Abstract Algebra
John A. Beachy and William D. Blair
Fourth edition, Waveland Press, 2019
ISBN 978-1-4786-3869-8
Errata and comments by Darij Grinberg

The page numbers below refer to the printed page numbers in the 565-page PDF. This list is not claimed to be exhaustive. It combines mathematical corrections, repairs to references and notation, and local copyedits into a single list ordered by page. Broader bibliography, index, and editorial recommendations appear separately at the end.

Almost all the errors in this list were found by GPT-5.6 Sol. I have verified (and occasionally reworded) them.

C. Corrections and comments

1. **Page ix, Preface to the Second Edition:** Replace "text books" by "textbooks".

2. **Page xix, "Writing Proofs":** After specializing Euclid's lemma to $p = 2$, $a = n$, and $b = n$, the text still concludes "if p is a factor of n^2, then p must be a factor of n". Replace both occurrences of "p" in that conclusion by "2".

3. **Page xx, "Writing Proofs":** Replace "descendents" by "descendants" for a more standard spelling.

4. **Page 7, Looking ahead:** In "and again in Chapter 5. when . . . ", replace the period after "5" by a comma.

5. **Page 12, Example 1.1.5:** Replace "$-5x + 81y = 0$" by "$-5x + 18y = 0$".

6. **Page 16, Exercise 23:** The exercise first says that a and b are not both zero, but then calls them "nonzero integers". Delete "nonzero" before "integers".

7. **Page 20, paragraph after proof of Theorem 1.2.7:** In "If $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then b is a divisor of a", add "a positive integer" before "b". Moreover, it is worth clarifying that the β_i should be nonnegative integers, so in particular are allowed to be 0 (so b does not have to use all prime factors of a).

8. **Page 22, Example 1.2.4, first paragraph of the proof:** The number $2^d - 1$ is called a "proper nontrivial divisor" of both $2^{dq} - 1$ and $2^{dp} - 1$. It need not be proper when $q = 1$ or $p = 1$. Say instead that it is a common divisor greater than 1 (or merely a nontrivial common divisor).

9. **Page 23, paragraph before Proposition 1.2.10:** Replace "as in next proposition" by "as in the next proposition".

10. **Page 26, Exercise 23:** The notion of "twin primes" has not been defined. It means two primes that have a difference of 2.

11. **Page 34, alternative proof of the Chinese remainder theorem:** After correctly starting with $x \equiv a \pmod{n}$, the recap says "the first congruence $x \equiv a \pmod{m}$". Change the modulus in the recap from "m" to "n".

12. **Page 37, Exercise 24, Hint:** Replace "How you can use the digits ...?" by "How can you use the digits ...?"

13. **Page 42, Corollary 1.4.6:** The hypothesis "$n > 0$" admits $n = 1$. For $n = 1$, conditions (2) and (3) hold vacuously because $\mathbf{Z}_1$ has no nonzero elements, whereas condition (1) fails because 1 is not prime. Replace "$n > 0$" by "$n > 1$", or strengthen conditions (2) and (3) to disallow $\mathbf{Z}_n$ being trivial.

14. **Page 43, paragraph before Example 1.4.2:** What is called "zero divisor" here has been previously called "divisor of zero" in Definition 1.4.3. The terminology should be made uniform (ideally towards the more commonly used "zero divisor").

15. **Page 43, paragraph before Example 1.4.2:** The claim that the set of powers $[1], [a], [a]^2, \ldots$ "must contain fewer than n distinct elements" fails for $n = 1$. Replace "fewer than n" by "at most n" (which is all that the repetition argument needs), or assume $n > 1$ here.

16. **Page 44, second paragraph:** The paragraph says that "the Chinese remainder theorem is used to show how to determine the solutions modulo a prime power p^α (for integers $\alpha \geq 2$) from the solutions modulo p". The Chinese remainder theorem combines solutions for coprime moduli; lifting a solution from p to p^α is a separate problem and is not always possible (Hensel's lemma is commonly used for this). Say that one first solves modulo the relevant prime powers and then uses the Chinese remainder theorem to combine those solutions.

17. **Page 46, second proof of Fermat's little theorem:** "Writing a as $(1 + 1 + \cdots + 1)$" only directly covers nonnegative integers, although the theorem is stated for every integer a. Choose a nonnegative representative of a mod p, or add a sentence treating negative a.

18. **Page 49:** In "the basic the basic building blocks", delete one occurrence of "the basic".

19. **Pages 54–55, Definition 2.1.1 and the following discussion:** Definition 2.1.1 identifies a function with a subset $F \subseteq S \times T$, but page 55 then distinguishes two functions with the same graph and domain when their

codomains differ. The subset F alone does not encode its codomain, so these two conventions are incompatible. If the latter convention is intended, define a function as a triple (S, T, F) consisting of the specified domain S, the specified codomain T and the graph F.

20. **Page 55:** Replace "use the more familiar notation to their definitions" by "use the more familiar notation to give their definitions".

21. **Page 62, proof of Proposition 2.1.7:** Replace "f maps $g(y)$ onto y" by "f maps $g(y)$ to y". The word "onto" is being used in its technical sense in the surrounding discussion, not as a substitute for "to".

22. **Page 65, Exercise 16:** For arbitrary sets, the implication from "f is onto" to the existence of a function $g : B \to A$ satisfying $f \circ g = 1_B$ uses the axiom of choice; indeed, the assertion that every surjection has a right inverse is equivalent to the axiom of choice. State that choice is being assumed, or restrict the exercise (for example, to finite B).

23. **Page 72, factorization of a function after Theorem 2.2.7:** "for each $x \in X$" should be "for each $x \in S$".

24. **Page 73, Definition 2.2.8:** "Let $S \to T$ be a function" should be "Let $f : S \to T$ be a function".

25. **Page 75, Exercise 12(h)–(j):** Literally, the embedding $f(x, y) = [x, y, 1]$ does not take an affine line onto a projective line: it omits the line's point at infinity. Consequently, images of parallel affine lines remain disjoint as subsets, although their projective closures meet. Ask about the *projective closure* of each image, or explicitly say that the image is a projective line with one point removed.

26. **Page 82, proof of Theorem 2.3.5:** It should be explained why all the cycles constructed by this procedure are disjoint. For example, why cannot some $\sigma^i(1)$ equal some $\sigma^j(a)$? This is not hard to prove (if $\sigma^i(1) = \sigma^j(a)$, then $a = \left(\sigma^j\right)^{-1}\left(\sigma^i(1)\right) = \sigma^{i-j}(1)$, and thus a must belong to the set $\left\{1, \sigma(1), \ldots, \sigma^{r-1}(1)\right\}$ because the latter set is closed under both σ and σ^{-1}), but some argument along these lines needs to be made.

