oplus U(n) = \{1\} \oplus U(n) \approx U(n)$.
67. Mimic the analysis for elements of order 12 in $U(105)$ in this chapter. The number is 14.
69. $A_4 \oplus Z_4$ has exactly 7 elements of order 2 whereas $D_{12} \oplus Z_2$ has more.
71. $Z \oplus D_4$.
73. Observe that $U(55)$ and $U(75)$ are both isomorphic to $Z_4 \oplus Z_{10}$ and $U(144)$ and $U(140)$ are both isomorphic to $Z_2 \oplus Z_4 \oplus Z_6$.
75. From Theorem 6.5 we know $\text{Aut}(Z_n) \approx U(n)$. So, $n = 8$ and 12 are the two smallest.
77. Since $U(pq) \approx U(p) \oplus U(q) \approx Z_{p-1} \oplus Z_{q-1}$ it follows that $k = \text{lcm}(p - 1, q - 1)$.
79. $Z_{p^{n-1}}$
81. $U_8(40) \approx U(5) \approx Z_4$.
83. $U_5(140) \approx U(28)$; $U_4(140) \approx U(35) \approx Z_4 \oplus Z_6$.
85. If $x \in U_{st}(n)$ then $x \in U(n)$ and $x - 1 = stm$ for some m . So,

- $x - 1 = s(tm)$ and $x - 1 = t(sm)$. If $x \in U_s(n) \cap U_t(n)$ then $x \in U(n)$ and both s and t divide $x - 1$. So, by Exercise 6 in Chapter 0, st divides $x - 1$.
87. $Z_2 \oplus Z_2$.
89. Since $5 \cdot 29 = 1 \pmod{36}$, we have that $s = 29$. So, we need to compute $34^{29} \pmod{2701}$. The result is 1415, which converts to NO.
91. Because the block 2505 exceeds the modulus 2263, sending $2505^e \pmod{2263}$ is the same as sending $242^e \pmod{2263}$ which decodes as 242 instead of 2505.

Chapter 9

There's a mighty big difference between good, sound reasons and reasons that sound good.

BURTON HILLIS

1. No.
3. $HR_{90} = R_{270}H$; $DR_{270} = R_{90}D$; $R_{90}V = VR_{270}$
5. Say $i < j$ and let $h \in H_i \cap H_j$. Then $h \in H_1H_2 \cdots H_i \cdots H_{j-1} \cap H_j = \{e\}$.
7. Recall that if A and B are matrices, then $\det(ABA^{-1}) = (\det A)(\det B)(\det A)^{-1}$.
9. Let $x \in G$. If $x \in H$, then $xH = H = Hx$. If $x \notin H$, then xH is the set of elements in G , not in H . But Hx is also the set of elements in G , not in H .
11. Let $G = \langle a \rangle$. Then $G/H = \langle aH \rangle$
13. in H .
15. $|9H| = 2$; $|13H| = 4$.
17. $1 + \langle 3.5 \rangle$.
19. Observe that in a group G if $|a| = 2$ and $\{e, a\}$ is a normal subgroup then $axa^{-1} = a$ for all x in G . Thus $a \in Z(G)$. So, the only normal subgroup of order 2 in D_n is $\{R_0, R_{180}\}$ when n is even.
21. By Theorem 9.5, the group has an element a of order 3 and an element b of order 11. Then $|ab| = 33$. For the general case use induction.
23. 4; no
25. Z_8 .
27. Yes; no
29. The subgroups would have orders 2 or 4 and therefore are Abelian. But the internal direct products of Abelian groups are Abelian.
31. Certainly, every nonzero real number is of the form $\pm r$, where r is a positive real number. Real numbers commute, and $\mathbf{R}^+ \cap \{1, -1\} = \{1\}$.
33. No. If $G = H \times K$, then $|g| = \text{lcm}(|h|, |k|)$, provided that $|h|$ and $|k|$ are finite. If $|h|$ or $|k|$ is infinite, so is $|g|$.
35. For the first question, note that $\langle 3 \rangle \cap \langle 6 \rangle = \{1\}$ and $\langle 3 \rangle \langle 6 \rangle \cap \langle 10 \rangle = \{1\}$. For the second question, observe that $12 = 3^{-1}6^2$. So $\langle 3 \rangle \langle 6 \rangle \cap \langle 12 \rangle \neq \{1\}$.
37. Say $|g| = n$. Then $(gH)^n = g^nH = eH = H$. Now use Corollary 2 to Theorem 4.1.
39. Let x be in G and h be in H . Then $xhx^{-1}H = (xh)x^{-1}H = (xh)Hx^{-1}H = xhHx^{-1}H = xHx^{-1}H = xH = H$, so xhx^{-1} belongs to H .
41. Suppose that H is a proper subgroup of Q of index n . Then Q/H is a finite group of order n . By Corollary 4 of Theorem 7.1, we know that for every x in Q we have nx is in H . Now observe that the function $f(x) = nx$ maps Q onto Q . So, $Q \subseteq H$.
43. Take $G = Z_6$, $H = \{0, 3\}$, $a = 1$, and $b = 9$.
45. Normality follows directly from Theorem 4.3 and Example 7.
47. In general, if p is a prime and $|H| = p^2m$ and $|K| = p^2n$ where $\gcd(m, n) = 1$, Then $H \cap K = 1, p$, or p^2 . So, by Corollary 3 of Theorem 7.1 and Theorem 9.7, $H \cap K$ is Abelian.
49. Use the G/Z Theorem.
51. Suppose that K is a normal subgroup of G and let $gH \in G/H$ and $kH \in K/H$. Then $gHkH(gH)^{-1} = gHkHg^{-1}H = gkg^{-1}H \in K/H$. Now suppose that K/H is a normal subgroup of G/H and let $g \in G$ and $k \in K$. Then

- $gkg^{-1}H = gHkHg^{-1}H = gHkH(gH)^{-1} \in K/H$ so $gkg^{-1} \in K$.
53. Say H has index n . Then $(\mathbf{R}^*)^n = \{x^n \mid x \in \mathbf{R}^*\} \subseteq H$. If n is odd, then $(\mathbf{R}^*)^n = \mathbf{R}^*$; if n is even, then $(\mathbf{R}^*)^n = \mathbf{R}^+$. So, $H = \mathbf{R}^*$ or $H = \mathbf{R}^+$.
55. Use Exercise 9 and observe that $VK \neq KV$.
57. G has elements of orders 1, 2, 3, and 6.
59. Let $N = \langle a \rangle$, $H = \langle a^k \rangle$, and x be in G . Then, $x(a^k)^m x^{-1} = (xa^m x^{-1})^k = (a^r)^k = (a^k)^r \in H$.
61. $\gcd(|x|, |G/H|) = 1$ implies $\gcd(|xH|, |G/H|) = 1$. But $|xH|$ divides $|G/H|$. Thus $|xH| = 1$ and therefore $xH = H$.
63. Use Example 5 and Lagrange's Theorem.
65. Observe that for every positive integer n , $(1+i)^n$ is not a real number. So, $(1+i) \in \mathbf{R}^*$ has infinite order.
67. Use Theorems 9.4 and 9.3.
69. Because $|g| = 16$ implies that $|gH|$ divides 16 it suffices to show that $(gH)^4$ is not H . Suppose that $(gH)^4 = g^4 H = H$. Then g^4 is in H . But then e, g^4 , and g^8 are in H , which is a contradiction. In the general case, say $|gH| = k$. Then $(gH)^k = g^k H = H$. So, g^k is in H and therefore $|g^k| = 1$ or 2. It follows that $k = 2n$ or n .
71. Use Theorem 9.3 and Theorem 7.3.
73. If A_5 had a normal subgroup of order 2 then, by Exercise 72, it would have an element of the form $(ab)(cd)$ that commutes with every element of A_5 . Try (abc) .
75. Note that $U(72) \approx U(8) \oplus U(9) \approx U_9(72) \oplus U_8(72) \approx \oplus Z_2 \oplus Z_2 \oplus Z_6$. $|U_9(72)| = 4$, $|U_8(72)| = 6$, and $|(19)U_8(72)| = 12$.
77. First recall that A_5 contains $5 \cdot 4 \cdot 3/3 = 20$ elements of order 3. Let α be any of these 20. Then, since $|A_5/H| = 5$, we have that $H = (\alpha^2 H)^5 = \alpha^{10} H = \alpha H$. But this means that all 20 elements of order 5 in A_5 are in H , which has order 12.
79. Because $51H = H$ we have $153H = (3 \cdot 51)H = 3(51H) = 3H$.
81. Let $|gH| = d$ and $|g| = m$. We know by Exercise 37 that $|gH|$ divides $|g|$ and, because $g^d \in H$, we also know that $|g^d| = m/d$ divides $|H|$. This means that $m/d = 1$.
83. By definition, every element of G can be written in the form $a_{j_1} a_{j_2} \dots a_{j_k}$ where $a_{j_1}, a_{j_2}, \dots, a_{j_k} \in \langle a_1, a_2, \dots, a_n \rangle$. Then $gH = a_{j_1} H a_{j_2} H \dots a_{j_k} H$.
85. Since G is Abelian the subgroups $H_1, H_2, \dots, H_k$ are normal in G . By assumption, $G = H_1 H_2 \dots H_k$. So, all that remains to prove is that for all $i = 2, 3, \dots, k-1$ we have $H_1 H_2 \dots H_i \cap H_{i+1} = \{e\}$. But if $x \in H_1 H_2 \dots H_i \cap H_{i+1}$ and $x \neq e$ then x can be written in the two distinct forms $h_1 h_2 \dots h_i e \dots e$ ($k-i$ e terms) and $e \dots e h_{i+1} e \dots e$ (i e terms on the left and $k-(i+1)$ e terms on the right) and each $h_j \in H_j$. This contradicts our assumption about G .
87. We know from Theorem 9.7 that $G/Z(G) \approx Z_{p^2}$ or $Z_p \oplus Z_p$ and from the G/Z Theorem (Theorem 9.3) Z_{p^2} is ruled out.
89. By Theorem 7.2 and Example 5 in Chapter 9, if H and K were distinct subgroups of order p^2 then HK would be a subgroup of order p^3 or p^4 , which contradicts Lagrange.
91. If G is cyclic then Theorem 4.4 says that G has exactly one element of order 2. If G is not cyclic, let a be any non-identity element of G and b be any element of G not in $\langle a \rangle$. Then $\langle a \rangle \times \langle b \rangle$ is isomorphic to a group of the form $Z_{2^s} \oplus Z_{2^t}$ where s and t are positive. But then G has at least three elements of order 2. The appropriate generalization is: "An Abelian group of order p^n for a prime p and some positive integer n is cyclic if and only if it has exactly $p-1$ elements of order p ."
93. Observe that for every two distinct primes p and q we have $pH \neq qH$.

(For if there are integers a, b, c, d such that $pa^2/b^2 = qc^2/d^2$ then p occurs an odd number of times on the left side of $pa^2d^2 = qb^2c^2$ but an even number of times on the right side). Every nonidentity element in Q/H has order 2.

Chapter 10

It's always helpful to learn from your mistakes, because then your mistakes seem worthwhile.

GARRY MARSHALL

1. Note that $\det(AB) = (\det A)(\det B)$.
3. Note that $(f + g)' = f' + g'$.
5. Observe that $(xy)^r = x^r y^r$. Odd values of r yield an isomorphism. For even values of r the kernel is $\{1, -1\}$.
7. $(\sigma\phi)(g_1g_2) = \sigma(\phi(g_1g_2)) = \sigma(\phi(g_1)\phi(g_2)) = \sigma(\phi(g_1))\sigma(\phi(g_2)) = (\sigma\phi)(g_1)(\sigma\phi)(g_2)$. $\text{Ker } \phi$ is a normal subgroup of $\text{Ker } \sigma\phi$.
 $|H|/|K| = |\text{Ker } \sigma\phi : \text{Ker } \phi|$.
9. $\phi((g, h)(g', h')) = \phi((gg', hh')) = gg' = \phi((g, h))\phi((g', h'))$. The kernel is $\{(e, h) | h \in H\}$.
11. Consider $\phi: Z \oplus Z \rightarrow Z_a \oplus Z_b$ given by $\phi((x, y)) = (x \bmod a, y \bmod b)$ and use Theorem 10.3.
13. $(a, b) \rightarrow b$ is a homomorphism from $A \oplus B$ onto B with kernel $A \oplus \{e\}$.
15. 3, 13, 23
17. Suppose ϕ is such a homomorphism. By Theorem 10.3,
 $\text{Ker } \phi = \langle(8, 1)\rangle, \langle(0, 1)\rangle$, or $\langle(8, 0)\rangle$. In these cases, $(1, 0) + \text{Ker } \phi$ has order either 16 or 8. So, $(Z_{16} \oplus Z_2)/\text{Ker } \phi$ is not isomorphic to $Z_4 \oplus Z_4$.
19. Since $|\text{Ker } \phi|$ is not 1 and divides 17, ϕ is the trivial map.
21. $\langle 5 \rangle$
23. $|\phi^{-1}(H)| = |H||\text{Ker } \phi|$.
25. 4 onto; 10 to
27. For each k with $0 \leq k \leq n-1$, the mapping $1 \rightarrow k$ determines a homomorphism.
29. Use Theorem 10.3 and properties 5, 7, and 9 of Theorem 10.2.
31. $\phi^{-1}(7) = 7 \text{ Ker } \phi = \{7, 17\}$
33. $11\text{Ker } \phi$
35. $\phi((a, b) + (c, d)) = \phi((a + c, b + d)) = (a + c) - (b + d) = a - b + c - d = \phi((a, b)) + \phi((c, d))$.
 $\text{Ker } \phi = \{(a, a) \mid a \in Z\}$.
 $\phi^{-1}(3) = \{(a + 3, a) \mid a \in Z\}$.
37. Use the property of complex numbers that $|xy| = |x||y|$ and the First Isomorphism Theorem.
39. $\phi(xy) = (xy)^6 = x^6y^6 = \phi(x)\phi(y)$.
 $\text{Ker } \phi = \langle 60^\circ + i \sin 60^\circ \rangle$.
41. Since $\phi(e) = e = e^{-2}$, $e \in H$. If $a \in H$, then $\phi(ab) = \phi(a)\phi(b) = a^{-2}b^{-2} = (ab)^{-2} \in H$. Also, $\phi(a^{-1}) = \phi(a)^{-1} = (a^{-2})^{-1} = (a^{-1})^{-2} \in H$. If $\phi(x) = x^3$ and $a \in H$, then $\phi(a) = a^3 = a^{-2}$ implies that $a^5 = e$. Thus, $|a| = 5$ or 1.
43. Property 2 of Theorem 10.2 handles the 2^m case. Suppose that there is a homomorphism from $G = Z_{2^m} \oplus Z_{2^n}$ onto $Z_2 \oplus Z_2 \oplus Z_2$ where m and n are at least 1 and let H be the kernel. We may assume that $m + n \geq 3$. Then $|H| = 2^{m+n-3}$. Because every nonidentity element of G/H has order 2 we know that
 $((1, 0)H)^2 = (2, 0)H = H$ and
 $((0, 1)H)^2 = (0, 2)H = H$. This means that $H_1 = \langle(2, 0)\rangle$ and $H_2 = \langle(0, 2)\rangle$ are subgroups of H . Then H_1H_2 is also a subgroup of H . But
 $|H_1H_2| = 2^{m-1} \cdot 2^{n-1} = 2^{m+n-2}$ exceeds $|H| = 2^{m+n-3}$. The argument works for any prime p .
45. Since S_4/H is a group of order 6 but has no element of order 6 (because S_4 does not have one) it follows from Theorems 7.3 and 10.3 that S_4/H is isomorphic S_3 .
47. It follows from Exercise 11 in Chapter 0 that the mapping ϕ from $U(st)$ to $U(s)$ given by $\phi(x) = x \bmod s$ is a homomorphism. Since $\text{Ker } \phi = U_s(st)$ we have by Theorem 10.3 that $U(st)/U_s(st)$ is isomorphic to a subgroup of $U(s)$. To see that ϕ is onto note that it follows from Theorem 8.3 that
 $|U(st)/U_s(st)| = |U(st)|/|U_s(st)| =$

- $|U(s) \oplus U(t)|/|U(t)| = |U(s)||U(t)|/|U(t)| = |U(s)|.$
49. Show that the mapping from K to KN/N given by $k \rightarrow kN$ is an onto homomorphism with kernel $K \cap N$.
 51. Since the eight elements of A_4 of order 3 must map to an element of order that divides 3, by Lagrange's Theorem, each of them must map to the identity. But then the kernel has at least 8 elements and its order divides 12. So, the kernel has order 12.
 53. $D_4, \{e\}, Z_2, Z_2 \oplus Z_2$
 55. It is divisible by 10. 10 can be replaced by any positive integer.
 57. It is infinite. Look at Z .
 59. Let γ be the natural homomorphism from G onto G/N . Let $\bar{H}$ be a subgroup of G/N and let $\gamma^{-1}(\bar{H}) = H$. Then H is a subgroup of G and $H/N = \gamma(H) = \gamma(\gamma^{-1}(\bar{H})) = \bar{H}$.
 61. The mapping $g \rightarrow \phi_g$ is a homomorphism with kernel $Z(G)$.
 63. $(f+g)(3) = f(3) + g(3)$. The kernel is the set of elements in $Z[x]$ whose graphs pass through the point $(3, 0)$. 3 can be replaced by any integer.
 65. Let g belong to G . Since $\phi(g)$ belongs to $Z_2 \oplus Z_2 = \langle(1, 0)\rangle \cup \langle(0, 1)\rangle \cup \langle(1, 1)\rangle$, it follows that $G = \phi^{-1}(\langle(1, 0)\rangle) \cup \phi^{-1}(\langle(0, 1)\rangle) \cup \phi^{-1}(\langle(1, 1)\rangle)$. Moreover, each of these three subgroups is proper and by property 9 of Theorem 10.2 normal.
 67. $\phi(a, b) = (2a, b)$.
 69. It fails because 5 does divide $|\text{Aut}(Z_{11})| = 10$.
 71. Mimic Example 19.
 73. Let ϕ be a homomorphism from S_3 to G . Since $|\phi(S_3)|$ must divide 6, we have that $|\phi(S_3)| = 1, 2, 3$, or 6. In the first case, ϕ maps every element to 0. If $|\phi(S_3)| = 2$, then n is even and ϕ maps the even permutations to 0 and the odd permutations to an element of order 2. The case that $|\phi(S_3)| = 3$ cannot occur, because it implies that $\text{Ker } \phi$ is a normal subgroup of order 2, whereas S_3 has no normal subgroup of

order 2. The case that $|\phi(S_3)| = 6$ cannot occur, because it implies that ϕ is an isomorphism from a non-Abelian group to an Abelian group.

75. $\phi(zw) = z^2w^2 = \phi(z)\phi(w)$. $\text{Ker } \phi = \{1, -1\}$ and, because ϕ is onto $\mathbf{C}^*$ we have by Theorem 10.3, $\mathbf{C}^*/\{1, -1\}$ is isomorphic to $\mathbf{C}^*$. When $\mathbf{C}^*$ is replaced by $\mathbf{R}^*$ we have that ϕ is onto $\mathbf{R}^+$ and by Theorem 10.3, $\mathbf{R}^*/\{1, -1\}$ is isomorphic to $\mathbf{R}^+$.

Chapter 11

Ever tried. Ever failed. No matter. Try again. Fail again. Fail better.

SAMUEL BECKETT

1. $n = 4; Z_4, Z_2 \oplus Z_2$
3. $n = 36; Z_9 \oplus Z_4, Z_3 \oplus Z_3 \oplus Z_4, Z_9 \oplus Z_2 \oplus Z_2, Z_3 \oplus Z_3 \oplus Z_2 \oplus Z_2$
5. The only Abelian groups of order 45 are Z_{45} and $Z_3 \oplus Z_3 \oplus Z_5$. In the first group, $|3| = 15$; in the second one, $|(1, 1, 1)| = 15$. $Z_3 \oplus Z_3 \oplus Z_5$ does not have an element of order 9.
7. $Z_9 \oplus Z_3 \oplus Z_4; Z_9 \oplus Z_3 \oplus Z_2 \oplus Z_2$
9. $Z_4 \oplus Z_2 \oplus Z_3 \oplus Z_5$
11. By the Fundamental Theorem, any finite Abelian group G is isomorphic to some direct product of cyclic groups of prime-power order. Now go across the direct product and, for each distinct prime you have, pick off the largest factor of the prime power. Next, combine all of these into one factor (you can do this, since the subscripts are relatively prime). Let us call the order of this new factor n_1 . Now repeat this process with the remaining original factors and call the order of the resulting factor n_2 . Then n_2 divides n_1 , since each prime-power divisor of n_2 is also a prime-power divisor of n_1 . Continue in this fashion. Example: If $G \approx Z_{27} \oplus Z_3 \oplus Z_{125} \oplus Z_{25} \oplus Z_4 \oplus Z_2 \oplus Z_2$, then $G \approx Z_{27 \cdot 125 \cdot 4} \oplus Z_{3 \cdot 25 \cdot 2} \oplus Z_2$. Now note that 2 divides $3 \cdot 25 \cdot 2$ and $3 \cdot 25 \cdot 2$ divides $27 \cdot 125 \cdot 4$.

13. $Z_2 \oplus Z_2$
15. **a. 1 b. 1 c. 1 d. 1 e. 1 f.** There is a unique Abelian group of order n if and only if n is not divisible by the square of any prime.
17. This is equivalent to asking how many Abelian groups of order 16 have no elements of order 8. From the Fundamental Theorem of Finite Abelian Groups the only choices are $Z_4 \oplus Z_4$, $Z_4 \oplus Z_2 \oplus Z_2$, and $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$.
19. $Z_2 \oplus Z_2$
21. $Z_3 \oplus Z_3$
23. n is square-free (no prime factor of n occurs more than once).
25. Among the first 11 elements in the table, there are nine elements of order 4. None of the other isomorphism classes has this many.
27. $Z_4 \oplus Z_2 \oplus Z_2$; one internal direct product is $\langle 7 \rangle \times \langle 101 \rangle \times \langle 199 \rangle$.
29. Since $|\langle (2, 2) \rangle| = 8$ we know $|(Z_{16} \oplus Z_{16})/\langle (2, 2) \rangle| = 32$. Then observing that $|(1, 0) + \langle (2, 2) \rangle| = 16$ and $|(0, 1) + \langle (2, 2) \rangle| = 16$, we know that the maximum order of any element in the factor group is 16. So, the isomorphism class is $Z_{16} \oplus Z_2$.
31. 3; 6; 12
33. $Z_4 \oplus Z_4$
35. Use Theorems 11.1, 8.1, and 4.3.
37. $|\langle a \rangle K| = |a||K|/|\langle a \rangle \cap K| = |a||K| = |\bar{a}||\bar{K}|p = |\bar{G}|p = |G|$
39. By the Fundamental Theorem of Finite Abelian Groups, it suffices to show that every group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \dots \oplus Z_{p_k^{n_k}}$ is a subgroup of a U -group. Consider first a group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}}$ (p_1 and p_2 need not be distinct). By Dirichlet's Theorem, for some s and t there are distinct primes q and r such that $q = tp_1^{n_1} + 1$ and $r = sp_2^{n_2} + 1$. Then $U(qr) = U(q) \oplus U(r) \approx Z_{tp_1^{n_1}} \oplus Z_{sp_2^{n_2}}$, and this latter group contains a subgroup isomorphic to $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}}$. The general case

follows in the same way.

41. Look at D_4 .
43. If G has an element of order greater than 2, then $\phi(x) = x^{-1}$ is a nontrivial automorphism of G (see Exercise 12 of Chapter 6).
45. By Theorem 11.1 and Corollary 1 of Theorem 8.2 it suffices to do the case where $|G| = p^m$ and p is prime. Then, if G is not cyclic, it follows from Theorem 11.1 together with Theorem 4.3 that $x^p = e$ has more than p solutions.
47. First observe by direct calculations we have $|8| = |12| = |18| = |21| = |27| = 4$.

Chapter 12

Mistakes are the portals of discovery.

JAMES JOYCE

1. For any $n > 1$, the ring $M_2(Z_n)$ of 2×2 matrices with entries from Z_n is a finite noncommutative ring. The set $M_2(2Z)$ of 2×2 matrices with even integer entries is an infinite noncommutative ring that does not have a unity.
3. In $\mathbf{R}$, consider $\{n\sqrt{2} \mid n \in Z\}$.
5. **a, b**
7. In Z_p , nonzero elements have multiplicative inverses. Use them.
9. If a and b belong to the intersection, then they belong to each member of the intersection. Thus, $a - b$ and ab belong to each member of the intersection. So, $a - b$ and ab belong to the intersection.
11. Rule 3: $0 = 0(-b) = (a + (-a))(-b) = a(-b) + (-a)(-b) = -(ab) + (-a)(-b)$. So, $ab = (-a)(-b)$.
Rule 4: $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.
Rule 5: Use rule 2.
Rule 6: Use rule 3.
13. *Hint:* Z is a cyclic group under addition, and every subgroup of a cyclic group is cyclic.
15. For positive m and n , observe that

- $(m \cdot a)(n \cdot b) = (a + a + \cdots + a)(b + b + \cdots + b) = (ab + ab + \cdots + ab)$, where the last term has mn summands. Similar arguments apply in the remaining cases.
17. From Exercise 15, we have $(n \cdot a)(m \cdot a) = (nm) \cdot a^2 = (mn) \cdot a^2 = (m \cdot a)(n \cdot a)$.
19. Let a, b belong to the center. Then $(a - b)x = ax - bx = xa - xb = x(a - b)$. Also, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.
21. $(x_1, \dots, x_n)(a_1, \dots, a_n) = (x_1, \dots, x_n)$ for all x_i in R_i if and only if $x_i a_i = x_i$ for all x_i in R_i and $i = 1, \dots, n$.
23. $\{1, -1, i, -i\}$
25. $f(x) = 1$ and $g(x) = -1$.
27. If a is a unit, then $b = a(a^{-1}b)$.
29. Consider $a^{-1} - a^{-2}b$.
31. $0^1 = 0$ so the set is nonempty. Let $a^m = 0$ and $b^n = 0$. We may assume that $m \geq n$. Then in the expansion of $(a - b)^{2m}$ each term has an expression of the form $a^{2m-i}b^i$. So when $i = 0, 1, \dots, m$ we have $a^{2m-i} = 0$ and when $i = m + 1, m + 2, \dots, 2m$ we have $b^i = 0$. So, all terms in the expansion are 0. (This argument also works when the exponent of $(a - b)$ is $m + n - 1$.) Finally, if r is any element in the ring then $(ab)^m = a^m b^m = 0$.
33. Try the ring $M_2(Z)$.
35. By inspection, R is closed under addition and multiplication. The elements $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ do not commute.
- For the general case use $m \times m$ matrices with the first $m - 1$ columns all 0 and the last column any elements from Z_n .
37. Observe that $-x = (-x)^4 = x^4 = x$.
39. For Z_6 , use $n = 3$. For Z_{10} , use $n = 5$. Say $m = p^2 t$, where p is a prime. Then $(pt)^n = 0$ in Z_m , since m divides $(pt)^n$.
41. Every subgroup of Z_n is closed under multiplication.
43. $ara - asa = a(r - s)a$. $(ara)(asa) = ara^2sa = arsa$. $a1a = a^2 = 1$, so $1 \in S$.
45. The Subring Test is satisfied.
47. They satisfy the subring test but the multiplication is trivial. This is, the product of any two elements is zero.
49. Look at $(1, 0, 1)$ and $(0, 1, 1)$.
51. Observe that $n \cdot 1 - m \cdot 1 = (n - m) \cdot 1$. Also, $(n \cdot 1)(m \cdot 1) = (nm) \cdot ((1)(1)) = (nm) \cdot 1$.
53. $\{2n/3^m \mid n \in Z, m \text{ is a positive integer}\}$. This set is a ring that contains $2/3$ and is contained in every ring that contains $2/3$.
55. $(a + b)(a - b) = a^2 + ba - ab - b^2 = a^2 - b^2$ if and only if $ba - ab = 0$.
57. $Z_2 \oplus Z_2; Z_2 \oplus Z_2 \oplus \cdots$ (infinitely many copies)
59. If (a, b) is a zero-divisor in $R \oplus S$ then there is a $(c, d) \neq (0, 0)$ such that $(a, b)(c, d) = (0, 0)$. Thus $ac = 0$ and $bd = 0$. So, a or b is a zero-divisor or exactly one of a or b is 0. Conversely, if a is a zero-divisor in R then there is a $c \neq 0$ in R such that $ac = 0$. In this case $(a, b)(c, 0) = (0, 0)$. A similar argument applies if b is a zero-divisor. If $a = 0$ and $b \neq 0$ then $(a, b)(x, 0) = (0, 0)$ where x is any nonzero element in A . A similar argument applies if $a \neq 0$ and $b = 0$.
61. Fix some a in $R, a \neq 0$. Then there is a b in R such that $ab = a$. Now if x in R and $x \neq 0$ then there is an element c in R such that $ac = x$. Then $xb = acb = c(ab) = ca = x$. Thus b is the unity. To show that every nonzero element r of R has an inverse note that since $rR = R$ there is an element s in R such that $rs = b$.
63. If $\det A = \pm 1$ then by Exercise 9 in Chapter 2 A^{-1} is in $M_2(Z)$ and by definition A is a unit. On the other hand, if A is a unit in $M_2(Z)$ then $1 = \det(AA^{-1}) = (\det A)(\det A^{-1})$ where both $\det A$ and $\det A^{-1}$ are integers and units in Z . But the only units in Z are ± 1 .

Chapter 13

Mathematics is not a careful march down a well-cleared highway, but a journey into a strange wilderness, where the explorers get lost.

W. S. Anglin

1. The verifications for Example 16 follow from elementary properties of real and complex numbers. For Example 7, note that

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

For Example 8, note that $(1, 0)(0, 1) = (0, 0)$.

3. Let $ab = 0$ and $a \neq 0$. Then $ab = a \cdot 0$, so $b = 0$.
5. Let $k \in \mathbb{Z}_n$. If $\gcd(k, n) = 1$, then k is a unit. If $\gcd(k, n) = d > 1$, write $k = sd$. Then $k(n/d) = sd(n/d) = sn = 0$.
7. Let $s \in R, s \neq 0$. Consider the set $S = \{sr \mid r \in R\}$. If $S = R$, then $sr = 1$ (the unity) for some r . If $S \neq R$, then there are distinct r_1 and r_2 such that $sr_1 = sr_2$. In this case, $s(r_1 - r_2) = 0$. To see what happens when the “finite” condition is dropped, consider $\mathbb{Z}$.
9. Take $a = (1, 1, 0), b = (1, 0, 1)$, and $c = (0, 1, 1)$.
11. $(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d}$; $(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$. Thus, the set is a ring. Since $\mathbb{Z}[\sqrt{d}]$ is a subring of the ring of complex numbers, it has no zero-divisors.
13. The even integers.
15. $(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1 + a + a^2 + \cdots + a^{n-1} - a - a^2 - \cdots - a^n = 1 - a^n = 1 - 0 = 1$.
17. Suppose $a \neq 0$ and $a^n = 0$ (where we take n to be as small as possible). Then $a \cdot 0 = 0 = a^n = a \cdot a^{n-1}$, so by cancellation, $a^{n-1} = 0$.
19. If $a^2 = a$ and $b^2 = b$, then $(ab)^2 = a^2b^2 = ab$. The other cases are

similar.

21. Let $f(x) = x$ on $[-1, 0]$, $f(x) = 0$ on $(0, 1]$, $g(x) = 0$ on $[-1, 0]$, and $g(x) = x$ on $(0, 1]$. Then $f(x)$ and $g(x)$ are in R and $f(x)g(x) = 0$ on $[-1, 1]$.
23. Suppose that a is an idempotent and $a^n = 0$. By the previous exercise, $a = 0$.
25. The generators are: $2 + i, 1 + 2i, 1 + i, 2 + 2i$.
27. $a^2 = a$ implies $a(a - 1) = 0$. So if a is a unit, $a - 1 = 0$ and $a = 1$.
29. See Theorems 3.1 and 12.3.
31. Note that $ab = 1$ implies $aba = a$. Thus $0 = aba - a = a(ba - 1)$. So, $ba - 1 = 0$.
33. A subdomain of an integral domain D is a subset of D that is an integral domain under the operations of D . To show that P is a subdomain, show that it is a subring and contains 1. Every subdomain contains 1 and is closed under addition and subtraction, so every subdomain contains P . $|P| = \text{char } D$ when $\text{char } D$ is prime and $|P|$ is infinite when $\text{char } D$ is 0.
35. Use Theorems 13.3, Lagrange’s Theorem, and Theorem 13.4.
37. By Exercise 36, 1 is the only element of an integral domain that is its own multiplicative inverse if and only if $1 = -1$. This is true only for integral domains of characteristic 2.
39. a. Since $a^3 = b^3, a^6 = b^6$. Then $a = b$ because we can cancel a^5 from both sides (since $a^5 = b^5$).
b. Use the fact that there exist integers s and t such that $1 = sn + tm$, but remember that you cannot use negative exponents in a ring.
41. Observe that F^* (the nonzero elements of F) form a group of order 31. So, for any a in F other than 0 or 1, we know by Lagrange’s Theorem that $|a| = 31$.
43. In $\mathbb{Z}_p[k]$ note that $(a + b\sqrt{k})^{-1} = \frac{1}{(a+b\sqrt{k})} \frac{(a-b\sqrt{k})}{(a-b\sqrt{k})} = \frac{a-b\sqrt{k}}{a^2-b^2k}$ exists if and only if $a^2 - b^2k \neq 0$ where $a \neq 0$ and $b \neq 0$.