    Furthermore, the theorem asserts the uniqueness of the disjoint cycles of length ≥ 2, but the proof establishes only existence; the next paragraph explicitly leaves uniqueness as an exercise. Either remove uniqueness from the theorem statement or add the short orbit argument: the support of the cycle containing i is $\{\sigma^k(i) \mid k \in \mathbf{Z}\}$, and its cyclic ordering is forced by the action of σ.

27. **Page 89, Exercise 12:** Replace "the number cycles" by "the number of cycles".

28. **Page 90, Notes:** The phrases "combinations of the coefficients" (twice) and "sums, differences, products, and quotients of the coefficients" are misleading. The coefficients are rational and do not get permuted. The relevant condition is preservation of all polynomial relations over $\mathbf{Q}$ among the roots (equivalently, of all rational expressions in the roots whose values lie in $\mathbf{Q}$). Rephrase all three occurrences accordingly.

29. **Page 107:** Replace "a abelian group" by "an abelian group".

30. **Page 111, paragraph before Corollary 3.2.4:** Replace "If the subset in question known to be finite" by "If the subset in question is known to be finite".

31. **Page 130, proof of Proposition 3.3.9:** Replace "if x is a word in S, the so ..." by "if x is a word in S, then so ...".

32. **Page 135, Example 3.4.1:** Replace "it is useful rearrange the table" by "it is useful to rearrange the table".

33. **Page 136, Example 3.4.3:** "defined in Example 3.2.14" should be "defined in Example 3.2.13".

34. **Page 145, proof of Proposition 3.5.3:** The comma before "The order" should be a period.

35. **Page 149, Exercise 12:** Replace "Proposition 3.5.5" by "Theorem 3.5.5".

36. **Page 158, Exercise 1(c):** The first cycle is printed as $(1, 3, \ )$, with its third entry missing. Restore the omitted entry, or remove the comma.

37. **Page 166, Proposition 3.7.6:** Replace "If H_2 is a normal in G_2" by "If H_2 is normal in G_2" or "If H_2 is a normal subgroup of G_2".

38. **Page 175, Example 3.8.1:** The proof has no end-of-proof symbol. Add $\square$ after its final sentence, for consistency with the other proofs in the chapter.

39. **Page 187, Exercise 33:** The exercise is stated as a declarative sentence without an instruction. Insert "Prove that" or "Show that" before "the left coset aH is a right coset ...".

40. **Page 187, Notes:** Replace "the use groups in the theory of equations" by "the use of groups in the theory of equations".

41. **Pages 203–204, proof of Theorem 4.2.1:** The theorem allows $f(x) = 0$, but the proof immediately writes $f(x) = a_m x^m + \cdots + a_0$ with $a_m \neq 0$ and never treats the zero polynomial. Begin by observing that if $f(x) = 0$, one may take $q(x) = r(x) = 0$; then assume $f(x) \neq 0$ for the argument that follows.

42. **Page 209, last sentence:** The irreducibility criterion for $x^4 + x^3 + x^2 + x + 1$ is not developed in the next section (Section 4.3), but in Section 4.4 (Theorem 4.4.6). Replace "in the next section" by "in Section 4.4".

43. **Page 210, proof of Proposition 4.2.11:** The proposition is stated for polynomials over **R**, but the proof suddenly places $a(x)$ and $b(x)$ in $F[x]$. Use $\mathbf{R}[x]$, or restate the proposition over a general field F if that generality is intended.

44. **Page 213, Exercise 20:** Replace "Your answer should have degree 1" by "Your answer should have degree at most 1", since the products can have constant (or even zero) remainders for particular values of a, b, c, d.

45. **Page 213, Exercise 22(a)–(c):** If $a = b = 0$, the congruence $(a + bx)q(x) \equiv 1$ has no solution. Add the hypothesis that a and b are not both zero.

46. **Page 217, paragraph after Example 4.3.2:** Replace "the cosets $[a]$ coming the from constant polynomials" by "the cosets $[a]$ coming from the constant polynomials".

47. **Page 218, proof of Corollary 4.3.9:** After all linear factors have been removed, the remaining factor $f_1(x)$ may be constant. In that case the desired factorization is already complete, whereas the next sentence incorrectly tries to find a root of $f_1(x)$. Insert "If $f_1(x)$ is constant, we are done; otherwise" before applying Kronecker's theorem.

48. **Page 221, Exercise 23(a)–(b):** The zero class, obtained when $a = b = 0$, has no multiplicative inverse. Add the hypothesis that a and b are not both zero.

49. **Page 227, proof of Corollary 4.4.10:** Replace "Corollary 4.1.1" by "Corollary 4.1.11".

50. **Page 233, historical note on the cubic:** After introducing the new variable $y = x + b/(3a)$, the depressed cubic and its three displayed cases are still written in x. Replace x by y in those four displays, or explicitly state that the new variable is being renamed x.

51. **Page 241, subfield discussion:** The reference "as in Definition 4.4.1" should be "as in Definition 4.3.1".

52. **Page 244, integral-domain discussion:** "as given in Definition 3.5.6" should be "as given in Definition 3.3.5" (or "as given in Definition 4.1.1" for the later expanded definition).

53. **Page 246, Exercise 5:** The assertion fails for $R = \{0\}$, which is a ring under the operations of the integral domain D but is not a subring of D, because

its identity is not the identity of D. Add the hypothesis that R is not the zero ring.

54. **Page 248, Exercise 25:** Replace "except that it does not have the multiplicative identity of R" by "except that it does not contain the multiplicative identity of R_1".

55. **Page 252, Example 5.2.4:** Replace "not onto" by "not onto unless R is the zero ring". (For the zero ring R, the natural inclusion $\iota : R \to R[x]$ is onto, since $R[x]$ is again the zero ring.)

56. **Page 253, Example 5.2.6:** Replace "$\phi(1) = 1$" by "$\phi_u(1) = 1$".

57. **Page 253:** Replace "The previous example can generalized" by "The previous example can be generalized".

58. **Page 261, Exercise 15:** Replace "Exercise 6 (c) of Section 4.3" by "Exercise 6 (c) of Section 4.4".

59. **Page 261, Exercise 15:** "no nonzero root in $\mathbf{Z}_4[x]$" should be "no nonzero root in $\mathbf{Z}_4$". (Roots are elements of the coefficient ring, not polynomials.)

60. **Page 268, first line:** Insert a period after "$g(x) \in \langle p(x) \rangle$" before the sentence beginning "Thus".

61. **Page 268, paragraph after Definition 5.3.8:** Replace "This observations shows" by "This observation shows".

62. **Page 271, Exercise 7:** Replace "any ideal" by "any nonzero ideal". (If $I = \{0\}$, then the claim of part (a) is false, since $\{0\}$ contains no monic polynomial.)