45. Let $S = \{a_1, a_2, \dots, a_n\}$ be the nonzero elements of the ring. First show that $S = \{a_1 a_1, a_1 a_2, \dots, a_1 a_n\}$. Thus, $a_1 = a_1 a_i$ for some i . Then a_i is the unity, for if a_k is any element of S , we have $a_1 a_k = a_1 a_i a_k$, so that $a_1(a_k - a_i a_k) = 0$.
47. Say $|x| = n$ and $|y| = m$ with $n < m$. Consider $(nx)y = x(ny)$.
49. **a.** For $n = 2$ the Binomial Theorem gives us $(x_1 + x_2)^p = x_1^p + p x_1^{p-1} x_2 + \dots + p x_1 x_2^{p-1} + x_2^p$, where each coefficient $p!/k!(p-k)!$ of every term between x_1^p and x_2^p is divisible by p . Thus, $(x_1 + x_2)^p = x_1^p + x_2^p$. The general case follows by induction on n .
- b.** This case follows from Part a and induction on m .
- c.** Note Z_4 is a ring of characteristic 4 and $(1+1)^4 = 2^4 = 0$, but $1^4 + 1^4 = 1 + 1 = 2$.
51. Use Theorems 13.4 and 9.5 and Exercise 47.
53. $n \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ for all members of $M_2(R)$ if and only if $na = 0$ for all a in R .
55. Use Exercise 54.
57. **a.** 2 **b.** 2, 3 **c.** 2, 3, 6, 11 **d.** 2, 3, 9, 10
59. 2
61. If $a \in Z_p$ and $a^2 + 1 = 0$, then $a^2 + 1 = (a+i)(a-i) = 0$.
63. Suppose that F is a field of order 16 and K is a subfield of F of order 8. Then K^* is a subgroup of F^* and $|K^*| = 7$ and $|F^*| = 15$, which contradicts LaGrange's Theorem.
65. Use Exercise 29 and part **a** of Exercise 49.
67. $\text{char } R = 0$. For positive integer n the subring $\{0\} \oplus \{0\} \oplus \dots \oplus \{0\} \oplus \dots \oplus Z_n \oplus \{0\} \oplus \dots$ is subring of characteristic n .
69. Observe that because $u_S u_R = u_S = u_S u_S$ we have $u_S(u_R - u_S) = 0$.
71. Since a field of order 27 has characteristic 3, we have $3a = 0$ for all a . From this, we have $6a = 0$ and $5a = -a$.

73. Let $F^* = \langle a \rangle$. Then $-1 = a^n$ for some n . Thus $1 = a^{2n}$ and $|a|$ divides $2n$.

Chapter 14

The paradox of excellence is that it is built upon the foundations of necessary failure.

MATTHEW SYED

- Let $r_1 a$ and $r_2 a$ belong to $\langle a \rangle$. Then $r_1 a - r_2 a = (r_1 - r_2)a \in \langle a \rangle$. If $r \in R$ and $r_1 a \in \langle a \rangle$, then $r(r_1 a) = (rr_1)a \in \langle a \rangle$.
- Clearly, I is not empty. Now observe that $(r_1 a_1 + \dots + r_n a_n) - (s_1 a_1 + \dots + s_n a_n) = (r_1 - s_1)a_1 + \dots + (r_n - s_n)a_n \in I$. Also, if $r \in R$, then $r(r_1 a_1 + \dots + r_n a_n) = (rr_1)a_1 + \dots + (rr_n)a_n \in I$. That $I \subseteq J$ follows from closure under addition and multiplication by elements from R .
- Let $a + bi, c + di \in S$. Then $(a + bi) - (c + di) = a - c + (b - d)i$ and $b - d$ is even. Also, $(a + bi)(c + di) = ac - bd + (ad + cb)i$ and $ad + cb$ is even. Finally, $(1 + 2i)(1 + i) = -1 + 3i \notin S$.
- Suppose that s is not prime. Then we can write $s = pm$ where p is prime and $m > 1$. Then $\langle s \rangle$ is properly contained in $\langle p \rangle$ and $\langle p \rangle$ is properly contained in Z_n . So $\langle s \rangle$ is not maximal. Now suppose that s is prime and there is a divisor $t > 1$ of n such that $\langle t \rangle$ properly contains $\langle s \rangle$ (recall every subgroup of Z_n has the form $\langle k \rangle$ where k is a divisor of n .) Then $s = rt$ for some r . So we have $t = s$.
- If aR is a non-zero ideal of R we know that $aR = R$. So a belongs to R .
- Since $ar_1 - ar_2 = a(r_1 - r_2)$ and $(ar_1)r = a(r_1 r)$, $4R = \{\dots, -16, -8, 0, 8, 16, \dots\}$.
- If n is prime, use Euclid's Lemma (Chapter 0). If n is not prime, say $n = st$ where $s < n$ and $t < n$; then st belongs to nZ but s and t do not.
- a.** $a = 1$ **b.** $a = 2$ **c.** $a = \gcd(m, n)$

17. **a.** $a = 12$
b. $a = 48$. To see this, note that every element of $\langle 6 \rangle \langle 8 \rangle$ has the form $6t_1 8k_1 + 6t_2 8k_2 + \cdots + 6t_n 8k_n = 48s \in \langle 48 \rangle$. So, $\langle 6 \rangle \langle 8 \rangle \subseteq \langle 48 \rangle$. Also, since $48 \in \langle 6 \rangle \langle 8 \rangle$, we have $\langle 48 \rangle \subseteq \langle 6 \rangle \langle 8 \rangle$.
c. $a = mn$
19. Let $r \in R$. Then $r = 1r \in A$.
21. Let $u \in I$ be a unit and let $r \in R$. Then $r = r(u^{-1}u) = (ru^{-1})u \in I$.
23. Observe that $\langle 2 \rangle$ and $\langle 3 \rangle$ are the only nontrivial ideals of Z_6 , so both are maximal. More generally, Z_{pq} , where p and q are distinct primes, has exactly two maximal ideals.
25. Clearly, I is closed under subtraction. Also, if b_1, b_2, b_3 , and b_4 are even, then every entry of $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$ is even.
27. The proof that I is an ideal is the same as the case that $n = 2$ in Exercise 25. The number of elements in I is n^4 .
29. That I satisfies the ideal test follows directly from the definitions of matrix addition and multiplication. To see that R/I is field first observe that
- $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + I = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} + I = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + I.$$
- Thus we need only show that
- $$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + I \text{ has an inverse in } R/I$$
- when $a \neq 0$. To this end note that
- $$\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + I \right) \left(\begin{bmatrix} a^{-1} & 0 \\ 0 & 0 \end{bmatrix} + I \right) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + I = \left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + I \right) + \left(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + I \right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + I.$$
- $$\left(\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} + I \right)^{-1} = \begin{bmatrix} 1/2 & 0 \\ 0 & 0 \end{bmatrix} + I.$$
31. $R = \{0 + \langle 2i \rangle, 1 + \langle 2i \rangle, i + \langle 2i \rangle, 1 + i + \langle 2i \rangle\}$.
 R is not an integral domain because

$$(1 + i + \langle 2i \rangle)^2 = (1 + i)^2 + \langle 2i \rangle = 1 + 1 + \langle 2i \rangle = 0 + \langle 2i \rangle.$$

33. First note that every element of R has the form $ax + b + I$ where $a, b \in Z_5$. Since 1 and -1 are zeros of $x^2 - 1$ we know that $0 + I = x^2 - 1 + I = (x - 1 + I)(x + 1 + I)$ and that $x - 1 + I = x + 4 + I$ and $x + 1 + I$ are zero-divisors in R . Then for every nonzero c in Z_5 , $c(x + 1) + I$ and $c(x + 4) + I$ are distinct zero-divisors in R . By Exercise 7 in Chapter 13 every nonzero element of R is a unit. So, $|U(R)| = 16$. Because $|4| = 2$ and $|x| = 2$, we know that $U(R)$ is not cyclic. Next we look for the unit of maximum order. Trying various possibilities we find that $(3x + 1)^4 = 4$ and $(3x + 1)^8 = 1$. So $U(R) \approx Z_8 \oplus Z_2$.
35. Use the observation that every member of R can be written in the form $\begin{bmatrix} 2q_1 + r_1 & 2q_2 + r_2 \\ 2q_3 + r_3 & 2q_4 + r_4 \end{bmatrix}$. Then note that $\begin{bmatrix} 2q_1 + r_1 & 2q_2 + r_2 \\ 2q_3 + r_3 & 2q_4 + r_4 \end{bmatrix} + I = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I$.
37. $(br_1 + a_1) - (br_2 + a_2) = b(r_1 - r_2) + (a_1 - a_2) \in B$; $r'(br + a) = b(r'r) + r'a \in B$ since $r'a$ is in A .
39. Use Exercise 21.
41. Let a be an idempotent other than 0 or 1. Then $a^2 = a$ implies that $a(a - 1) = 0$.
43. Since every element of $\langle x \rangle$ has the form $xg(x)$, we have $\langle x \rangle \subseteq I$. If $f(x) \in I$, then $f(x) = a_n x^n + \cdots + a_1 x = x(a_n x^{n-1} + \cdots + a_1) \in \langle x \rangle$.
45. Suppose $f(x) + I \neq I$. Then $f(x) + I = f(0) + I$ and $f(0) \neq 0$. Thus,
- $$(f(x) + I)^{-1} = \frac{1}{f(0)} + I.$$

This shows that R/I is a field. Now use Theorem 14.4.

47. Since $(3+i)(3-i) = 10$, $10 + \langle 3+i \rangle = 0 + \langle 3+i \rangle$. Also,
 $i + \langle 3+i \rangle = -3 + \langle 3+i \rangle = 7 + \langle 3+i \rangle$.
 So, $Z[i]/\langle 3+i \rangle = \{k + \langle 3+i \rangle \mid k = 0, 1, \dots, 9\}$, since $1 + \langle 3+i \rangle$ has additive order 10.
49. Use Theorems 14.3 and 14.4.
51. Since every $f(x)$ in $\langle x, 2 \rangle$ has the form $f(x) = xg(x) + 2h(x)$, we have $f(0) = 2h(0)$, so that $f(x) \in I$. If $f(x) \in I$, then $f(x) = a_n x^n + \dots + a_1 x + 2k = x(a_n x^{n-1} + \dots + a_1) + 2k \in \langle x, 2 \rangle$. I is prime and maximal. $Z[x]/I$ has two elements.
53. One example is $J = \langle x^2 + 1, 2 \rangle$. To see that 1 is not in J note that if there were $f(x), g(x) \in Z[x]$ such that $(x^2 + 1)f(x) + 2g(x) = 1$ then evaluating the left side at 1 yields an even integer.
55. $3x + 1 + I$
57. Every ideal is a subgroup. Every subgroup of a cyclic group is cyclic.
59. Let I be any ideal of $R \oplus S$ and let $I_R = \{r \in R \mid (r, s) \in I \text{ for some } s \in S\}$ and $I_S = \{s \in S \mid (r, s) \in I \text{ for some } r \in R\}$. Then I_R is an ideal of R and I_S is an ideal of S . Let $I_R = \langle r \rangle$ and $I_S = \langle s \rangle$. Since, for any $(a, b) \in I$ there are elements $a' \in R$ and $b' \in S$ such that $(a, b) = (a'r, b's) = (a', b')(r, s)$, we have that $I = \langle (r, s) \rangle$.
61. Say $b, c \in \text{Ann}(A)$. Then $(b-c)a = ba - ca = 0 - 0 = 0$. Also, $(rb)a = r(ba) = r \cdot 0 = 0$.
63. **a.** $\langle 3 \rangle$ **b.** $\langle 3 \rangle$ **c.** $\langle 3 \rangle$
65. Suppose $(x + N(\langle 0 \rangle))^n = 0 + N(\langle 0 \rangle)$. We must show that $x \in N(\langle 0 \rangle)$. We know that $x^n + N(\langle 0 \rangle) = 0 + N(\langle 0 \rangle)$, so that $x^n \in N(\langle 0 \rangle)$. Then, for some m , $(x^n)^m = 0$, and therefore $x \in N(\langle 0 \rangle)$.
67. The set $Z_2[x]/\langle x^2 + x + 1 \rangle$ has only four elements and each of the nonzero ones has a multiplicative inverse. For example,
 $(x + \langle x^2 + x + 1 \rangle)(x + 1 + \langle x^2 + x + 1 \rangle) = 1 + \langle x^2 + x + 1 \rangle$.
69. $x + 2 + \langle x^2 + x + 1 \rangle$ is not zero, but its square is.
71. If f and $g \in A$, then $(f - g)(0) = f(0) - g(0)$ is even and $(f \cdot g)(0) = f(0) \cdot g(0)$ is even.
 $f(x) = \frac{1}{2} \in R$ and $g(x) = 2 \in A$, but $f(x)g(x) \notin A$.
73. *Hint:* Any ideal of R/I has the form A/I , where A is an ideal of R .
75. In Z , $\langle 2 \rangle \cap \langle 3 \rangle = \langle 6 \rangle$ is not prime.
77. According to Theorem 13.3 we need only determine the additive order of $1 + \langle 2 + i \rangle$. Since $5(1 + \langle 2 + i \rangle) = 5 + \langle 2 + i \rangle = (2 + i)(2 - i) + \langle 2 + i \rangle = 0 + \langle 2 + i \rangle$, we know that $1 + \langle 2 + i \rangle$ has order 5.
79. The set K of all polynomials whose coefficients are even is closed under subtraction and multiplication by elements from $Z[x]$ and therefore K is an ideal. By Theorem 14.3 to show that K is prime it suffices to show that $Z[x]/K$ has no zero-divisors. Suppose that $f(x) + K$ and $g(x) + K$ are nonzero elements of $Z[x]/K$. Since K absorbs all terms that have even coefficients we may assume that $f(x) = a_m x^m + \dots + a_0$ and $g(x) = b_n x^n + \dots + b_0$ are in $Z[x]$ and a_m and b_n are odd integers. Then $(f(x) + K)(g(x) + K) = a_m b_n x^{m+n} + \dots + a_0 b_0 + K$ and $a_m b_n$ is odd. So, $f(x)g(x) + K$ is nonzero.
81. Use the fact that R/I is an integral domain to show that $R/I = \{I, 1 + I\}$.
83. $\langle x \rangle \subset \langle x, 2^n \rangle \subset \langle x, 2^{n-1} \rangle \subset \dots \subset \langle x, 2 \rangle$

Chapter 15

For every problem there is a solution which is simple, clean and wrong.

H. L. MENCKEN

- Property 3 $\phi(A)$ is a subgroup because ϕ is a group homomorphism. Let $s \in S$ and $\phi(r) = s$. Then $s\phi(a) = \phi(r)\phi(a) = \phi(ra)$ and $\phi(a)s = \phi(a)\phi(r) = \phi(ar)$. Property 4: Let a and b belong to $\phi^{-1}(B)$ and r belong to R . Then $\phi(a)$ and $\phi(b)$ are

- in B . So, $\phi(a) = \phi(b) = \phi(a) + \phi(-b) = \phi(a - b) \in B$. Thus, $a - b \in B$. Also, $\phi(ra) = \phi(r)\phi(a) \in B$ and $\phi(ar) = \phi(a)\phi(r) \in B$. So, ra and $ar \in \phi^{-1}(B)$.
3. We already know the mapping is an isomorphism of groups. Let $\Phi(x + \text{Ker } \phi) = \phi(x)$. Note that $\Phi((r + \text{Ker } \phi)(s + \text{Ker } \phi)) = \Phi(rs + \text{Ker } \phi) = \phi(rs) = \phi(r)\phi(s) = \Phi(r + \text{Ker } \phi)\Phi(s + \text{Ker } \phi)$.
 5. $\phi(2 + 4) = \phi(1) = 5$, whereas $\phi(2) + \phi(4) = 0 + 0 = 0$.
 7. Observe that $(x + y)/1 = x/1 + y/1$ and $(xy)/1 = (x/1)(y/1)$.
 9. $a = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = aa = a^2$. For the example look at Z_6 .
 11. For groups, $\phi(x) = ax$ for $a = 2, 4, 6, 8$ since each of these has additive order 5. For rings, only $\phi(x) = 6x$ since 6 is the only non-zero idempotent in R .
 13. If a and $b(b \neq 0)$ belong to every member of the collection, then so do $a - b$ and ab^{-1} . Thus, by Exercise 29 in Chapter 13, the intersection is a subfield.
 15. Apply the definition.
 17. Multiplication is not preserved.
 19. Yes.
 21. The set of all polynomials passing through the point $(1, 0)$.
 23. $a = a^2$ implies that $\phi(a) = \phi(a^2) = \phi(a)\phi(a) = (\phi(a))^2$.
 25. For Z_6 to Z_6 , $1 \rightarrow 0$, $1 \rightarrow 1$, $1 \rightarrow 3$, and $1 \rightarrow 4$ each define a homomorphism. For Z_{20} to Z_{30} , $1 \rightarrow 0$, $1 \rightarrow 6$, $1 \rightarrow 15$, and $1 \rightarrow 21$ each define a homomorphism.
 27. The zero map and the identity map.
 29. Use Exercise 28.
 31. First note that every element of $R[x]/\langle x^2 \rangle$ can be written uniquely in the form $a_1x + a_0 + \langle x^2 \rangle$. Then mapping that takes $a_1x + a_0 + \langle x^2 \rangle$ to $\left\{ \begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix} \right\}$ is a ring isomorphism.
 33. First observe that $\phi((0, 1)) = \phi((1, 1)) - \phi((1, 0)) = (1, 1) - (0, 1) = (1, 0)$. Then $\phi((a, b)) = a\phi((1, 0)) + b\phi((0, 1)) =$
 $a(0, 1) + b(1, 0) = (b, a)$.
 35. Observe that an idempotent must map to an idempotent. So, $(1, 0)$ and $(0, 1)$ must map to 0 or 1. It follows that $(a, b) \rightarrow a$, $(a, b) \rightarrow b$, and $(a, b) \rightarrow 0$ are the only ring homomorphisms.
 37. Say $m = a_k a_{k-1} \cdots a_1 a_0$ and $n = b_k b_{k-1} \cdots b_1 b_0$. Then $m - n = (a_k - b_k)10^k + (a_{k-1} - b_{k-1})10^{k-1} + \cdots + (a_1 - b_1)10 + (a_0 - b_0)$. Now use the test for divisibility by 9.
 39. Use the appropriate divisibility tests.
 41. Mimic Example 8.
 43. Observe that the mapping ϕ from $Z_n[x]$ is isomorphic to Z_n given by $\phi(f(x)) = f(0)$ is a ring-homomorphism onto Z_n with kernel $\langle x \rangle$ and use Theorem 15.3.
 45. The ring homomorphism from $Z \oplus Z$ to Z given by $\phi(a, b) = a$ takes $(1, 0)$ to 1. Or define ϕ from Z_6 to Z_6 by $\phi(x) = 3x$ and let $R = Z_6$ and $S = \phi(Z_6)$. Then 3 is a zero-divisor in R and $\phi(3) = 3$ is the unity of S .
 47. Observe that $(2 \cdot 10^{75} + 2) \bmod 3 = 1$ and $(10^{100} + 1) \bmod 3 = 2 = -1 \bmod 3$.
 49. This follows directly from Theorem 13.3 and Theorem 10.1, part 3.
 51. No. The kernel must be an ideal.
 53. **a.** Suppose $ab \in \phi^{-1}(A)$. Then $\phi(a)\phi(b) \in A$, so that $a \in \phi^{-1}(A)$ or $b \in \phi^{-1}(A)$.
b. Consider the natural homomorphism from R to S/A . Then use Theorems 15.3 and 14.4.
 55. **a.** $\phi((a, b) + (a', b')) = \phi((a + a', b + b')) = a + a' = \phi((a, b)) + \phi((a', b'))$, so ϕ preserves addition. Also, $\phi((a, b)(a', b')) = \phi((aa', bb')) = aa' = \phi((a, b))\phi((a', b'))$.
b. $\phi(a) = \phi(b)$ implies that $(a, 0) = (b, 0)$, which implies that $a = b$. $\phi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$. Also, $\phi(ab) = (ab, 0) = (a, 0)(b, 0) = \phi(a)\phi(b)$.
c. Use $(r, s) \rightarrow (s, r)$.

57. The mapping $\phi(x) = (x \bmod m, x, \bmod n)$ from Z_{mn} to $Z_m \oplus Z_n$ is a ring isomorphism.
59. First note that $\phi(1) = 1$ implies that $\phi(m) = \phi(m \cdot 1) = m\phi(1) = m$. Now let $\phi(\sqrt[3]{2}) = a$. Then $2 = \phi(2) = \phi(\sqrt[3]{2}^3) = (\phi(\sqrt[3]{2}))^3$ and therefore $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$.
61. Use Exercises 52 and 60.
63. If $a/b = a'/b'$ and $c/d = c'/d'$, then $ab' = ba'$ and $cd' = dc'$. So, $ac'b'd' = (ab')(cd') = (ba')(dc') = bda'c'$. Thus, $ac/bd = a'c'/b'd'$ and therefore $(a/b)(c/d) = (a'/b')(c'/d')$.
65. First note that any field containing Z and i must contain $Q[i]$. Then prove $(a + bi)/(c + di) \in Q[i]$.
67. The subfield of E is $\{ab^{-1} | a, b \in D, b \neq 0\}$.
69. Reflexive and symmetric properties follow from the commutativity of D . For transitivity, assume $a/b \equiv c/d$ and $c/d \equiv e/f$. Then $adf = (bc)f = b(cf) = bde$, and cancellation yields $af = be$.
71. Try $ab^{-1} \rightarrow a/b$.
73. The mapping $a + bi \rightarrow a \rightarrow bi$ is a ring isomorphism of $\mathbf{C}$.
75. Certainly the unity 1 is contained in every subfield. So, if a field has characteristic p , the subfield $\{0, 1, \dots, p-1\}$ is contained in every subfield. If a field has characteristic 0, then $\{(m \cdot 1)(n \cdot 1)^{-1} | m, n \in Z, n \neq 0\}$ is a subfield contained in every subfield. This subfield is isomorphic to Q [map $(m \cdot 1)(n \cdot 1)^{-1}$ to m/n].
3. 1, 2, 4, 5
5. The only place in the proof of Theorem 16.2 and its corollaries that uses the fact the coefficients were from a field is where we used the multiplicative inverse of lead coefficient b_m of $g(x)$.
7. Note the functions defined by $f(x) = x^3, x^5, x^7, \dots$, are the same one defined by $f(x) = x$ and the ones defined by $f(x) = x^4, x^6, x^8, \dots$, are the same one defined by $f(x) = x^2$. So all such terms may be replaced by x and x^2 . In the general case note that by Fermat's Little Theorem (Corollary 5 to Theorem 7.1) the function from Z_p to Z_p defined by $g(x) = x^p$ is the same as the function $f(x) = x$ from Z_p to Z_p . So, every polynomial function with coefficients from Z_p can be written in the form $a_{p-1}x^{p-1} + \dots + a_0$ where $a_{p-1}, \dots, a_0 \in Z_p$.
9. $(x-1)^2(x-2)$
11. $4x^2 + 3x + 6$ is the quotient and $6x + 2$ is the remainder.
13. Let $f(x), g(x) \in R[x]$. By inserting terms with the coefficient 0, we may write $f(x) = a_n x^n + \dots + a_0$ and $g(x) = b_n x^n + \dots + b_0$. Then

$$\begin{aligned}\overline{\phi}(f(x) + g(x)) &= \phi(a_n + b_n)x^n + \dots + \\ &\quad \phi(a_0 + b_0) \\ &= (\phi(a_n) + \phi(b_n))x^n + \\ &\quad \dots + \phi(a_0) + \phi(b_0) \\ &= (\phi(a_n)x^n + \dots + \phi(a_0)) + \\ &\quad (\phi(b_n)x^n + \dots + \phi(b_0)) \\ &= \overline{\phi}(f(x)) + \overline{\phi}(g(x)).\end{aligned}$$

Chapter 16

You know my methods. Apply them!

SHERLOCK HOMES

*The Hound of the Baskervilles*¹

1. $f + g = 3x^4 + 2x^3 + 2x + 2$; $f \cdot g = 2x^7 + 3x^6 + x^5 + 2x^4 + 3x^2 + 2x + 2$.
15. Note that $(2x^n + 1)^2 = 1$ and $(2x^n)^2 = 0$ for all n .
17. It is its own inverse.
19. If $f(x) = a_n x^n + \dots + a_0$ and $g(x) = b_m x^m + \dots + b_0$, then $f(x) \cdot g(x) = a_n b_m x^{m+n} + \dots + a_0 b_0$.

¹Copyright © 1968 (Renewed) Sony/ATV Tunes LLC. All rights administered by Sony/ATV Music Publishing, 8 Music Square West, Nashville, TN 37203. All rights reserved. Used by permission.

21. Let m be the multiplicity of b in $q(x)$. Then we may write $f(x) = (x-a)^n(x-b)^m q'(x)$, where $q'(x)$ is in $F[x]$ and $q'(b) \neq 0$. This means that b is a zero of $f(x)$ of multiplicity at least m . If b is a zero of $f(x)$ greater than m , then b is a zero of $g(x) = f(x)/(x-b)^m = (x-a)^n q'(x)$. But then $0 = g(b) = (b-a)^n q'(b)$, and therefore $q'(b) = 0$.
23. Apply the definitions of function addition and multiplication and ring homomorphism.
25. Since $f(2) = 16 - 4 - 2 = 10$, $p = 2$ or 5.
27. By observation, $U(2)$ and $U(3)$ are cyclic. If $U(p)$ is not cyclic and $p > 3$, then by the Fundamental Theorem of Finite Abelian groups there is some prime q such that $U(p)$ has a subgroup isomorphic to $Z_q \oplus Z_q$. But the polynomial $x^q - 1$ in $Z_q[x]$ has $q^2 - 1$ zeros, which contradicts Theorem 16.3.
29. In Z_{10} , let $f(x) = 5x$. Then 0, 2, 4, 6, 8 are zeros.
31. If $(f(x)/g(x))^2 = x$ then $x^2(k(x))^2 = x(g(x))^2$. But the right side has even degree whereas the left side has odd degree.
33. Suppose that $f(x) \in D[x]$ has degree at least 1 and there is a $g(x) \in D[x]$ such that $f(x)g(x) = 1$. Then by Exercise 19 we have $0 = \deg f(x)g(x) = \deg(f(x) + \deg g(x)) \geq 1$.
35. For char 2, 1 is a zero; char 3, 2 is a zero; char $p > 3$, 3 is a zero.
37. By Theorem 16.5, $g(x) = (x-1)(x-2)$.
39. First note that $-1 = 16$ is zero. Since $x^9 + 1 = 0$ implies $x^{18} = 1$ in the group $U(17)$, for any solution a of $x^9 + 1 = 0$ in the group $U(17)$ we know that $|a|$ must divide 18 and $|a|$ must divide $|U(17)| = 16$. This gives us $|a| = 2$ and $a^9 + 1 = a + 1$ so that $a = -1$. Because $U(17)$ is cyclic, 16 is the unique element of order 2. $Q[x]/\langle x^2 + 1 \rangle$ is isomorphic to $Q(i)$.
41. Since -1 is a zero of $x^{25} + 1$, $x + 1$ is a factor. Suppose that $x^{25} + 1 = (x + 1)^2 g(x)$ for some $g(x) \in Z_{37}[x]$. Then the derivative $f'(x) = 25x^{24} = (x + 1)^2 g'(x) + g(x)2(x + 1)$. This gives $f'(-1) = 25 = 0$, which is false.
43. *Hint:* $F[x]$ is a PID. So $\langle f(x), g(x) \rangle = \langle a(x) \rangle$ for some $a(x) \in F[x]$. Thus, $a(x)$ divides both $f(x)$ and $g(x)$. This means that $a(x)$ is a constant.
45. Suppose that $I = \langle f(x) \rangle$. Then there is some $g(x) \in Z[x]$ such that $2 = f(x)g(x)$. This implies that $f(x) = \pm 2$. But $x + 2 \in I$ and is not in $\langle 2 \rangle$.
47. If $f(x) \neq g(x)$, then $\deg[f(x) - g(x)] < \deg p(x)$. But the minimum degree of any member of $\langle p(x) \rangle$ is $\deg p(x)$.
49. For any positive integer k that are at most k zeros of $x^k - 1$. So, there are at most k elements in the field that are solutions to $x^k = 1$.
51. "Long divide" $x - a$ into $f(x)$ and induct on $\deg f(x)$.
53. By Theorem 16.5, $I = \langle x - 1 \rangle$.
55. Observe that every term of $f(a)$ has the form $c_i a^i$ and $c_i a^i \bmod m = c_i b^i \bmod m$. To prove the second statement, assume that there is some integer k such that $f(k) = 0$. If k is even, then because $k \bmod 2 = 0$, we have by the first statement $0 = f(k) \bmod 2 = f(0) \bmod 2$ so that $f(0)$ is even. This shows that k is not even. If k is odd, then $k \bmod 2 = 1$, so by the first statement $f(k) = 0$ is odd. This contradiction completes the proof.
57. For any a in $U(p)$, $a^{p-1} = 1$, so every member of $U(p)$ is a zero of $x^{p-1} - 1$. Now use the Factor Theorem and a degree argument.
59. Use Exercise 58.
61. Let $x^{48} + x^{21} + a$. Since $x + 4 = x - 1 \in Z_5[x]$ from the Factor Theorem we need only find an a in Z_5 such that $f(1) = 1 + 1 + a = 0$.

63. $\mathbf{C}(x)$ (field of quotients of $\mathbf{C}[x]$).
65. Take $R = \mathbf{Z}$ and $I = \langle 2 \rangle$.
67. A solution to $x^{25} - 1 = 0$ in $\mathbf{Z}_{37}$ is a solution to $x^{25} = 1$ in $U(37)$. So, by Corollary 2 of Theorem 4.1, $|x|$ divides 25. Moreover, we must also have that $|x|$ divides $|U(37)| = 36$. So, $|x| = 1$ and therefore $x = 1$.
69. Write $f(x) = (x - a)g(x)$. Use the product rule to compute $f'(x)$.
71. Say $\deg g(x) = m$, $\deg h(x) = n$, and $g(x)$ has leading coefficient a . Let $k(x) = g(x) - ax^{m-n}h(x)$. Then $\deg k(x) < \deg g(x)$ and $h(x)$ divides $k(x)$ in $\mathbf{Z}[x]$ by induction. So, $h(x)$ divides $k(x) + ax^{m-n}h(x) = g(x)$ in $\mathbf{Z}[x]$.
73. If $f(x)$ takes on only finitely many values, then there is at least one a in $\mathbf{Z}$ with the property that $f(x) = a$ for infinitely many x in $\mathbf{Z}$. But then $g(x) = f(x) - a$ has infinitely many zeros. This contradicts Corollary 3 of Theorem 16.2.
75. Use Theorem 15.3, Theorem 14.4, and Example 14 in Chapter 14.
77. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and assume that p/q is a zero of $f(x)$, where p and q are integers and n is even. We may assume that p and q are relatively prime. Substituting p/q for x and clearing fractions, we have $a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} = -a_0 q^n$. If p is even, then the left side is even. If p is odd, then each summand on the left side is odd and since there is an even number of summands, the left side is still even. Because a_0 is odd, we then have that q is even. It follows that $a_n p^n = -(a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n)$ is even, since the right side is divisible by q . This implies that p is even. This contradicts the assumption that p and q are relatively prime.
79. Consider the remainder when x^{43} is divided by $x^2 + x + 1$.

Chapter 17

Experience enables you to recognize a mistake when you make it again.

FRANKLIN P. JONES²

- Use Theorem 17.1.
- If $f(x)$ is not primitive, then $f(x) = ag(x)$, where a is an integer greater than 1. Then a is not a unit in $\mathbf{Z}[x]$ and $f(x)$ is reducible.
- If $f(x) = g(x)h(x)$, then $af(x) = ag(x)h(x)$.
 - If $f(x) = g(x)h(x)$, then $f(ax) = g(ax)h(ax)$.
 - If $f(x) = g(x)h(x)$, then $f(x+a) = g(x+a)h(x+a)$.
 - Try $a = 1$.
- Suppose that $r + 1/r = 2k + 1$ where k is an integer. Then $r^2 - 2kr - r + 1 = 0$. It follows from Exercise 4 of this chapter that r is an integer. But the mod 2 irreducibility test shows that the polynomial $x^2 - (2k+1)x + 1$ is irreducible over $\mathbf{Q}$ and an irreducible quadratic polynomial cannot have a zero in $\mathbf{Q}$.
- Use part a Exercise 5 and clear fractions.
- Find an irreducible polynomial $p(x)$ of degree 2 over $\mathbf{Z}_5$. Then $\mathbf{Z}_5[x]/\langle p(x) \rangle$ is a field of order 25.
- Note that -1 is a zero. No, since 4 is not a prime.
- x ; $x+1$ What can you conclude about a polynomial $f(x)$ in $\mathbf{Z}[x]$ if $f(x)$ is reducible over $\mathbf{Z}_p[x]$ for every prime p (i.e., when the coefficients of $f(x)$ are reduced modulo p)?
- $f(x)$ is irreducible over $\mathbf{Q}$. Nothing.
- $|x+I| = 12$; $|x+1+I| = 48$; $(x+I)^{-1} = 3x+I$.
- Let $f(x) = x^4 + 1$ and $g(x) = f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Then $f(x)$ is irreducible over $\mathbf{Q}$ if $g(x)$ is. Eisenstein's Criterion shows that $g(x)$ is irreducible over $\mathbf{Q}$. To see that

²Copyright © 1968 (Renewed) Sony/ATV Tunes LLC. All rights administered by Sony/ATV Music Publishing, 8 Music Square West, Nashville, TN 37203. All rights reserved. Used by permission.