63. **Page 271, Exercise 9:** "Let R be a commutative ring" should be "Let R be a nontrivial commutative ring". (The zero ring has no proper ideals, so the hypothesis that every proper ideal is prime holds vacuously, but the zero ring is not a field under the book's definition.)

64. **Page 282, last paragraph:** Replace "then $\{f(x) \in F[x] \mid f(u) = 0\}$ is an ideal of the ring $F[x]$" by "then $\{f(x) \in K[x] \mid f(u) = 0\}$ is an ideal of the ring $K[x]$".

65. **Page 286, middle of the page:** The displayed minimal-polynomial relation "$c_0 + c_1 u + \ldots + c_{n-1} u^{n-1} + x^n = 0$" should end with "$+u^n = 0$" rather than with "$+x^n = 0$".

66. **Page 287, Example 6.1.5:** In "$1 + I = \left(1 + x^2 + I\right)\left(\frac{1}{2} + \frac{2}{5}x - \frac{1}{5}x^2 + I\right)$", replace "$\frac{1}{2}$" by "$\frac{1}{5}$".

67. **Page 292, Example 6.2.5:** The displayed computation ends with an extra closing bracket. Delete the stray bracket.

68. **Page 295, introductory paragraph to Section 6.3:** Replace “passing though a point” by “passing through a point”.

69. **Page 298, proof of Lemma 6.3.5:** Replace “Given two circles in F” by “Given two circles over F”.

70. **Page 298, proof of Theorem 6.3.6:** “then $\sqrt{u}$ is constructible for all $u \in F$” should be “then $\sqrt{u}$ is constructible for all nonnegative $u \in F$” (since constructible numbers have to be real). Similarly, “Given $u \in F$” should be “Given a positive $u \in F$”.

71. **Page 301, after Definition 6.4.1:** “if E contains the splitting field of F” should be “if E contains a splitting field of $f(x)$ over K” (or, more explicitly: “if $f(x)$ splits into constant and linear factors in $E[x]$”).

72. **Page 303, Example 6.4.4:** Replace “can be expressed as element of F” by “can be expressed as an element of F”.

73. **Page 307, last paragraph:** In “identity element1is”, insert spaces to obtain “identity element 1 is”.

74. **Page 310, Example 6.5.2:** Replace “GF(p)” by “GF(2)”.

75. **Page 311, Example 6.5.3:** In the last sentence, replace “GF(3)” by “GF(2)”.

76. **Page 312, Corollary 6.5.12:** “For each positive integer n” should be “For each prime p and each positive integer n”.

77. **Page 316, proof of Proposition 6.6.6:** Replace “follows form” by “follows from”.

78. **Page 316, proof of Theorem 6.6.7:** Delete the stray opening quotation mark before the fourth equality in the displayed computation.

79. **Page 316, paragraph before Theorem 6.6.8:** In the last paragraph of the page, replace “$F(n) = \log f(n)$” by “$F(n) = \log G(n)$”. Also, this reduction requires the values of g (and hence of G) to be positive.

80. **Page 317, Theorem 6.6.8:** The multiplicative Möbius inversion formula is stated for an arbitrary function into a commutative ring R, but the exponents $\mu(m/n) = -1$ require multiplicative inverses and are not defined for arbitrary elements of R. Require $g : \mathbf{Z}^+ \to R^\times$ (and hence $G : \mathbf{Z}^+ \to R^\times$), or more generally let g take values in an abelian group written multiplicatively.

81. **Page 318, proof of Corollary 6.6.12:** Replace "$q^{n-1} + \cdots + q + 1$" by "$q^{m-1} + \cdots + q + 1$" in the last sentence.

82. **Page 319, Exercise 4:** Specify that the asserted roots u^{ip^k} are obtained for all integers $k \geq 0$.

83. **Page 320, Exercise 12(a)–(b):** Several mathematical symbols run into adjacent words. Insert spaces in "that$\mathcal{R}$ is", "operations$+$ and $*$", "$f \in \mathcal{R}$ has", and "$f(1)$ is".

84. **Page 321, Proposition 6.7.2:** Bad word spacing strikes again. Insert the missing spaces in "$a \in \mathbf{Z}$ with $p \nmid a$".

85. **Page 322, proof of Theorem 6.7.3:** Replace "multiplication by$a$defines" by "multiplication by a defines".

86. **Page 327, Exercise 6:** As written, the hypotheses permit $p = q$ and $t = 0$, in which case both displayed Legendre symbols are undefined. Require p and q to be *distinct* odd primes (equivalently, add $t \neq 0$), or extend the definition of the Legendre symbol to $\left(\dfrac{n}{p}\right) = 0$ for $p \mid n$.

87. **Page 328, historical note on constructible polygons:** The historical directions are reversed. Gauss proved the *sufficiency* of the Fermat-prime form for constructibility; Wantzel later proved the *necessity*. The criterion itself should read
$$n = 2^{\alpha} p_1 \cdots p_k,$$
where the p_i are *distinct* Fermat primes of the form $p_i = 2^{2^{m_i}} + 1$. Thus change Gauss's result to "if n has the form ...", identify the later result as the converse (the necessity), replace the displayed product beginning with p_2 by one beginning with p_1, and do not reuse the polygon variable n in the Fermat-prime exponent.

88. **Page 329, Chapter 7 introduction:** The text proposes finding "polynomial equations over $\mathbf{C}$ of degree 5 that cannot be solved by radicals". Over the base field $\mathbf{C}$, the roots already lie in the base field. Say "polynomial equations over $\mathbf{Q}$" or "equations with rational coefficients (and complex roots)".

89. **Page 330, first paragraph:** "which have no nontrivial normal subgroups" should be "which have no nontrivial proper normal subgroups". After all, every nontrivial group is itself a nontrivial normal subgroup.

90. **Page 330, discussion of projective special linear groups:** The assertion that "the factor group N/Z is simple except for the cases $n = 2$ and $F = \mathrm{GF}(2)$ or $\mathrm{GF}(3)$" needs the hypothesis $n \geq 2$. For $n = 1$, this factor

group (which is later called $\mathrm{PSL}_n(F)$) is trivial, and thus is not simple under Definition 3.8.10.

91. **Page 331, Example 7.1.2:** Insert the missing spaces in "let$H$" and "Since$N$", obtaining "let H" and "Since N".

92. **Page 338, paragraph preceding Example 7.2.1:** Replace "each elements" by "each element".

93. **Page 339, Example 7.2.1, last paragraph:** The three order-2 subgroups of S_3 are listed as $\{e, b\}$, $\{e, ab\}$, and $\{e, a^2\}$. The last set is not one of them. Replace $\{e, a^2\}$ by $\{e, a^2b\}$.

94. **Page 340, Example 7.2.2:** It is said that $a^i = a^{-i}$ "holds if and only if $i = 2$". In truth, this holds if and only if i is even (including $i = 0$).