- $x^4 + 1$ is reducible over $\mathbf{R}$, observe that $x^8 - 1 = (x^4 + 1)(x^4 - 1)$, so any complex zero of $x^4 + 1$ is a complex zero of $x^8 - 1$. Also note that the complex zeros of $x^4 + 1$ must have order 8 (when considered as an element of $\mathbf{C}$). Let $\omega = \sqrt{2}/2 + i\sqrt{2}/2$. Then Example 2 in Chapter 16 tells us that the complex zeros of $x^4 + 1$ are $\omega, \omega^3, \omega^5$, and ω^7 , so $x^4 + 1 = (x - \omega)(x - \omega^3)(x - \omega^5)(x - \omega^7)$. But we may pair these factors up as $((x - \omega)(x - \omega^7))((x - \omega^3)(x - \omega^5)) = (x^2 - \sqrt{2}x + 1) \cdot (x^2 + \sqrt{2}x + 1)$ to factor using reals (see DeMoivre's Theorem, Example 15 in Chapter 0).
23. $(x + 3)(x + 5)(x + 6)$
25. By the Mod 2 Irreducibility Test (Theorem 17.3 with $p = 2$) it is enough to show that $x^4 + x^3 + 1$ is irreducible over Z_2 . By inspection, $x^4 + x^3 + 1$ has no zeros in Z_2 and so it has no linear factors over Z_2 . The only quadratic irreducible in $Z_2[x]$ is $x^2 + x + 1$ and it is ruled out as a factor by long division.
27. a. Consider the number of distinct expressions of the form $(x - c)(x - d)$.
b. Reduce the problem to the case considered in part a.
29. Use Exercise 28, and imitate Example 10.
31. Map $Z_3[x]$ onto $Z_3[i]$ by $f(x) \rightarrow f(i)$. This is a ring homomorphism with kernel $\langle x^2 + 1 \rangle$.
33. $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$
35. We know that $a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$. So $a_n r^n + s a_{n-1} r^{n-1} + \cdots + s^n a_0 = 0$. This shows that $s \mid a_n r^n$ and $r \mid s^n a_0$. Now use Euclid's Lemma and the fact that r and s are relatively prime.
37. Suppose that $p(x)$ can be written in the form $g(x)h(x)$ where $\deg g(x) < \deg p(x)$ and $\deg h(x) < \deg p(x)$ with $g(x), h(x) \in F[x]$. By Theorem 14.4 $F[x]/\langle p(x) \rangle$ is a field with $0 + \langle p(x) \rangle = p(x) + \langle p(x) \rangle = g(x)h(x) + \langle p(x) \rangle = (g(x) + \langle p(x) \rangle)(h(x) + \langle p(x) \rangle)$.
- Thus $g(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$ or $h(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$. This implies that $g(x) \in \langle p(x) \rangle$ or $h(x) \in \langle p(x) \rangle$. In either case we have contradicted Theorem 16.4.
39. Since $(f + g)(a) = f(a) + g(a)$ and $(f \cdot g)(a) = f(a)g(a)$, the mapping is a homomorphism. Clearly, $p(x)$ belongs to the kernel. By Theorem 17.5, $\langle p(x) \rangle$ is a maximal ideal, so the kernel is $\langle p(x) \rangle$.
41. The mapping $a \rightarrow a + \langle p(x) \rangle$ is an isomorphism.
43. $f(x)$ is primitive.

Chapter 18

If you are going through hell, keep going.

Winston Churchill

- $|a^2 - db^2| = 0$ implies $a^2 = db^2$. Thus, $a = 0 = b$, since otherwise $d = 1$ or d is divisible by the square of a prime.
- $N((a + b\sqrt{d})(a' + b'\sqrt{d})) = N(aa' + dbb' + (ab' + a'b)\sqrt{d}) = |(aa' + dbb')^2 - d(ab' + a'b)^2| = |a^2a'^2 + d^2b^2b'^2 - da^2b'^2 - da'^2b^2| = |a^2 - db^2||a'^2 - db'^2| = N(a + b\sqrt{d})N(a' + b'\sqrt{d})$.
- If $xy = 1$, then $1 = N(1) = N(xy) = N(x)N(y)$ and $N(x) = 1 = N(y)$. If $N(a + b\sqrt{d}) = 1$, then $\pm 1 = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$ and $a + b\sqrt{d}$ is a unit.
- This property follows directly from properties 2 and 3.
- Let $I = \cup I_i$. Let $a, b \in I$ and $r \in R$. Then $a \in I_i$ for some i and $b \in I_j$ for some j . Thus, $a, b \in I_k$, where $k = \max\{i, j\}$. So, $a - b \in I_k \subseteq I$ and $ra, ar \in I_k \subseteq I$.
- Clearly, $\langle ab \rangle \subseteq \langle b \rangle$. If $\langle ab \rangle = \langle b \rangle$, then $b = rab$, so that $1 = ra$ and a is a unit. If a is a unit then $b = a^{-1}(ab) \in \langle ab \rangle$. Thus $\langle b \rangle \subseteq \langle ab \rangle$.
- Say $x = a + bi$ and $y = c + di$. Then $xy = (ac - bd) + (bc + ad)i$.

So

$$d(xy) = (ac - bd)^2 + (bc + ad)^2 = (ac)^2 + (bd)^2 + (bc)^2 + (ad)^2.$$

On the other hand,

$$d(x)d(y) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2.$$

9. Suppose $a = bu$, where u is a unit. Then $d(b) \leq d(bu) = d(a)$. Also, $d(a) \leq d(au^{-1}) = d(b)$.
11. Use the fact that x is a unit if and only if $N(x) = 1$.
13. $3 \cdot 7$ and $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Mimic Example 8 to show that these are irreducible.
15. Observe that $10 = 2 \cdot 5$ and $10 = (2 - \sqrt{-6})(2 + \sqrt{-6})$ and mimic Example 8. A PID is a UFD.
17. Suppose $3 = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$ and neither is a unit. Then $9 = d(3) = d(\alpha)d(\beta)$, so that $d(\alpha) = 3$. But there are no integers such that $a^2 + b^2 = 3$. Observe that $2 = -i(1 + i)^2$ and $5 = (1 + 2i)(1 - 2i)$.
19. Use Exercise 1 with $d = -1.5$ and $1 + 2i$; 13 and $3 + 2i$; 17 and $4 + i$.
21. Mimic Example 1.
23. $(-1 + \sqrt{5})(1 + \sqrt{5}) = 4 = 2 \cdot 2$. Now use Exercise 22.
25. $m = 0$ and $n = -1$ give $q = -i$, $r = -2 - 2i$.
27. $1 = N(ab) = N(a)N(b)$, so that $N(a) = 1 = N(b)$.
29. Suppose that $bc = pt$ in $\mathbb{Z}_n$. Then there exists an integer k such that $bc = pt + kn$. This implies that p divides bc in $\mathbb{Z}$, and by Euclid's Lemma we know that p divides b or p divides c .
31. See Example 3.
33. $p|(a_1a_2 \cdots a_{n-1})a_n$ implies that $p|a_1a_2 \cdots a_{n-1}$ or $p|a_n$. Thus, by induction, p divides some a_i .
35. Use Exercise 10 and Theorem 14.4.
37. Suppose R satisfies the ascending chain condition and there is an ideal I of R that is not finitely generated.

Then pick $a_1 \in I$. Since I is not finitely generated, $\langle a_1 \rangle$ is a proper subset of I , so we may choose $a_2 \in I$ but $a_2 \notin \langle a_1 \rangle$. As before, $\langle a_1, a_2 \rangle$ is proper, so we may choose $a_3 \in I$ but $a_3 \notin \langle a_1, a_2 \rangle$. Continuing in this fashion, we obtain a chain of infinite length

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \cdots$$

Now suppose every ideal of R is finitely generated and there is a chain $I_1 \subset I_2 \subset I_3 \subset \cdots$. Let $I = \cup I_i$. Then $I = \langle a_1, a_2, \dots, a_n \rangle$.

Since $I = \cup I_i$, each a_i belongs to some member of the union, say $I_{i'}$. Letting $k = \max\{i' | i = 1, \dots, n\}$, we see that all $a_i \in I_k$. Thus, $I \subseteq I_k$ and the chain has length at most k .

39. Say $I = \langle a + bi \rangle$. Then $a^2 + b^2 + I = (a + bi)(a - bi) + I = I$ and $a^2 + b^2 \in I$. For any $c, d \in \mathbb{Z}$, let $c = q_1(a^2 + b^2) + r_1$ and $d = q_2(a^2 + b^2) + r_2$, where $0 \leq r_1, r_2 < a^2 + b^2$. Then $c + di + I = r_1 + r_2i + I$.
41. $N(6 + 2\sqrt{-7}) = 64 = N(1 + 3\sqrt{-7})$. For the other part, use Exercise 25.
43. Theorem 18.1 shows that primes are irreducible. So, assume that a is an irreducible in a UFD R and that $a|bc$ in R . We must show that $a|b$ or $a|c$. Since $a|bc$, there is an element d in R such that $bc = ad$. Now replace b, c , and d by their factorizations as a product of irreducibles and use uniqueness.
45. See Exercise 21 in Chapter 0.
47. $13 = (2 + 3i)(2 - 3i)$; $5 + i = (1 + i)((3 - 2i)$
49. The case that $I = R$ is trivial. So we can write $I = \langle a \rangle$ where a is not a zero or a unit. Let J/I be any non-trivial ideal in R/I and let $J = \langle b \rangle$. Since I properly contains I we have that $a = br$ where r is not a unit. Then from Theorem 18.3 we know that a can be written uniquely (up to associates) as a product of irreducibles in R . So there are only finite possibilities for b .

Chapter 19

All things are difficult before they are easy.

THOMAS FULLER

1. $\{a5^{2/3} + b5^{1/3} + c \mid a, b, c \in \mathbb{Q}\}$.
3. $\mathbb{Q}(\sqrt{-3})$
5. $\mathbb{Q}(\sqrt{-3})$
7. Since $ac + b \in F(c)$ we have $F(ac + b) \subseteq F(c)$. But $c = a^{-1}(ac + b) - a^{-1}b$, so $F(c) \subseteq F(ac + b)$.
9. $a^5 = a^2 + a + 1$; $a^{-2} = a^2 + a + 1$; $a^{100} = a^2$
11. The set of all expressions of the form
$$(a_n\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_0)/(b_m\pi^m + b_{m-1}\pi^{m-1} + \cdots + b_0),$$
 where $b_m \neq 0$.
13. $x^7 - x = x(x^6 - 1) = x(x^3 + 1)(x^3 - 1) = x(x - 1)^3(x + 1)^3$; $x^{10} - x = x(x^9 - 1) = x(x - 1)^9$ (see Exercise 49 in Chapter 13).
15. *Hint:* Use Exercise 49 in Chapter 13.
17. $a = 4/3$, $b = 2/3$, $c = 5/6$
19. Use the fact that $1 + i = -(4 - i) + 5$ and $4 - i = 5 - (1 + i)$.
21. If the zeros of $f(x)$ are $a_1, a_2, \dots, a_n$, then the zeros of $f(x + a)$ are $a_1 - a, a_2 - a, \dots, a_n - a$. Now use Exercise 20.
23. $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$
25. 64
27. Let $F = \mathbb{Z}_3[x]/\langle x^3 + 2x + 1 \rangle$ and denote the cosets $x + \langle x^3 + 2x + 1 \rangle$ by β and $2 + \langle x^3 + 2x + 1 \rangle$ by 2. Then $x^3 + 2x + 1 = (x - \beta)(x - \beta - 1)(x + 2\beta + 1)$.
29. Suppose that $\phi: \mathbb{Q}(\sqrt{-3}) \rightarrow \mathbb{Q}(\sqrt{3})$ is an isomorphism. Since $\phi(1) = 1$, we have $\phi(-3) = -3$. Then $-3 = \phi(-3) = \phi(\sqrt{-3}\sqrt{-3}) = (\phi(\sqrt{-3}))^2$. This is impossible, since $\phi(\sqrt{-3})$ is a real number.
31. Use long division.
33. Use Theorem 19.5.

35. Use Theorem 19.5.
37. Let K be the intersection of all subfields of E that contain F and the set $\{a_1, a_2, \dots, a_n\}$. It follows from the subfield test given in Exercise 29 Chapter 13 that K is a subfield of E and, by the definition, that K contains F and the set $\{a_1, a_2, \dots, a_n\}$. Since $F(a_1, a_2, \dots, a_n)$ is the smallest such field we have $F(a_1, a_2, \dots, a_n) \subseteq K$. Moreover, since the field $F(a_1, a_2, \dots, a_n)$ is one member of the intersection we have $K \subseteq F(a_1, a_2, \dots, a_n)$. This proves that $K = F(a_1, a_2, \dots, a_n)$.
39. Since $|(Z_2[x]/\langle f(x) \rangle)^*| = 31$, every nonidentity is a generator.
41. Use the Fundamental Theorem of Field Theory (Theorem 19.1) and the Factor Theorem (Corollary 2 of Theorem 16.2).
43. Mimic the argument given in Example 9 of this chapter.
45. Since $-1 = 1$, $x^n - x$ would have 1 as a multiple zero. But then, by Theorem 19.5, $x^n - x$ and its derivative, which is $-1 = 1$, must have a common factor of positive degree. This is impossible.
47. $\mathbb{Q}(\sqrt[3]{2})(\omega)$ where $\omega = -1/2 + \sqrt{3}i/2$; $\mathbb{Q}(\sqrt{3}i)(\sqrt[3]{2})$.
49. Observe that the polynomial $x^2 - 2x - 1$ is irreducible over $\mathbb{Z}_5$. So Theorems 19.1 and 19.3 shows that such a field exists.
51. If $\alpha \in F(\beta)$, then we have $\alpha = a\beta + b$ for some $a, b \in F$. Squaring both sides, replacing β^2 with $-\beta - 1$, and solving for β , we find that $\beta \in F$. For the second part, if $\beta \in F(\alpha)$ we have $\beta = a\alpha + b$ for some $a, b \in F$. Solving for α in terms of β and proceeding as before we get that β is in F .

Chapter 20

A good proof is one which makes us wiser.

YU. MANIN

1. It follows from Theorem 20.1 that if $p(x)$ and $q(x)$ are both monic

- irreducible polynomials in $F[x]$ with $p(a) = q(a) = 0$, then $\deg p(x) = \deg q(x)$. If $p(x) \neq q(x)$, then $(p - q)(a) = p(a) - q(a) = 0$ and $\deg(p(x) - q(x)) < \deg p(x)$, contradicting Theorem 20.1. To prove Theorem 20.3, use the Division Algorithm for $F[x]$ (Theorem 16.2).
3. Note that $[Q(\sqrt[3]{2}):Q] = n$ and use Theorem 20.5.
 5. Use Exercise 4.
 7. Suppose $Q(\sqrt{a}) = Q(\sqrt{b})$. If $\sqrt{b} \in Q$, then $\sqrt{a} \in Q$ and we may take $c = \sqrt{a}/\sqrt{b}$. If $\sqrt{b} \notin Q$, then $\sqrt{a} \notin Q$. Write $\sqrt{a} = r + s\sqrt{b}$. It follows that $r = 0$ and $a = bs^2$. The other direction follows from Exercise 7 in Chapter 19.
 9. Since $[F(a):F] = 5$, $\{1, a, a^2, a^3, a^4\}$ is a basis for $F(a)$ over F . Also, from $5 = [F(a):F] = [F(a):F(a^3)][F(a^3):F]$ we know that $[F(a^3):F] = 1$ or 5 . However, $[F(a^3):F] = 1$ implies that $a^3 \in F$ and therefore the elements $1, a, a^2, a^3, a^4$ are not linearly independent over F . So, $[F(a^3):F] = 5$.
 11. If a is a zero of $f(x)$ in E then $n = [E:F] = [E:F(a)][F(a):F] = [E:F](\deg f(x))$.
 13. $g(x) = f(x/b - c/b)$
 15. By the Primitive Element Theorem there is an element b in $F(a_1, a_2)$ such that $F(a_1, a_2) = F(b)$. Then, by induction on n , there is an element c in $F(b, a_3, \dots, a_n)$ such that $F(c) = F(b, a_3, \dots, a_n) = F(a_1, a_2, \dots, a_n)$.
 17. 6; 3; 2.
 19. They are the same.
 21. If $b = 0$ for then $x - c$ is minimal. If $b \neq 0$ for $g(x) = f((x - c)/b)$ we have $g(ab + c) = f((ab + c - c)/b) = f(a) = 0$.
 23. If an irreducible polynomial $p(x)$ in $\mathbf{R}[x]$ has degree n and a is a zero in $\mathbf{C}$ of $p(x)$ then $2 = [\mathbf{C}:\mathbf{R}] = [\mathbf{C}:\mathbf{R}(a)][\mathbf{R}(a):\mathbf{R}] = [\mathbf{C}:\mathbf{R}(a)]n$. So, $n = 1$ or 2 .
 25. $Q(\sqrt[4]{2})$.
 27. Suppose that $[E:F] = 1$. Because $\{1\}$ is a linearly independent set over F it is a basis for E over F . So every element of E has the form $a \cdot 1 = a$ for some a in F . If $E = F$, then $\{1\}$ is a basis of E over F and therefore $[E:F] = 1$.
 29. Pick a in K but not in F . Now use Theorem 20.5.
 31. Mimic Example 5.
 33. Mimic Example 6.
 35. Suppose $E_1 \cap E_2 \neq F$. Then $[E_1:E_1 \cap E_2][E_1 \cap E_2:F] = [E_1:F]$ implies $[E_1:E_1 \cap E_2] = 1$, so that $E_1 = E_1 \cap E_2$. Similarly, $E_2 = E_1 \cap E_2$.
 37. Observe that $F(a) = F(1 + a^{-1})$.
 39. We need only show that if $a \in R$, then $a^{-1} \in R$. But $a^{-1} \in F(a) \subseteq R$ (see Theorem 19.3).
 41. Every element of $F(a)$ can be written in the form $f(a)/g(a)$, where $f(x), g(x) \in F[x]$. If $f(a)/g(a)$ is algebraic and not a member of F , then there is some $h(x) \in F[x]$ such that $h(f(a)/g(a)) = 0$. By clearing fractions and collecting like powers of a , we obtain a polynomial in a with coefficients from F equal to 0. But then a would be algebraic over F .
 43. Note that a is a zero of $x^3 - a^3$ over $F(a^3)$. For the second part, take $F = Q, a = 1; F = Q, a = (-1 + i\sqrt{3})/2; F = Q, a = 3\sqrt{2}$.
 45. E must be an algebraic extension of R , so that $E \subseteq C$. But then $[C:E][E:R] = [C:R] = 2$.
 47. Let a be a zero of $p(x)$ in some extension of F . First note $[E(a):E] \leq [F(a):F] = \deg p(x)$. Then observe that $[E(a):F(a)][F(a):F] = [E(a):F] = [E(a):E][E:F]$. This implies that $\deg p(x)$ divides $[E(a):E]$, so that $\deg p(x) = [E(a):E]$. It now follows from Theorem 19.3 that $p(x)$ is irreducible over E .
 49. Hint: If $\alpha + \beta$ and $\alpha\beta$ are algebraic, then so is $\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}$.
 51. $\sqrt{b^2 - 4ac}$
 53. Because $a \in Q(\sqrt{a})$ it suffices to show that $\sqrt{a} \in Q(a)$. Since $a^3 = 1$ we have $a^4 = a$. Then $a^2 = \sqrt{a} \in Q(a)$.
 55. Say a is a generator of F^* . If $\text{char } F$

- $= 0$, then the prime subfield of F is isomorphic to Q . Since Q^* is not cyclic, we have that $F = Z_p(a)$, and it suffices to show that a is algebraic over Z_p . If $a \in Z_p$, we are done. Otherwise, $1 + a = a^k$ for some $k \neq 0$. If $k > 0$, we are done. If $k < 0$, then $a^{-k} + a^{1-k} = 1$ and we are done.
57. If $[K:F] = n$, then there are elements $v_1, v_2, \dots, v_n$ in K that constitute a basis for K over F . The mapping $a_1 v_1 + \dots + a_n v_n \rightarrow (a_1, \dots, a_n)$ is a vector space isomorphism from K to F^n . If K is isomorphic to F^n , then the n elements in K corresponding to $(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)$ in F^n constitute a basis for K over F .
59. Observe that $[F(a, b):F(a)] = [F(a)(b):F(a)] \leq [F(b):F] \leq [F(a)(b):F(b)][F(b):F] = [F(a)(b):F] = [F(a, b):F]$.
61. Observe that $K = F(a_1, a_2, \dots, a_n)$, where $a_1, a_2, \dots, a_n$ are the zeros of the polynomial. Now use Theorem 20.5.
63. Elements of $Q(\pi)$ have the form $(a_m \pi^m + a_{m-1} \pi^{m-1} + \dots + a_0) / (b_n \pi^n + b_{n-1} \pi^{n-1} + \dots + b_0)$, where the a 's and b 's are rational numbers. So, if $\sqrt{2} \in Q(\pi)$, we have an expression of the form $2(b_n \pi^n + b_{n-1} \pi^{n-1} + \dots + b_0)^2 = (a_m \pi^m + a_{m-1} \pi^{m-1} + \dots + a_0)^2$. Equating the lead terms of both sides, we have $2b_n^2 \pi^{2n} = a_m^2 \pi^{2m}$. But then we have $m = n$, and $\sqrt{2}$ is equal to the rational number a_m/b_n .
65. If $f(a^m) = 0$ for some polynomial $f(x)$ in $F[X]$, then a is a zero of $g(x) = f(x^m)$ which is in $F[x]$.
3. The lattice of subfields of $\text{GF}(64)$ looks like Figure 21.3 with $\text{GF}(2)$ at the bottom, $\text{GF}(64)$ at the top, and $\text{GF}(4)$ and $\text{GF}(8)$ on the sides.
5. $\text{GF}(2^6)$
7. $2a + 1$
9. Since each binomial coefficient $\binom{p^i}{j}$ other than $j = 1$ and $j = p^i$ is divisible by p we have $(a + b)^p = a^{p^i} + b^{p^i}$. Clearly $(ab)^{p^i} = a^{p^i} b^{p^i}$. Since $\text{GF}(p^{p^i})$ is a field and $a^{p^i} = 0$ only when $a = 0$ so the $\text{Ker } \phi = \{0\}$.
11. Observe that $x^2 + 1 = (x + 1)^2$
13. The only possibilities for $f(x)$ are $x^3 + x + 1$ and $x^3 + x^2 + 1$. See Exercise 8 in Chapter 19 for the first case. See Example 2 in this chapter for the second case.
15. By Theorem 21.4 an element of $\text{GF}(64)$ has the desired property if and only if it is not in $\text{GF}(4)$ or $\text{GF}(8)$. Since $\text{GF}(4)$ is not a subgroup of $\text{GF}(8)$ their intersection is $\{0, 1\}$. This means there are 54 elements with the property. Given that a^7 in $\text{GF}(16)$ is a zero of the irreducible polynomial of degree 4 over Z_2 , find the other three zeros.
17. Let $|F| = p^n$. Then n must be divisible by both 4 and 6. So, by Theorem 21.4, F must also have subfields of order p^{12}, p^3, p^2 and p .
19. Because $|\text{GF}(8)^*| = 7$, $\text{GF}(2)(a) = \text{GF}(8)$.
21. The statement is trivially true for 0 and 1. Since $a^{16} = a^4$ implies that $a^{12} = 1$ we know that $|a|$ divides 12. But $|a|$ also divides $|\text{GF}(2^n)^*| = 2^n - 1$, which is odd. So, $|a| = 3$ and the statement follows.
23. First note that $x, x - 1$ and $x - 2$ are factors and that are the only linear factors. If $p(x)$ is an irreducible factor of $x^{27} - x$ then a is a zero of an irreducible factor $x^{27} - x$ of degree d then $Z_3(a)$ is a subfield of $\text{GF}(27)$ of order 3^d and by Theorem 21.4 we have that $d = 1$ or 3. So, the irreducible factorization of $x^{27} - x$ consists of

Chapter 21

Difficulties strengthen the mind, as labor does the body.

SENECA

1. $[\text{GF}(729):\text{GF}(9)] = 3$; $[\text{GF}(64):\text{GF}(8)] = 2$

- three linear factors and eight cubic factors.
25. $\text{GF}(p^{2n})$.
27. To show that F is field let $a, b \in F$. Then $a \in F_i$ for some i and $b \in F_j$ for some j and $a, b \in F_k$ where k is the maximum of i and j . It follows that $a - b \in F_k, ab \in F_k$ and $a^{-1} \in F_k$ when $a \neq 0$.
29. Since 0, 1, and 2 are zeros we know $x, x - 1$ and $x - 2$ are factors and by Theorem 19.8 these each have multiplicity 1. Theorem 21.5 tells us that all other irreducible factors have degree 2 and, since their degrees must sum to six, there are three of them. Finally, from the proof of Theorem 21.1 we know that each of the nine elements of $\text{GF}(9)$ are zeros of $x^9 - x$. So no two quadratic reducibles can be the same. The factorization $x^9 - x = x(x - 1)(x - 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$.
31. Direct calculations show that given $x^3 + 2x + 1 = 0$, we have $x^2 \neq 1$ and $x^{13} \neq 1$.
33. Direct calculations show that $x^{13} = 1$, whereas $(2x)^2 \neq 1$ and $(2x)^{13} \neq 1$. Thus, $2x$ is a generator.
35. First observe that for any field F , the set F^* is a group under multiplication. Now use Theorem 21.2 and Theorem 4.3.
37. Let $a, b \in K$. Then, by Exercise 49b in Chapter 13, $(a - b)^{p^m} = a^{p^m} - b^{p^m} = a - b$. Also, $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$. So, K is a subfield.
39. Consider $x^{p^n-1} - 1$ and use Corollary 4 of Lagrange's Theorem (Theorem 7.1).
41. Structurally identical
43. Consider $g(x) = x^2 - a$. Note that $|\text{GF}(p)[x]/\langle g(x) \rangle| = p^2$, so that $g(x)$ has a zero in $\text{GF}(p^2)$. Now use Theorem 21.3.
45. $F^*; \text{GF}(2^5)^* = \langle a^{33} \rangle$;
 $\text{GF}(2^2)^* = \langle a^{341} \rangle$;
 $\text{GF}(2)^* = \langle a^{1023} \rangle = \{1\}$.
47. Since F^* is a cyclic group of order 124, it has a unique element of order 2.
49. Use Corollary 2 of Theorem 21.2.
51. Observe that $p - 1 = -1$ has multiplicative order 2 and $a^{(p^n-1)/2}$ is the unique element in $\langle a \rangle$ of order 2.
53. Since $0 = 0^2$ it suffices to show that in F^* there are exactly $(p^n - 1)/2$ elements that can be written as a square of an element of F^* . Observe that the mapping from the cyclic group F^* to itself that takes x to x^2 is a group homomorphism with the kernel $\{\pm 1\}$. So, the mapping is 2-1.
55. Since $p \equiv 1 \pmod{4}$ we have $p^n \equiv 1 \pmod{4}$ and $\text{GF}(p^n)^*$ is a cyclic of order $p^n - 1$. So, by Theorem 4.4 there is exactly two elements of order 4.
57. First note that a not in Z_5 for then $x - a$ would be a factor of the irreducible. Then taking $b = 0$ and we solve for $c = (4a + 1)(3a + 2)^{-1}$.
59. It is a field of order 4^5 .
61. For the case $\text{GF}(p^n)$ observe that if $1 + a + a^2 + a^3 + \cdots + a^i = 1 + a + a^2 + a^3 + \cdots + a^j$ for some $i < j$ then $0 = a^{i+1} + \cdots + a^j = a^{i+1}(1 + a + a^2 + \cdots + a^{j-i-1})$ and therefore a^{i+1} is a zero-divisor.
63. Let $F_1 = \text{GF}(p^n), F_2 = \text{GF}(p^{2n}), F_3 = \text{GF}(p^{4n}), F_4 = \text{GF}(p^{8n}), \dots$
65. The algebraic closure of Z_2 .
67. By Theorem 21.4, for each prime q the only proper subfield of $\text{GF}(p^q)$ is $\text{GF}(p)$.

Chapter 22

Why, sometimes I've believed as many as six impossible things before breakfast.

LEWIS CARROLL

- To construct $a + b$, first construct a . Then use a straightedge and compass to extend a to the right by marking off the length of b . To construct $a - b$, use the compass to mark off a length of b

from the right endpoint of a line of length a .

3. Let y denote the length of the hypotenuse of the right triangle with base 1, and let x denote the length of the hypotenuse of the right triangle with base $|c|$. Then $y^2 = 1 + d^2$, $y^2 + x^2 = (1 + |c|)^2$, and $|c|^2 + d^2 = x^2$. So, $1 + 2|c| + |c|^2 = 1 + d^2 + |c|^2 + d^2$, which simplifies to $|c| = d^2$.
5. Use $\sin^2 \theta + \cos^2 \theta = 1$.
7. Use $\cos 2\theta = 2\cos^2 \theta - 1$.
9. Use $\sin(\alpha - \beta) = \sin \alpha \cos \beta - \cos \alpha \sin \beta$ and Exercise 8.
11. Solving two linear equations with coefficients from F involves only the operations of F .
13. Use Theorem 17.1.
15. If so, then an angle of 40° is constructible. Now use Exercise 10.
17. This amounts to showing that $\sqrt{\pi}$ is not constructible. But if $\sqrt{\pi}$ is constructible, so is π . However, $[Q(\pi):Q]$ is infinite.
19. No, since $[Q(\sqrt[3]{3}):Q] = 3$.
21. No, since $[Q(\sqrt[3]{\pi}):Q]$ is infinite.

Chapter 23

Difficulty, my brethren, is the nurse of greatness.

WILLIAM CULLEN BRYANT

1. $a = eae^{-1}$; $cac^{-1} = b$ implies $a = c^{-1}bc = c^{-1}b(c^{-1})^{-1}$; $a = xbx^{-1}$ and $b = ycy^{-1}$ imply $a = xycy^{-1}x^{-1} = xyc(xy)^{-1}$.
3. Note that $|a^2| = |a|/2$ and appeal to Exercise 2.
5. Observe that $T(xC(a)) = xax^{-1} = yay^{-1} = T(yC(a))$ if and only if $y^{-1}xa = ay^{-1}x$, which is true if and only if $y^{-1}x \in C(a)$, which in turn is true if and only if $yC(a) = xC(a)$. This proves that T is well-defined and one-to-one. T is onto by definition.
7. Say $\text{cl}(e)$ and $\text{cl}(a)$ are the only two conjugacy classes of a group G of

order n . Then $\text{cl}(a)$ has $n - 1$ elements all of the same order, say m . If $m = 2$, then it follows from Exercise 45 in Chapter 2 that G is Abelian. But then $\text{cl}(a) = \{a\}$ and so $n = 2$. If $m > 2$, then $\text{cl}(a)$ has at most $n - 2$ elements, since conjugation of a by e, a , and a^2 each yields a .

9. Consider the correspondence T from the left cosets of $N(H)$ in G to the conjugates of H in G given by $T(xN(H)) = xHx^{-1}$.
11. Say $\text{cl}(x) = \{x, g_1xg_1^{-1}, g_2xg_2^{-1}, \dots, g_kxg_k^{-1}\}$. If $x^{-1} = g_ixg_i^{-1}$, then for each $g_jxg_j^{-1}$ in $\text{cl}(x)$, we have $(g_jxg_j^{-1})^{-1} = g_jx^{-1}g_j^{-1} = g_j(g_ixg_i^{-1})g_j^{-1} \in \text{cl}(x)$. Because $|G|$ has odd order, $g_jxg_j^{-1} \neq (g_jxg_j^{-1})^{-1}$. It follows that $|\text{cl}(x)|$ is even. But $|\text{cl}(x)|$ divides $|G|$.
13. Part **a** is not possible by the corollary of Theorem 23.2. Part **b** is not possible because it implies that the center would have order 2, and 2 does not divide 21. Part **c** is the class equation for D_5 . Part **d** is not possible because of Corollary 1 of Theorem 23.1.
15. Use Theorem 7.2.
17. Use Example 5 of Chapter 9 and Theorem 7.2.
19. Use Theorem 23.5 and its corollary.
21. 8
23. 15
25. The number of Sylow q -subgroups has the form $1 + qk$ and divides p . So, $k = 0$.
27. A group of order 100 has 1, 5, or 25 subgroups of order 4; exactly one subgroup of order 25 (which is normal); at least one subgroup of order 5; and at least one subgroup of order 2.
29. Let H be a Sylow 5-subgroup. Since the number of Sylow 5-subgroups is 1 mod 5 and divides $7 \cdot 17$, the only possibility is 1. So, H is normal in G . Then by the N/C Theorem (Example 17 of Chapter 10), $|G/C(H)|$ divides both 4 and $|G|$. Thus $C(H) = G$.