95. **Page 341, Example 7.2.3:** Insert the missing space in "conjugate inS_n", obtaining "conjugate in S_n".

96. **Page 345, Exercise 20 (and the selected answer on page 525):** The book elsewhere defines D_n as the dihedral group of order $2n$, with a of order n. Here D_{12} is explicitly given with a of order 6, so the group has order 12; the selected answer repeats the inconsistent notation. Rename this group D_6, or change a to have order 12 and adjust the exercise and answer.

97. **Page 349, paragraph after proof of Proposition 7.3.4:** "Applying the above proposition to Example 7.3.6" should be "Applying the above proposition to Example 7.3.7".

98. **Page 350, paragraph after proof of Theorem 7.3.6:** "If we apply Theorem 7.3.6 to Example 7.3.5" should be "If we apply Theorem 7.3.6 to Example 7.3.6".

99. **Page 351, Exercise 4:** "Let G act on the subgroup H by conjugation" is not well-defined unless H is normal. The next clause introduces the correct G-set, namely the set S of conjugates of H. Replace the opening "Let G act on the subgroup H by conjugation, let S be the set of all conjugates of H" by "Let H be a subgroup of a group G. Let S be the set of all conjugates of H in G. Let G act by conjugation on the set S".

100. **Page 353, Exercise 18(b) from Section 7.3:** Replace "Given an example" by "Give an example".

101. **Page 353, proof of Theorem 7.4.1:** The theorem allows $\alpha = 0$, but the proof assumes $p \mid |G|$ and in Case 1 invokes a subgroup of order $p^{\alpha-1}$. Begin by observing that when $\alpha = 0$ the trivial subgroup has the required order, and then assume $\alpha \geq 1$ for the two-case argument.

102. **Page 363, paragraph preceding Lemma 7.5.11:** Replace "cyclic of order of 2" by "cyclic of order 2".

103. **Page 364, proof of Theorem 7.5.12:** Replace "$\varphi(p^k)$" by "$\varphi(2^k)$".

104. **Page 376, discussion before Example 7.7.1:** The claim "With two exceptions, when $n = 2$ and either $|F| = 2$ or $|F| = 3$, the groups $\mathrm{PSL}_n(F)$ are simple" holds only for $n \geq 2$. For $n = 1$, the group $\mathrm{PSL}_n(F)$ is trivial and thus not simple under the book's definition.

105. **Page 377, Example 7.7.2:** Replace "It can be shown the action" by "It can be shown that the action".

106. **Page 388, proof of Theorem 8.1.8:** In the first paragraph, "Since $f(x)$ has no repeated roots" should be "Since $x^{p^n} - x$ has no repeated roots".

107. **Page 391, proof of Proposition 8.2.3:** In the last paragraph, the factorization
$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_t)$$
of $f(x)$ omits its leading coefficient. Write
$$f(x) = c(x - r_1)(x - r_2) \cdots (x - r_t), \qquad c \neq 0.$$

108. **Page 396, proof of Lemma 8.3.4:** Replace "Dividing each of the solutions by a_1 still gives us a set of solutions" by "Dividing each entry of this solution by a_1 still gives us a solution".

109. **Page 396, proof of Lemma 8.3.4:** Replace "We can again relabel the indices on $x_2, \ldots, x_n$ and $u_2, \ldots, u_n$" by "We can again relabel the indices on $x_2, \ldots, x_{n+1}$ and $u_2, \ldots, u_{n+1}$".

110. **Page 397, Example 8.3.1:** Replace "Corollary 8.1.8" by "Theorem 8.1.8" (twice).

111. **Page 397, Example 8.3.1, last paragraph:** In "for any integer we have $\phi^t(x) = \phi^{t+rs}(x)$", add "$s$" after "integer".

112. **Page 399, proof of Theorem 8.3.8(c):** Insert the missing spaces in "If$u \in E$", "polynomial$p(x)$", and "then$\phi(u)$".

113. **Page 406, proof of Theorem 8.4.3:** The theorem permits $a = 0$, but the proof does not quite work in this case (since "the exponent i of ζ in $\phi(u) = \zeta^i u$" is not uniquely determined when $a = 0$). Thus, this case needs to be handled first (it is easy: $a = 0$ entails $F = K$, and the Galois group is trivial). Then assume $a \neq 0$ for the rest of the proof.

114. **Page 407, Theorem 8.4.4:** Add the hypothesis $\mathrm{char}(K) \neq p$ (in particular, characteristic zero suffices). In characteristic p, the field has only one pth root of unity, the Vandermonde matrix in the proof is not invertible, and the conclusion fails for nontrivial cyclic Artin–Schreier extensions of degree p.

115. **Page 408, proof of Lemma 8.4.5:** Replace "for $i = 1, \ldots, n$" by "for $i = 1, \ldots, m$" on line 4 of the proof.

116. **Page 408, proof of Theorem 8.4.6:** The proof uses F_{i-1} when $i = 1$ without defining F_0, and defines N_i only for $i = 1, \ldots, m-1$ although the displayed chain ends with $N_m = \{e\}$. Set

$$F_i = K(\zeta, u_1, \ldots, u_i), \qquad N_i = \mathrm{Gal}(F(\zeta)/F_i)$$

for $0 \leq i \leq m$. Then $F_0 = K(\zeta)$ and $N_0 = N$ and $N_m = \{e\}$.

117. **Page 409, converse proof of Theorem 8.4.6:** The first group in the "finite chain of subgroups" and the first field in the "ascending chain of subfields" are not indexed, yet the factor groups N_i/N_{i+1} and fields F_i are used immediately. Define

$$N_0 = \mathrm{Gal}(F/K(\zeta)), \quad N_m = \{e\}, \quad F_i = F^{N_i} \quad (0 \leq i \leq m),$$

so that $F_0 = K(\zeta)$, $F_m = F$, and $\mathrm{Gal}(F_{i+1}/F_i) \cong N_i/N_{i+1}$ for $0 \leq i < m$.

118. **Page 409, converse proof of Theorem 8.4.6:** The words around the formula $f(x)$ are run together. Insert spaces before and after the formula, yielding "show that $f(x)$ is solvable".

119. **Page 412, proof of Proposition 8.5.2(c):** Replace "$\Phi_d(x)$ with $d > n$" by "$\Phi_d(x)$ with $d < n$".

120. **Page 412, proof of Proposition 8.5.2(c):** "from Exercise 1 of Section 4.3" should be "from Exercise 1 of Section 4.4".

121. **Page 414, Corollary 8.5.5:** As stated for positive n, the classification omits the case $n = 1$: The polynomial $\Phi_1(x) = x - 1$ has trivial, hence cyclic, Galois group. Include 1 in the list (as in the standard classification) or state the corollary only for $n > 1$. This is also the omitted edge case in the cited Corollary 7.5.13 unless p^0 is explicitly intended.

122. **Page 415, Example 8.5.2:** In the Gauss–Wantzel form for a constructible regular polygon, the product begins with p_2. Replace "$n = 2^k p_2 \cdots p_m$" by "$n = 2^k p_1 \cdots p_m$".

123. **Page 415, proof of Theorem 8.5.6:** Replace "if it has dimension is n" by "if it has dimension n".

124. **Page 416, proof of Theorem 8.5.6:** From $|\Phi_n(q)| \geq (q-1)^{\varphi(n)}$ and $\Phi_n(q) \mid (q-1)$, the text immediately concludes $n = 1$. The displayed weak inequality alone does not exclude equality for $n > 1$. Instead, argue that for $n > 1$, every primitive nth root α^j is different from 1, whence $|q - \alpha^j| > q - 1$; the resulting strict inequality $|\Phi_n(q)| > (q-1)^{\varphi(n)}$ does give the contradiction.

125. **Page 417, Exercises 7 and 8:** In both exercises, replace "Let D be division ring" by "Let D be a division ring".

126. **Page 418, list of transitive subgroups of S_5:** The list of possible Galois groups for an irreducible polynomial $f(x)$ of degree 5 given here includes $\mathbf{Z}_4$. But $\mathbf{Z}_4$ cannot act transitively on five points (since $|\mathbf{Z}_4| = 4$ is not divisible by 5), hence does not belong into this list. The correct list is $S_5, A_5, F_{20}, D_5, \mathbf{Z}_5$.

127. **Page 419, proof of Lemma 8.6.4:** The statement that "each subgroup in the series is a transitive subgroup" incorrectly includes the last subgroup $N_k = \{(1)\}$. Say instead that repeated use of Lemma 8.6.3 shows that each *nontrivial* N_i is transitive; in particular N_{k-1} is transitive, which is what the conclusion needs.

128. **Page 420, proof of Proposition 8.6.5:** The inequality $q < p$ could use some justification. Here is why it holds: We have $q = [N_{i-1} : N_i] \mid [G : N_{k-1}]$ (since N_{i-1} is a subgroup of G, while N_{k-1} is a subgroup of N_i), but $[G : N_{k-1}] = \dfrac{|G|}{|N_{k-1}|} = \dfrac{p!}{p} = (p-1)!$, so that $q \mid [G : N_{k-1}] = (p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$. Since q is prime, this entails that q divides one of $1, 2, \ldots, p-1$. Thus, $q < p$.

129. **Page 420, Example 8.6.3:** Replace "The order of the Galois group is order $p(p-1)$" by "The order of the Galois group is $p(p-1)$".

130. **Page 421, definition of the discriminant:** The definition
$$\Delta = \prod_{i<j} (r_i - r_j)^2$$
of the discriminant Δ omits the leading-coefficient factor. It is therefore inconsistent with the next assertion that the discriminant of $ax^2 + bx + c$ is $b^2 - 4ac$.

    A correct definition of Δ proceeds as follows: For $f(x) = a_n \prod_i (x - r_i)$, define
$$\Delta = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2.$$

131. **Page 421, Proposition 8.6.6:** The "if" direction requires the additional hypothesis $\text{char}(K) \neq 2$. Indeed, in characteristic 2, changing the order of

two roots does not change the sign of $\prod_{i<j}(r_i - r_j)$, so that $\prod_{i<j}(r_i - r_j)$ always belongs to K and therefore Δ is always a square in K.

132. **Page 421, Example 8.6.4:** Replace "-216" by "-108".

133. **Page 424, Example 8.6.7:** In the last sentence, replace "the only transitive subgroup that contains a 4-cycle and a 3-cycle is S_4" by "... is S_5".

134. **Page 425, Exercise 2:** This needs additional requirements that $f(x)$ be separable and $\text{char}(K) \neq 2$. Without separability, an irreducible cubic in characteristic 3 can have trivial Galois group and zero discriminant; in characteristic 2, Proposition 8.6.6 itself does not apply (see above).

135. **Page 431, proof of Proposition 9.1.6:** Replace all three occurrences of "R" by "D".

136. **Page 434, Exercise 5:** Replace "for all $x, y \in D$" by "for all nonzero $x, y \in D$".

     More importantly, the conclusion $\delta(1) = 1$ is false under Definition 9.1.1, whose codomain includes zero: if D is a field, then $\delta(x) = 0$ for every $x \neq 0$ is a multiplicative Euclidean norm. Add the assumption that δ is not identically zero, assume more strongly that D is not a field, or require Euclidean norms to take positive-integer values. Under any of these corrections, the intended conclusions do follow.

137. **Page 436, Definition 9.2.4:** Replace "nonconstant" by "nonzero". There is no reason to exclude nonzero constant polynomials from primitivity.

138. **Page 437, Lemma 9.2.6(a):** Require a, b, c, d to be nonzero. As written, the statement fails when D is a field: for example, $a = b = 0$ and $c = d = 1$ satisfy the stated relative-primality and associate product hypotheses (indeed, Definition 9.2.3 makes any two elements of a field relatively prime, since the field has no irreducible elements), but a and c are not associates.

139. **Page 437, Lemma 9.2.6(b):** Require $f \neq 0$. (Otherwise, the uniqueness part becomes false.)

140. **Page 438, proof of Proposition 9.2.7:** Replace "gives rise to a factorization $f(x) = tg^*(x)h^*(x)$" by "gives rise to a factorization $f(x) = \frac{s}{t}g^*(x)h^*(x)$".

141. **Page 438, proof of Theorem 9.2.8, first paragraph:** Restore the missing spaces in "Let$f(x)$be a nonzero element of$D[x]$", "that$f(x)$is", and "degree of$f(x)$".

142. **Page 441, Exercise 6(c):** Replace "and $x + \langle s \rangle = a + \langle s \rangle$" by "$x + \langle s \rangle = b + \langle s \rangle$".

143. **Page 441, Exercise 9(c):** Replace "$\cup_{k=1}^{n}$" by "$\cup_{k=0}^{n}$". (It is well possible that $n = 0$.)

144. **Page 444, proof of Theorem 9.3.3:** Replace "must differ from $m + ni$ by a unit" by "must differ from either $m + ni$ or $m - ni$ by a unit".

145. **Page 449, proof of Lemma 9.3.7(c):** Replace "or $z = [0]$" by "or $[z] = [0]$".

146. **Page 449, proof of Lemma 9.3.7(c):** Replace "It follows from by part (b)" by "It follows from part (b)".