31. By Theorem 23.6 $G/Z(G)$ would be cyclic and therefore by Theorem 9.3 G would be Abelian. But then $G = Z(G)$.
33. If p does not divide $q - 1$, and q does not divide $p^2 - 1$, then a group of order p^2q is Abelian.
35. Sylow's Third Theorem implies that the Sylow 3- and Sylow 5-subgroups are unique. Pick any x not in the union of these. Then $|x| = 15$.
37. By Sylow's Third Theorem, $n_{17} = 1$ or 35. Assume $n_{17} = 35$. Then the union of the Sylow 17-subgroups has 561 elements. By Sylow's Third Theorem, $n_5 = 1$. Thus, we may form a cyclic subgroup of order 85 (Theorem 23.6). But then there are 64 elements of order 85. This gives too many elements.
39. Use the G/Z Theorem (Theorem 9.3) and Theorem 23.6.
41. Let H be the Sylow 3-subgroup and suppose that the Sylow 5-subgroups are not normal. By Sylow, there must be six Sylow 5-subgroups, call them $K_1, \dots, K_6$. These subgroups have 24 elements of order 5. Also, each of the cyclic subgroups $HK_1, \dots, HK_6$ has eight generators. Thus, there are 48 elements of order 15, which results in more than 60 elements in the group.
43. By Theorem 23.2 and Theorem 9.5, $Z(G)$ has an element x of order p . By induction, the group $G/\langle x \rangle$ has normal subgroups of order p^k for every k between 1 and $n - 1$, inclusively. Now use Exercise 59 in Chapter 9 and Exercise 59 of Chapter 10.
45. Pick $x \in Z(G)$ such that $|x| = p$. If $x \in H$, by induction, $N(H/\langle x \rangle) > H/\langle x \rangle$, say $y\langle x \rangle \in N(H/\langle x \rangle)$ but not $H/\langle x \rangle$. Now show $y \in N(H)$ but not H . If $x \notin H$, then $x \in N(H)$, so that $N(H) > H$.
47. Since 7 does not divide $11^2 - 1 = 120$ and 11 does not divide $7^2 - 1 = 48$, we know that the Sylow 7-subgroup of G and the Sylow 11-subgroup of G are normal in G . Call them H and K , respectively. Then, by Example 5 of Chapter 9, Theorem 7.2, Theorem 9.6, and the Corollary to Theorem 23.2, HK is subgroup of order $7^2 \cdot 11^2$ and $HK = H \times K \approx H \oplus K$, which is Abelian by Exercise 4 of Chapter 8.
49. Sylow's Third Theorem shows that all the Sylow subgroups are normal. Then Theorem 7.2 and Example 5 of Chapter 9 ensure that G is the internal direct product of its Sylow subgroups. G is cyclic because of Theorem 9.6 and Corollary 1 of Theorem 8.2. G is Abelian because of Theorem 9.6 and Exercise 4 in Chapter 8.
51. Automorphisms preserve order.
53. That $|N(H)| = |N(K)|$ follows directly from the last part of Sylow's Third Theorem and Exercise 9.
55. Normality of H implies $\text{cl}(h) \subseteq H$ for h in H . Now observe that $h \in \text{cl}(h)$. This is true only when H is normal.
57. Suppose that G is a group of order 12 that has nine elements of order 2. By the Sylow theorems, G has three Sylow 2-subgroups whose union contains the identity and the nine elements of order 2. If H and K are both Sylow 2-subgroups, then by Theorem 7.2, $|H \cap K| = 2$. Thus, the union of the three Sylow 2-subgroups has at most seven elements of order 2, since there are three in H , two more in K that are not in H , and at most two more that are in the third but not in H or K .
59. By Lagrange's Theorem any nontrivial proper subgroup of G has order p or q . It follows from Theorem 23.5 and its corollary that there is exactly one subgroup of order q which is normal (for otherwise there would be $(q + 1)(q - 1) = q^2 - 1$ elements of order q). On the other hand, there cannot be a normal subgroup of order p for then G would be an internal direct product of a cyclic group of order q and a cyclic group of order p , which is Abelian. So, by Theorem 23.5 there must be exactly q subgroups of order p .
61. Note that any subgroup of order 4 in a group of order $4m$ where m is odd is a

Sylow 2-subgroup. By Sylow's Third Theorem, the Sylow 2-subgroups are conjugate and therefore isomorphic. S_4 contains both the subgroups $\langle (1234) \rangle$ and $\{(1), (12), (34), (12)(34)\}$.

63. By Sylow's Third Theorem, the number of Sylow 13-subgroups is equal to 1 mod 13 and divides 55. This means that there is only one Sylow 13-subgroup, so it is normal in G . Thus $|N(H)/C(H)| = 715/|C(H)|$ divides both 55 and 12. This forces $715/|C(H)| = 1$ and therefore $C(H) = G$. This proves that H is contained in $Z(G)$. Applying the same argument to K , we get that K is normal in G and $|N(K)/C(K)| = 715/|C(K)|$ divides both 65 and 10. This forces $715/|C(K)| = 1$ or 5. In the latter case, K is not contained in $Z(G)$.

65. First observe that because $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & ka \\ 0 & 1 \end{bmatrix}$ the element $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ has order p . By Sylow's Second Theorem every element of order p is contained in a Sylow p -subgroup. So, if A is any element in $GL(2, Z_p)$ of order p then A and $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ belong to Sylow p -subgroups and, by Sylow's Third Theorem, every two Sylow p -subgroups are conjugate.

Chapter 24

He who learns must suffer.

Aeschylus

1. Use the 2 · Odd Test.
3. Use the Index Theorem.
5. Suppose G is a simple group of order 525. Let L_7 be a Sylow 7-subgroup of G . It follows from Sylow's theorems that $|N(L_7)| = 35$. Let L be a subgroup of $N(L_7)$ of order 5. Since $N(L_7)$ is cyclic (Theorem 23.6), $N(L) \geq N(L_7)$, so that 35 divides $|N(L)|$. But L is contained in a Sylow 5-subgroup (Theorem 23.4), which is

Abelian (see the corollary to Theorem 23.2). Thus, 25 divides $|N(L)|$ as well. It follows that 175 divides $|N(L)|$. The Index Theorem now yields a contradiction.

7. $n_{11} = 12$. Use the N/C Theorem (Example 17 in Chapter 10) to show that there is an element of order 22; then use the Embedding Theorem and observe that A_{12} has no element of order 22.
9. Suppose that there is a simple group of order 396 and L_{11} is a Sylow 11-subgroup. Use the N/C Theorem given in Example 17 of Chapter 10 to show that $C(L_{11})$ has an element of order 33, whereas A_{12} does not.
11. If we can find a pair of distinct Sylow 2-subgroups A and B such that $|A \cap B| = 8$, then $N(A \cap B) \geq AB$, so that $N(A \cap B) = G$. Now let H and K be any distinct pair of Sylow 2-subgroups. Then $16 \cdot 16/|H \cap K| = |HK| \leq 112$ (Theorem 7.2), so that $|H \cap K|$ is at least 4. If $|H \cap K| = 8$, we are done. So, assume $|H \cap K| = 4$. Then $N(H \cap K)$ picks up at least 8 elements from H and at least 8 from K (see Exercise 45 in Chapter 23). Thus, $|N(H \cap K)| \geq 16$ and is divisible by 8. So, $|N(H \cap K)| = 16, 56$, or 112. Since the latter two cases yield normal subgroups, we may assume $|N(H \cap K)| = 16$. If $N(H \cap K) = H$, then $|H \cap K| = 8$, since $N(H \cap K)$ contains at least 8 elements from K . So, we may assume that $N(H \cap K) \neq H$. Then, we may take $A = N(H \cap K)$ and $B = H$.
13. If H is a proper subgroup of A_{n+1} of order greater than $n!/2$, then $[A_{n+1} : H] < [A_{n+1} : A_n] = n + 1$ and it follows from the Embedding Theorem that A_{n+1} is isomorphic to a subgroup of A_n , which is impossible.
15. Use the Index Theorem.
17. (Gurmeet Singh) By Sylow's third theorem we know that number of Sylow 5-subgroups is 6. This means

- that 6 is the index of the normalizer of a Sylow 5-subgroup. But then, by embedding theorem, G is isomorphic to a subgroup of A_6 of order 120. This contradicts Exercise 16.
19. Let α be as in the proof of the Generalized Cayley Theorem. Then $\text{Ker } \alpha \leq H$ and $|G/\text{Ker } \alpha|$ divides $|G:H|$!. Now show $|\text{Ker } \alpha| = |H|$. A subgroup of index 2 is normal.
 21. Since A_5 is simple, if H is a proper normal subgroup of S_5 , then $H \cap A_5 = A_5$ or $\{\varepsilon\}$. But $H \cap A_5 = A_5$ implies $H = A_5$, whereas $H \cap A_5 = \{\varepsilon\}$ implies $H = \{\varepsilon\}$ or $|H| = 2$. (See Exercise 27 in Chapter 5.) Now use Exercise 72 in Chapter 9 and Exercise 70 in Chapter 5.
 23. See Example 9 in Chapter 9.
 25. Mimic Exercise 24.
 27. Suppose there is a simple group of order 60 that is not isomorphic to A_5 . The Index Theorem implies $n_2 \neq 1$ or 3, and the Embedding Theorem implies $n_2 \neq 5$. Thus, $n_2 = 15$. Counting shows that there must be two Sylow 2-subgroups whose intersection has order 2. Now mimic the argument used in showing that there is no simple group of order 144 to show that the normalizer of this intersection has index 5, 3, or 1, but the Embedding Theorem and the Index Theorem rule these out.
 29. Suppose there is such a simple group G . Since the number of Sylow q -subgroups is 1 modulo q and divides p^2 , it must be p^2 . Thus there are $p^2(q-1)$ elements of order q in G . These elements, together with the p^2 elements in one Sylow p -subgroup, account for all p^2q elements in G . Thus, there cannot be another Sylow p -subgroup. But then the Sylow p -subgroup is normal in G .
 31. Consider the right regular representation of G . Let g be a generator of the Sylow 2-subgroup and suppose that $|G| = 2^k n$ where n is odd. Then every cycle of the permutation T_g in the right regular representation of G has length 2^k . This means that there are exactly n such cycles. Since each cycle is odd and there is an odd number of them, T_g is odd. This means that the set of even permutations in the regular representations has index 2 and is therefore normal. (See Exercise 27 in Chapter 5 and Exercise 9 in Chapter 9).
 33. By direct computation, show that $PSL(2, Z_7)$ has more than four Sylow 3-subgroups, more than one Sylow 7-subgroup, and more than one Sylow 2-subgroup. *Hint:* Observe that $\begin{bmatrix} 1 & 4 \\ 1 & 5 \end{bmatrix}$ has order 3. Now use conjugation to find four other subgroups of order 3; observe that $\left| \begin{bmatrix} 5 & 5 \\ 1 & 4 \end{bmatrix} \right| = 7$ and use conjugation to find another subgroup of order 7; observe that $\left| \begin{bmatrix} 5 & 1 \\ 3 & 5 \end{bmatrix} \right| = 4$ and use conjugation to find six more elements of order 4 (which guarantees that more than one Sylow 2-subgroup exists). Now argue as we did to show that A_5 is simple. In the cases that the supposed normal subgroup N has order 2 or 4, show that in G/N , the Sylow 7-subgroup is normal. But then, G has a normal subgroup of order 14 or 28, which were already ruled out.
 35. By Sylow if the group has only one subgroup of order p^n it is normal. So suppose L_1 and L_2 are distinct subgroups of order p^n . Observe that if $|L_1 \cap L_2| \leq p^{n-2}$ then $|L_1 L_2| = p^n p^n / |L_1 \cap L_2| \geq p^n p^n / p^{n-2} = p^2 p^n > 4p^n$. So, $|L_1 \cap L_2| = p^{n-1}$. Then, by Exercise 45 of Chapter 23 $N(L_1 \cap L_2)$ contains L_1 and L_2 . So, $|N(L_1 \cap L_2)| > p^{n+1} > 2p^n$ and is divisible by p^n . So, $N(L_1 \cap L_2) = G$ and therefore $L_1 \cap L_2$ is normal in G .
 37. By Theorem 24.3 we know that there is a homomorphism ϕ from G into the

symmetric group S_p such that $\text{Ker } \phi$ is a subgroup of H . Then, because $G/\text{Ker } \phi$ is isomorphic to a subgroup of S_p , we have that $|G/\text{Ker } \phi|$ divides $p!$ and that $|G/\text{Ker } \phi|$ divides $|G|$. So, if $|G/\text{Ker } \phi|$ were anything other than p , it would have a prime divisor less than p , which would mean that G would have a prime divisor less than p . So, $p = |G : H| = |G/\text{Ker } \phi|$, which implies that $|H| = |\text{Ker } \phi|$. Since $\text{Ker } \phi$ is a subgroup of H they are equal.

Chapter 25

If you make a mistake, make amends.

LOU HOLTZ

- u is related to u because u is obtained from itself by no insertions; if v can be obtained from u by inserting or deleting words of the form xx^{-1} or $x^{-1}x$, then u can be obtained from v by reversing the procedure; if u can be obtained from v and v can be obtained from w , then u can be obtained from w by obtaining first v from w and then u from v .
- $$b(a^2N) = b(aN)a = a^3bNa = a^3b(aN)$$

$$= a^3a^3bN$$

$$= a^6bN = a^6Nb = a^2Nb = a^2bN$$

$$b(a^3N) = b(a^2N)a = a^2bNa = a^2b(aN)$$

$$= a^2a^3bN$$

$$= a^5bN = a^5Nb = aNb = abN$$

$$b(bN) = b^2N = N$$

$$b(abN) = baNb = a^3bNb = a^3b^2N = a^3N$$

$$b(a^2bN) = ba^2Nb = a^2bNb = a^2b^2N$$

$$= a^2N$$

$$b(a^3bN) = ba^3Nb = abNb = ab^2N = aN$$
- Let F be the free group on $\{a_1, a_2, \dots, a_n\}$. Let N be the smallest normal subgroup containing $\{w_1, w_2, \dots, w_t\}$ and let M be the smallest normal subgroup containing $\{w_1, w_2, \dots, w_t, w_{t+1}, \dots, w_{t+k}\}$. Then $F/N \approx G$ and $F/M \approx \bar{G}$. The homomorphism from F/N to F/M given by $aN \rightarrow aM$ induces a homomorphism from G onto $\bar{G}$. To prove the corollary, observe that the theorem shows that K is a homomorphic image of G , so $|K| \leq |G|$.
- Clearly, a and ab belong to $\langle a, b \rangle$, so $\langle a, ab \rangle \subseteq \langle a, b \rangle$. Now show that a and b belong to $\langle a, ab \rangle$.
- Show that $|G| \leq 2n$ and that D_n satisfies the relations that define G .
- Since $x^2 = y^2 = e$, we have $(xy)^{-1} = y^{-1}x^{-1} = yx$. Also, $xy = z^{-1}yz$, so $(xy)^{-1} = (z^{-1}yz)^{-1} = z^{-1}y^{-1}z = z^{-1}yz = xy$.
- a.** b^6 **b.** b^7a
- First observe that since $xy = (xy)^3(xy)^4 = (xy)^7 = (xy)^4(xy)^3 = yx$, x and y commute. Also, since $y = (xy)^4 = (xy)^3xy = x(xy) = x^2y$ we know that $x^2 = e$. Then $y = (xy)^4 = x^4y^4 = y^4$ and therefore, $y^3 = e$. This shows that $|G| \leq 6$. But Z_6 satisfies the defining relations with $x = 3$ and $y = 2$. So, $G \approx Z_6$.
- Note that $yxxy^3 = e$ implies that $yxxy^{-1} = x^5$ and therefore $\langle x \rangle$ is normal. So, $G = \langle x \rangle \cup y\langle x \rangle$ and $|G| \leq 16$. Use $y^2 = e$ and $yxxy^3 = e$, to prove that $x^2 \in Z(G)$. Then prove G is not Abelian and use Theorem 9.3 to show that $|Z(G)| \neq 8$. Thus, $Z(G) = \langle x^2 \rangle$. Finally, prove that $(xy)^2 = x^{-2}$, so that $|xy| = 8$.
- Use the fact that the mapping from G onto G/N given by $x \rightarrow xN$ is a homomorphism.
- For H to be a normal subgroup we must have $yxxy^{-1} \in H = \{e, y^3, y^6, y^9, x, xy^3, xy^6, xy^9\}$. But $yxxy^{-1} = yxy^{11} = (yxy)y^{10} = xy^{10}$.
- 6; the given relations imply that $a^2 = e$. G is isomorphic to Z_6 .
- 1, 2, and ∞
- $ab = c \Rightarrow abc^{-1} = e$
 $cd = a \Rightarrow (abc^{-1})cd = ae \Rightarrow bd = e \Rightarrow$

$$d = b^{-1}$$

$$da = b \Rightarrow bda = b^2 \Rightarrow ea = b^2 \Rightarrow a = b^2$$

$$ab = c \Rightarrow b^3 = c$$

So $G = \langle b \rangle$.

$$bc = d \Rightarrow bb^3 = b^{-1} \Rightarrow b^5 =$$

e . So $|G| = 1$ or 5 .