147. **Page 451, end of the proof of Theorem 9.3.8:** To complete the minimal-descent contradiction, we need not just some new solution (x^*, y^*, z^*) whose third entry z^* is divisible by $1 - \omega$ but not by $(1 - \omega)^k$, but we need such a solution that additionally satisfies conditions (i) and (ii) from page 450. Lemma 9.3.7(c) says that one of x_*^3, y_*^3, z_*^3 is divisible by $(1 - \omega)^4$; because exactly one of x_*, y_*, z_* is divisible by $1 - \omega$ (since exactly one of u, v, w is divisible by $1 - \omega$), it must be z_*^3. Hence $(1 - \omega)^4 \mid z_*^3$, so the exponent of $1 - \omega$ in z_* is at least 2. Moreover, if our solution (x^*, y^*, z^*) does not satisfy condition (i) from page 450, then we can divide x^*, y^*, z^* by their gcd without breaking condition (ii). The resulting solution then satisfies both conditions (i) and (ii) and is therefore among those over which the minimal exponent k was chosen.

148. **Page 452, Exercise 6(b):** Replace "show this it *suffices*" by "show that it *suffices*".

149. **Page 453, opening description of Chapter 10:** Insert "finite" before "groups in this class". (The claim that nilpotent groups are direct products of groups of prime-power order applies only to finite nilpotent groups. For example, the infinite cyclic group is nilpotent but is not such a direct product.)

150. **Page 455, proof of Theorem 10.1.4, (2) implies (3):** Replace "This implies the P is normal" by "This implies that P is normal".

151. **Page 455, proof of Theorem 10.1.4, (3) implies (4):** "for some integers $k_1, \ldots, k_n$" should be "for some integers $k_1, \ldots, k_i$".

152. **Page 456, proof of Lemma 10.1.6:** "The second Sylow theorem (Theorem 7.7.4)" should be "The second Sylow theorem (Theorem 7.4.4(a))".

153. **Page 458, first paragraph:** In "Let $N' = \phi(N)$ and $K = \phi(K)$", replace "$K = \phi\,(K)$" by "$K' = \phi(K)$".

154. **Page 459, Example 10.2.3:** For arbitrary additive $G_1 \leq F$ and multiplicative $G_2 \leq F^\times$, the set G is not necessarily a subgroup of $\mathrm{GL}_2\,(F)$: Indeed,

closure requires $ax \in G_1$ for all $a \in G_2$ and $x \in G_1$. So this requirement needs to be added in order to obtain a subgroup G.

155. **Page 459, Example 10.2.3:** In "shows that shows that", delete one occurrence of "shows that".

156. **Page 462, Exercise 6(b):** The displayed set K includes the singular matrix obtained when $a_{22} = 0$, so as written it is not even a subset of $\mathrm{GL}_2(\mathbf{R})$. Add the condition $a_{22} \neq 0$ to the definition of K.

157. **Page 462, Exercises 11(a) and 11(b):** In "show that that G_1" and "show that that G_2", delete the second "that".

158. **Page 463, definition of Heisenberg group:** Replace "G" by "H" in "If $F = \mathrm{GF}\,(p)$, then G is called".

159. **Page 463, semidirect-product setup:** Replace "$g_2 = h_2k_2$ in the" by "$g_2 = n_2k_2$ in the".

160. **Page 465, construction of N' in an external semidirect product:** On the penultimate line of the calculation of $(n,k)\,(n',e)\,(n,k)^{-1}$, the second coordinate is printed as "3". It must be the identity "e".

161. **Page 465, same paragraph:** The calculation is meant to prove that the conjugate lies in N', but the text only says that it lies in $N \rtimes_\alpha K$, which is automatic. Replace the conclusion by "is in N', so N' is normal".

162. **Page 465, Example 10.3.2:** "external direct product" should be "external semidirect product".

163. **Page 467, paragraph after Example 10.3.3:** Replace "external direct product $N \rtimes_\alpha K$" by "external semidirect product $N \rtimes_\alpha K$".

164. **Page 468, Proposition 10.3.7:** "for all $x, y \in X$" should be "for all $x, y \in N$".

165. **Page 468, final sentence of Example 10.3.4:** Replace "an linear action" by "a linear action".

166. **Page 469, Example 10.3.6, second sentence:** Replace "$\mathrm{GL}_n(F)$. and let N" by "$\mathrm{GL}_n(F)$, and let N".

167. **Page 472, proof of Proposition 10.4.3:** Replace "in unambiguous" by "is unambiguous".

168. **Page 473, proof of Proposition 10.4.4:** Add a full-stop after "isomorphic to $C_4 \cong \mathbf{Z}_5^\times$ or V".

169. **Page 474, paragraph before Proposition 10.4.5:** Replace "if $|G|$ is p^n, $n = pq^m$, or $n = p^2q$" by "if $|G|$ is p^n, pq^m, or p^2q".

170. **Page 475, opening of the proof of Proposition 10.4.6:** Cauchy's theorem does not by itself rule out a nonabelian simple group of prime-power order. Replace "Cauchy's theorem" by "Theorem 7.2.8" (the theorem that a finite p-group has nontrivial center).

171. **Page 475, same proof:** Replace "Examples 7.4.2 provides" by "Example 7.4.2 provides".

172. **Page 475, Exercise 1:** The displayed matrices do not form a subgroup for an arbitrary subgroup $H \leq \mathbf{C}^\times$. For example, if $H = \{1\}$, the second matrix
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
belongs to the displayed set, but its square $-I$ does not. It is enough to assume that H is stable under complex conjugation and contains -1 (or, more restrictively, that H is a subgroup of the unit circle containing -1). The subsequent choice $H = C_{2n}$ has these properties.

173. **Page 477, proof of Lemma 10.5.1:** Replace "0 is all other rows" by "0 in all other rows".

174. **Page 477, last line:** "plane R^2" should be "plane $\mathbf{R}^2$".

175. **Page 479, half-angle calculation for the reflection line:** The equations
$$\cos(\theta/2) = \sqrt{\frac{1+\cos\theta}{2}}, \qquad \sin(\theta/2) = \sqrt{\frac{1-\cos\theta}{2}}$$
lose signs when $0 \leq \theta < 2\pi$; in particular, the first one fails for $\pi < \theta < 2\pi$. The subsequent replacement of $\sqrt{1-\cos^2\theta}$ by $\sin\theta$ has the same problem.

    Instead, the slope $m = \tan(\theta/2)$ of the x-axis rotated by $\theta/2$ in a counter-clockwise direction can be computed using the signed half-angle identity
$$\tan(\theta/2) = \frac{1-\cos\theta}{\sin\theta} = \frac{1-c}{s}.$$
    This gives the claimed reflection line without the invalid square roots.

176. **Page 480, proof of Theorem 10.5.4, Case 1:** Replace "where $k \in \mathbf{Z}^+$" by "where $k \in \mathbf{Z}_{\geq 0}$".

    Replace "Since $A_\theta, A_\rho \in G$" by "Since $A_\theta, A_\mu \in G$".

177. **Page 481, Theorem 10.5.4:** This is not literally true, since the book defines D_n for $n \geq 3$ only, but a finite subgroup of $\mathrm{O}_2(\mathbf{R})$ can also be the dihedral group D_2 (aka the Klein four-group).

    To fix this, define the dihedral group D_n for each positive integer n as the semidirect product of the cyclic group $\mathbf{Z}_n$ by $\mathbf{Z}_2$, where $\mathbf{Z}_2$ acts on $\mathbf{Z}_n$ by

$x \mapsto -x$ (or $x \mapsto x^{-1}$, if you write $\mathbf{Z}_n$ multiplicatively). Note that D_1 is isomorphic to $\mathbf{Z}_2$ (so it is not really necessary), but D_2 is isomorphic to the Klein four-group.

178. **Page 481, final sentence of Theorem 10.5.4:** Replace "that $B \cong D_n$" by "that $G \cong D_n$".

179. **Page 482, proof of Proposition 10.6.2:** Replace "$(f(X-Y)) \cdot (f(X-Y))$" by "$(f(X) - f(Y)) \cdot (f(X) - f(Y))$".

180. **Page 484, Proposition 10.6.9 and Theorem 10.6.10:** Replace "$O_2(\mathbf{R}^2)$" by "$O_2(\mathbf{R})$" throughout these two results and their proofs.

181. **Page 484, paragraph after Theorem 10.6.10:** Replace "straight forward" by "straightforward".

182. **Page 485:** Replace "H. S. M, Coxeter" by "H. S. M. Coxeter".

183. **Page 486, paragraph before the exercises:** Replace "a translation on a line parallel to the line of reflection" by "a translation along a line parallel to the line of reflection".

184. **Page 492, construction of Z, Q, and R:** The constructions specify equivalence relations but then speak as though the raw pairs or sequences themselves were the numbers. Define $\mathbf{Z}$ and $\mathbf{Q}$ as sets of *equivalence classes* of the indicated pairs, and $\mathbf{R}$ as the set of equivalence classes of Cauchy sequences. In particular, the sentence identifying $\mathbf{N}$ with "the set of ordered pairs (a, b) such that $a \geq b$" is false literally: that set has many representatives of each nonnegative integer. Instead embed

$$n \longmapsto [(n, 0)],$$

or say that the nonnegative integer classes are precisely those having a representative (a, b) with $a \geq b$.

185. **Page 493:** Replace "various text books" by "various textbooks".

186. **Page 494, Proposition A.3.6:** The labels jump from (h) to (k), then to (m) and (n). Relabel the final three parts consecutively as (i), (j), and (k).

187. **Page 496, proof of Theorem A.4.3:** Replace "natural numbers" by "positive integers". (The natural numbers include 0 by definition.)

188. **Page 498, Exercise A.4.15:** The asserted identity fails for $n = 1$: its left-hand side is 1, not 0. Add the hypothesis $n \geq 2$.

189. **Page 498, Exercise A.4.19:** The strict inequality $(1 + h)^n > 1 + nh$ fails when $h = 0$. Either replace $>$ by $\geq$, or retain the strict inequality and add $h \neq 0$.

190. **Page 500, polar form of a complex number:** The definitions $\cos\theta = a/r$ and $\sin\theta = b/r$ divide by r and therefore apply only when $a + bi \neq 0$. Add this hypothesis. The zero complex number may instead be represented by $r = 0$ with arbitrary angle θ.

191. **Page 500, proof of Corollary A.5.3:** The proof exhibits n distinct roots of $z^n - 1$, but it does not say why there are no others. Add an invocation of Corollary 4.1.12, which says that a nonzero polynomial of degree n has at most n distinct roots.

192. **Page 505, Section A.6.2:** For a real quadratic with discriminant zero, the assertion
$$ax^2 + bx + c = (mx + k)^2 \qquad (m, k \in \mathbf{R})$$
is false when $a < 0$. Say instead that the quadratic is a real scalar multiple of the square of a linear polynomial (indeed, $a(x + b/(2a))^2$), or add the hypothesis $a > 0$ to the displayed square characterization.

193. **Pages 505–509, discriminants of quadratics and cubics:** Replace "imaginary" by "nonreal complex" when describing roots and the quantities whose cube roots occur. For example, when a real cubic has one real root and a conjugate pair, the nonreal roots need not be purely imaginary; likewise the two radicands on page 509 generally have nonzero real parts.

194. **Page 506, solution of the reduced cubic:** The substitution $y = z - p/(3z)$ requires $z \neq 0$. Handle the degenerate case $p = q = 0$ separately: then the reduced equation is simply $y^3 = 0$, while its resolvent supplies only $z = 0$, for which the displayed substitution is undefined.

195. **Page 506, discriminant of a cubic:** Replace "in F.4" by "in Section A.6.4".

196. **Page 510, general quartic equation:** Remove "$a \neq 0$" from the first displayed equation in Section A.6.5.

197. **Page 511, Descartes's solution of the quartic:** The formulas for m and n involve division by k, although the resolvent in k^2 can have the root $k^2 = 0$ (in particular when $q = 0$). Require $k \neq 0$ for this derivation and treat $k = 0$ separately: then $q = 0$, and the biquadratic can be factored by choosing $m + n = p$ and $mn = r$.

198. **Page 513, Definition A.7.1:** Replace "A vector space over the field F is set V" by "A vector space over the field F is a set V".

199. **Pages 513–515, Definitions A.7.3–A.7.5:** Span and linear independence are defined only for a displayed finite set $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$, but the later results use arbitrary subsets. Extend the definitions to arbitrary S using finite linear combinations, and define independence by requiring every finite linear relation to be trivial.

200. **Page 525, selected answer to Exercise 7.7.15:** The exercise asks for the orders of $\mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$, and $\mathrm{PSL}_n(F)$, but the selected answer gives only the first. For $|F| = q$, complete it with

$$|\mathrm{SL}_n(F)| = \frac{|\mathrm{GL}_n(F)|}{q-1}, \qquad |\mathrm{PSL}_n(F)| = \frac{|\mathrm{GL}_n(F)|}{(q-1)\gcd(n, q-1)}.$$

201. **Page 526, selected answer to Exercise 8.1.2:** The exercise asks for an explicit formula for each element of the Galois group, but the answer only names a generator. Add that the three automorphisms of $\mathrm{GF}(2^3) / \mathrm{GF}(2)$ are

$$x \longmapsto x, \qquad x \longmapsto x^2, \qquad x \longmapsto x^4.$$

D. Additional bibliography, index, and editorial recommendations

D.1. Bibliography

- **Page 516:** Add terminal periods to the Jacobson and Halmos entries.
- **Page 516:** In "Niven, I. Irrational Numbers", add a comma after "I.".
- **Page 517:** Add a terminal period to the Hall entry.
- Consider standardizing publisher punctuation ("Dover Publications Inc." versus "Dover Publications, Inc."), edition typography, and capitalization of titles and volume designations.