But Z_5 satisfies the defining relations with

$$a = 1, b = 3, c = 4, \text{ and } d = 2.$$

29. Z_6

Chapter 26

If at first you don't succeed—that makes you about average.

BRADENTON, [*Florida*] *Herald*

1. If T is a distance-preserving function and the distance between points a and b is positive, then the distance between $T(a)$ and $T(b)$ is positive.
3. See Figure 1.5.
5. 12
7. $4n$
9. a. Z_2 b. $Z_2 \oplus Z_2$ c. $G \oplus Z_2$, where G is the plane symmetry group of a circle (see Exercise 55 of Chapter 3).
11. 6
13. An inversion in $\mathbf{R}^3$ leaves only a single point fixed, whereas a rotation leaves a line fixed.
15. In $\mathbf{R}^4$, a plane is fixed. In $\mathbf{R}^n$, a hyperplane of dimension $n - 2$ is fixed.
17. Create a coordinate system for the plane. Let T be an isometry; p, q , and r the three noncollinear points; and s any other point in the plane. Then the quadrilateral determined by $T(p), T(q), T(r)$, and $T(s)$ is congruent to the one formed by p, q, r , and s . Thus, $T(s)$ is uniquely determined by $T(p), T(q)$, and $T(r)$.
19. a rotation

Chapter 27

Failure is the key to success; each mistake teaches us something.

MORIHEI UESHIBA

1. 6
3. 30
5. 13
7. 45
9. 126
11. $\frac{1}{6}(n^6 + 2 \cdot n + 2 \cdot n^2 + n^3)$
13. For the first part, see Exercise 13 in Chapter 6. For the second part, try D_4 .
15. R_0, R_{180}, H, V act as the identity and R_{90}, R_{270}, D, D' interchange L_1 and L_2 .

Chapter 28

I am not bound to please thee with my answers.

SHAKESPEARE, *The Merchant of Venice*

1. $4 * (b, a)$
3. $(m/2) * \{3 * [(a, 0), (b, 0)], (a, 0), (e, 1) 3 * (a, 0), (b, 0), 3 * (a, 0), (e, 1)\}$
5. a^3b
7. Both yield paths from e to a^3b .
11. Say we start at x . Then we know the vertices $x, xs_1, xs_1s_2, \dots, xs_1s_2 \cdots s_{n-1}$ are distinct and $x = xs_1s_2 \cdots s_n$. So if we apply the same sequence beginning at y , then cancellation shows that $y, ys_1, ys_1s_2, \dots, ys_1s_2 \cdots s_{n-1}$ are distinct and $y = ys_1s_2 \cdots s_n$.
13. If there were a Hamiltonian path from $(0, 0)$ to $(2, 0)$, there would be a Hamiltonian circuit in the digraph, since $(2, 0) + (1, 0) = (0, 0)$. This contradicts Theorem 28.1.
15. **a.** If $s_1, s_2, \dots, s_{n-1}$ traces a Hamiltonian path and $s_i s_{i+1} \cdots s_j = e$, then the vertex $s_1 s_2 \cdots s_{i-1}$ appears twice. Conversely, if $s_i s_{i+1} \cdots s_j \neq e$, then the sequence $e, s_1, s_1 s_2, \dots, s_1 s_2 \cdots s_{n-1}$ yields the n vertices (otherwise, cancellation gives a contradiction).
b. This follows directly from part **a**.
17. The sequence traces the digraph in a clockwise fashion.
19. Abbreviate $(a, 0)$, $(b, 0)$, and $(e, 1)$ by a, b , and 1 , respectively. A circuit is

- $4 * (4 * 1, a), 3 * a, b, 7 * a, 1, b, 3 * a, b, 6 * a, 1, a, b, 3 * a, b, 5 * a, 1, a, a, b, 3 * a, b, 4 * a, 1, 3 * a, b, 3 * a, b, 3 * a, b.$
21. Abbreviate $(R_{90}, 0)$, $(H, 0)$, and $(R_0, 1)$ by R, H , and 1 , respectively. A circuit is $3 * (R, 1, 1), H, 2 * (1, R, R), R, 1, R, R, 1, H, 1, 1.$
23. Abbreviate $(a, 0)$, $(b, 0)$, and $(e, 1)$ by a, b , and 1 , respectively. A circuit is $2 * (1, 1, a), a, b, 3 * a, 1, b, b, a, b, b, 1, 3 * a, b, a, a.$
25. Abbreviate $(r, 0)$, $(f, 0)$, and $(e, 1)$ by r, f , and 1 , respectively. Then the sequence is
 $r, r, f, r, r, 1, f, r, r, f, r, 1, r, f, r, r, f, 1, r, r,$
 $f, r, r, 1, f, r, r, f, r,$
 $1, r, f, r, r, f, 1.$
27. $m * [(n - 1) * (0, 1), (1, 1)]$
29. Abbreviate $(r, 0)$, $(f, 0)$, and $(e, 1)$ by r, f , and 1 , respectively. A circuit is $1, r, 1, 1, f, r, 1, r, 1, r, f, 1.$
31. $5 * [3 * (1, 0), (0, 1)], (1, 0)$
33. $12 * [(1, 0), (0, 1)]$
35. Letting V denote a vertical move and H a horizontal move and starting at $(1, 0)$ a circuit is $V, V, H, 6 * (V, V, V, H).$
37. In the proof of Theorem 28.3, we used the hypothesis that G is Abelian in two places: We needed H to satisfy the induction hypothesis, and we needed to form the factor group G/H . Now, if we assume only that G is Hamiltonian, then H also is Hamiltonian and G/H exists.
- 000000, 100011, 010101, 001110, 110110, 101101, 011011, 111000
7. By using $t = 1/2$ in the proof of Theorem 29.2 we have that all single errors can be detected.
9. Observe that a vector has even weight if and only if it can be written as a sum of an even number of vectors of weight 1.
11. No, by Theorem 29.3.
13. 0000000, 1000111, 0100101, 0010110, 0001011, 1100010, 1010001, 1001100, 0110011, 0101110, 0011101, 1110100, 1101001, 1011010, 0111000, 1111111;
- $$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$
- yes.
15. Suppose that u is decoded as v and that x is the coset leader of the row containing u . Coset decoding means v is at the head of the column containing u . So, $x + v = u$ and $x = u - v$. Now suppose $u - v$ is a coset leader and u is decoded as y . Then y is at the head of the column containing u . Since v is a code word, $u = u - v + v$ is in the row containing $u - v$. Thus, $u - v + y = u$ and $y = v$.
17. 000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000;

Chapter 29

We must view with profound respect the infinite capacity of the human mind to resist the introduction of useful knowledge.

THOMAS R. LOUNSBURY

- wt(0001011) = 3; wt(0010111) = 4; wt(0100101) = 3; etc.
- 1000110; 1110100
- 5.

001001 is decoded as 001101 by all four methods.

011000 is decoded as 111000 by all four methods.

000110 is decoded as 100110 by all four methods.

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since there are no code words whose distance from 100001 is 1 and three whose distance is 2, the nearest-neighbor method will not decode or will arbitrarily choose a code word; parity-check matrix decoding does not decode 100001; the standard-array and syndrome methods decode 100001 as 000000, 110101, or 101011, depending on which of 100001, 010100, or 001010 is a coset leader.

19. For any received word w , there are only eight possibilities for wH . But each of these eight possibilities satisfies condition 2 or the first portion of condition 3' of the decoding procedure, so decoding assumes that no error was made or one error was made.
21. There are 3^4 code words and 3^6 possible received words.
23. No; row 3 is twice row 1.
25. No. For if so, nonzero code words would be all words with weight at least 5. But this set is not closed under addition.
27. Use Exercise 24, together with the fact that the set of code words is closed under addition.
29. Abbreviate the coset $a + \langle x^2 + x + 1 \rangle$ with a . The following generating matrix will produce the desired code:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & x & x+1 & x+1 \end{bmatrix}.$$

31. Use Exercise 14.
33. Let $c, c' \in C$. Then,
 $c + (v + c') = v + c + c' \in v + C$ and
 $(v + c) + (v + c') = c + c' \in C$, so the set $C \cup (v + C)$ is closed under addition.
35. If the i th component of both u and v is 0, then so is the i th component of $u - v$ and au , where a is a scalar.

Chapter 30

Wisdom rises upon the ruins of folly.

THOMAS FULLER, *Gnomologia*

1. Note that $\phi(1) = 1$. Thus $\phi(n) = n$. Also, $1 = \phi(1) = \phi(nn^{-1}) = \phi(n)\phi(n^{-1}) = n\phi(n^{-1})$, so that $1/n = \phi(1/n)$.
3. If α and β are automorphisms of E fixing F , so are α^{-1} and $\alpha\beta$.
5. If a and b are fixed by elements of H , so are $a + b, a - b, a \cdot b$, and a/b .
7. It suffices to show that each member of $\text{Gal}(K/F)$ defines a permutation on the a_i 's. Let $a \in \text{Gal}(K/F)$ and write

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$$

$$= c_n (x - a_1)(x - a_2) \cdots (x - a_n).$$
Then $f(x) = \alpha(f(x)) = c_n (x - \alpha(a_1))(x - \alpha(a_2)) \cdots (x - \alpha(a_n))$. Thus, $f(a_i) = 0$ implies $a_i = \alpha(a_j)$ for some j , so that α permutes the a_i 's.
9. Observe that $\phi^6(\omega) = \omega^{729} = \omega$ whereas $\phi^3(\omega) = \omega^{27} = \omega^{-1}$ and $\phi^2(\omega) = \omega^9 = \omega^2$.
 $\phi^3(\omega + \omega^{-1}) = \omega^{27} + \omega^{-27} = \omega^{-1} + \omega$;
 $\phi^2(\omega^3 + \omega^5 + \omega^6) = \omega^{27} + \omega^{45} + \omega^{54} = \omega^6 + \omega^3 + \omega^5$.
11. **a.** $Z_{20} \oplus Z_2$ has three subgroups of order 10.
b. 25 does not divide 40, so there are none.
c. $Z_{20} \oplus Z_2$ has one subgroup of order 5.
13. The splitting field over $\mathbf{R}$ is $\mathbf{R}(\sqrt{-3})$. The Galois group is the identity and the mapping $a + b\sqrt{-3} \rightarrow a - b\sqrt{-3}$.
15. Use Theorem 22.3.
17. Recall that A_4 has no subgroup of order 6. (See Example 5 in Chapter 7.)
19. Use Sylow's First Theorem.
21. Let ω be a primitive cube root of 1. Then $Q \subset Q(\sqrt[3]{2}) \subset Q(\omega, \sqrt[3]{2})$ and $Q(\sqrt[3]{2})$ is not the splitting field of a polynomial in $Q[x]$.
23. Use the lattice of Z_{10} .
25. Z_6 (Be sure you know why the group is cyclic.)
27. See Exercise 21 in Chapter 24.
29. Use Exercise 43 in Chapter 23.
31. Use Exercise 50 in Chapter 10.
33. Since $K/N \triangleleft G/N$, for any $x \in G$ and $k \in K$, there is a $k' \in K$ such that $k'N = (xN)(kN)(xN)^{-1} =$

$xNkNx^{-1}N = xkx^{-1}N$. So,
 $xkx^{-1} = k'n$ for some $n \in N$. And
 since $N \subseteq K$, we have $k'n \in K$.

35. Since G is solvable there is a series
 $\{e\} = K_0 \subset K_1 \subset \cdots \subset K_m = G$ such
 that K_{i+1}/K_i is Abelian. Now there is a series

$$\frac{K_i}{K_i} = \frac{L_0}{K_i} \subset \frac{L_1}{K_i} \subset \cdots \subset \frac{L_t}{K_i} = \frac{K_{i+1}}{K_i},$$

where $|(L_{j+1}/K_i)/(L_j/K_i)|$ is prime.
 Then $K_i = L_0 \subset L_1 \subset L_2 \subset \cdots \subset$
 $L_t = K_{i+1}$ and each $|L_{j+1}/L_j|$ is
 prime (see Exercise 42 of Chapter 10).
 We may repeat this process for each i .

Chapter 31

All wish to possess knowledge, but
 few, comparatively speaking, are will-
 ing to pay the price.

JUVENAL

1. $x^2 - x + 1$
3. Over Z , $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$. Over Z_2 , $x^2+1 = (x+1)^2$ and $x^4+1 = (x+1)^4$. So, over Z_2 , $x^8-1 = (x+1)^8$. Over Z_3 , x^2+1 is irreducible, but x^4+1 factors into irreducibles as $(x^2+x+2)(x^2-x-1)$. So, $x^8-1 = (x-1)(x+1)(x^2+1)(x^2+x+2)(x^2-x-1)$. Over Z_5 , $x^2+1 = (x-2)(x+2)$, $x^4+1 = (x^2+2)(x^2-2)$, and these last two factors are irreducible. So, $x^8-1 = (x-1)(x+1)(x-2)(x+2)(x^2+2)(x^2-2)$.
5. Let ω be a primitive n th root of unity. We must prove $\omega\omega^2 \cdots \omega^n = (-1)^{n+1}$. Observe that $\omega\omega^2 \cdots \omega^n = \omega^{n(n+1)/2}$. When n is odd, $\omega^{n(n+1)/2} = (\omega^n)^{(n+1)/2} = 1^{(n+1)/2} = 1$. When n is even, $(\omega^{n/2})^{n+1} = (-1)^{n+1} = -1$.
7. If $[F:Q] = n$ and F has infinitely many roots of unity, then there is no finite bound on their multiplicative orders. Let ω be a primitive m th root of unity in F such that $\phi(m) > n$.
 Then $[Q(\omega):Q] = \phi(m)$. But
 $F \supseteq Q(\omega) \supseteq Q$ implies $[Q(\omega):Q] \leq n$.
9. Let $2^n + 1 = q$. Then $2 \in U(q)$ and $2^n = q - 1 = -1$ in $U(q)$ implies that $|2| = 2n$. So, by Lagrange's Theorem, $2n$ divides $|U(q)| = q - 1 = 2^n$.
11. Let ω be a primitive n th root of unity. Then $2n$ th roots of unity are $\pm 1, \pm\omega, \dots, \pm\omega^{n-1}$. These are distinct, since $-1 = (-\omega^i)^n$, whereas $1 = (\omega^i)^n$.
13. First observe that $\deg \Phi_{2n}(x) = \phi(2n) = \phi(n)$ and $\deg \Phi_n(-x) = \deg \Phi_n(x) = \phi(n)$. Thus, it suffices to show that every zero of $\Phi_n(-x)$ is a zero of $\Phi_{2n}(x)$. But the fact that ω is a zero of $\Phi_n(-x)$ means that $|\omega| = n$, and because n is odd, this implies that $|\omega| = 2n$.
15. Let $G = \text{Gal}(Q(\omega)/Q)$ and H_1 be the subgroup of G of order 2 that fixes $\cos(\frac{2\pi}{n})$. Then, by induction, G/H_1 has a series of subgroups $H_1/H_1 \subset H_2/H_1 \subset \cdots \subset H_t/H_1 = G/H_1$, so that $|H_{i+1}/H_1:H_i/H_1| = 2$. Now observe that $|H_{i+1}/H_1:H_i/H_1| = |H_{i+1}/H_i|$.
17. Instead, prove that $\Phi_n(x)\Phi_{pn}(x) = \Phi_n(x^p)$. Since both sides are monic and have degree $p\phi(n)$, it suffices to show that every zero of $\Phi_n(x)\Phi_{pn}(x)$ is a zero of $\Phi_n(x^p)$. If ω is a zero of $\Phi_n(x)$, then $|\omega| = n$. By Theorem 4.2, $|\omega^p| = n$ also. Thus, ω is a zero of $\Phi_n(x^p)$. If ω is a zero of $\Phi_{pn}(x)$, then $|\omega| = pn$ and therefore $|\omega^p| = n$.
19. Use Theorem 31.4 and Theorem 30.1.
21. Suppose that a prime $p = 2^m + 1$ and m is not a power of 2. Then $m = st$ where s is an odd integer greater than 1 (the case where $m = 1$ is trivial). Let $n = 2^t + 1$. Then $1 < n < p$ and $2^t \bmod n = -1$. Now looking at $p \bmod n$ and replacing 2^t with -1 , we have $(2^t)^s + 1 = (-1)^s + 1 = 0$. This means that n divides the prime p , which is a contradiction.