D.2. Index

- **Page 534, "group(s), exponent of":** Remove the stray trailing comma after "148".
- **Page 538, "permutation(s), even":** Add the missing comma after "even".
- A final mechanical pass should standardize entries that alternate between noun-first and inverted forms (for example, "transitive subgroup" versus "subgroup, transitive").

D.3. Editorial recommendations

- **Use a single convention for dihedral groups.** Most of the book uses D_n for the group of order $2n$, but Exercise 7.2.20 and its selected answer use D_{12} for a group of order 12. This is especially risky in a textbook because both conventions occur in the literature.

- **Standardize theorem labels in references.** The most common reference errors are correct numbers paired with the wrong label ("Corollary" instead of "Theorem") and references to the right topic in the wrong section.
- **Give Chapter 10 an additional notation pass.** This chapter contains a noticeably higher concentration of duplicated words, primed/unprimed symbols, and mismatched ambient sets than the earlier chapters.
- **Preserve the leading coefficient in discriminant discussions.** The monic convention in the appendix is coherent, but Chapter 8 immediately discusses nonmonic quadratics. Stating the full discriminant definition once will keep both discussions consistent.

E. Corrections to the student solutions booklet

In this section, page numbers refer to the printed page numbers in the booklet *Selected Solutions for Students to Accompany Abstract Algebra, Fourth Edition* (downloadable from `https://www.johnabeachy.com/abstractalgebra`); the roman-numbered front matter is cited in the same way.

1. **Page iii, Contents:** Change the second occurrence of "3.6" (before "Cosets, Normal Subgroups, and Factor Groups") to "3.8". Also replace "Homomophisms" by "Homomorphisms".
2. **Page v, To the Student:** Replace "everthing" by "everything".
3. **Page 1, solution to Exercise 1.1.17:** Replace "$k = n^2 - m^2$" by "$k = m^2 - n^2$" in the first sentence.
4. **Page 5, solution to Exercise 2.1.3(d):** In "for all $x \in \mathbf{R}$, This shows", replace the comma by a period.
5. **Page 6, solution to Exercise 2.2.11(d):** Replace "the horizontal line through y" by "the horizontal line at height y".
6. **Page 7, solution to Exercise 2.2.12(d):** Replace "then $(\lambda a_1)\,x + (\lambda b_1)\,y + (\lambda c_1)\,z = 0$" by "then $(\lambda a_2)\,x + (\lambda b_2)\,y + (\lambda c_2)\,z = 0$".
7. **Page 8, solutions to Exercise 2.2.12(h)–(j):** These solutions confuse the image of an affine line with its projective closure. If $f(x,y) = [x,y,1]$ and

   $$\ell = \{(x,y) \in \mathbf{R}^2 \mid ax+by+c=0\}, \qquad L = \{[x,y,z] \in \mathbf{P}^2 \mid ax+by+cz=0\},$$

   then

   $$f(\ell) = L \cap \{[x,y,z] \mid z \neq 0\},$$

not L itself. Thus in part (i) the displayed common point only proves that the two projective closures meet; the literal equality of the images of the intersection and the intersection of the images follows instead from the injectivity of f. In part (j), the images of two parallel affine lines are still disjoint, while their projective closures meet in a point at infinity. Accordingly, the final sentence should say that all *projective* lines in $\mathbf{P}^2$ intersect.

8. **Page 11, solution to Exercise 3.1.13:** In the last parenthetical sentence, replace "$(2-1) * a = 1$" by "$(2-a) * a = 1$".

9. **Page 15, solution to Exercise 3.3.19:** Replace "$ab = e$ implies $b \neq a$" by "$ab = e$ implies $b = a$". (This contradicts the choice of distinct a and b, and hence proves $ab \neq e$.)

10. **Page 15, solution to Exercise 3.3.21:** The label of the last row of the multiplication table should be a^2b, not a^b.

11. **Page 16, solution to Exercise 3.4.26:** In the computation of $\phi(a) + \phi(b)$, replace "$mb - m1$" by "$mb - m$".

    In the final note, if $\theta(x) = x - 1$ and $\psi(x) = mx$, then the required composition is $\phi = \theta \circ \psi$, not "$\phi = \psi\theta$".

12. **Page 17, solution to Exercise 3.5.13:** The conclusion "$c \in \{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$" could use more explanation: Let q be the remainder of tr modulo m. Thus, $tr \equiv q \pmod{m}$ and $0 \leq q < m$. Now, $o(a) = n = mk$ and $k \cdot tr \equiv kq \pmod{mk}$ (since $tr \equiv q \pmod{m}$), so that $a^{k \cdot tr} = a^{kq}$. Thus, $c = a^{k \cdot tr} = a^{kq} \in \{e, a^k, a^{2k}, \ldots, a^{(m-1)k}\}$ (since $0 \leq q < m$).

13. **Page 18, solution to Exercise 3.7.6:** Exercise 2.1.11 only shows that $[x]_n \mapsto [x]_m$ is a well-defined map into $\mathbf{Z}_m$. To see that its displayed codomain is really $\mathbf{Z}_m^\times$, add that $\gcd(x, n) = 1$ and $m \mid n$ imply $\gcd(x, m) = 1$.

14. **Page 18, alternate solution to Exercise 3.7.14:** "determinant homomorphism from $\mathrm{GL}_n(R)$ to $\mathbf{R}$" should be "determinant homomorphism from $\mathrm{GL}_n(\mathbf{R})$ to $\mathbf{R}^\times$".

15. **Page 23, solution to Exercise 4.3.20:** In the line for $[x]^3$, remove the mismatched closing parenthesis in "$[4x + 2 + x)]$".

    In the comment, replace "$\mathbf{Z}_3/\langle x^2 + x - 1\rangle$" by "$\mathbf{Z}_3[x]/\langle x^2 + x - 1\rangle$".

16. **Page 27, solution to Exercise 5.3.32(c):** The argument proves only $I \subseteq 2^k R$. For the reverse inclusion, argue that $u = 2^k v \in I$ with v odd. Since $1/v \in R$, it follows that $2^k = u/v \in I$, and hence $2^k R \subseteq I$.

17. **Page 27, solution to Exercise 5.3.32(d):** Replace "and so $\dfrac{m}{n} = \dfrac{mu + mv2^k}{n}$" by "and so $\dfrac{m}{n} = mu + \dfrac{mv2^k}{n}$".

18. **Page 28, solution to Exercise 5.3.32(d):** After proving that each coset has a unique representative r with $0 \le r < 2^k$ and checking the homomorphism laws, the solution establishes only that ϕ is onto. Add a justification that it is one-to-one: if $\phi(r + 2^k R) = [r]_{2^k} = 0$, the chosen range for r forces $r = 0$.

19. **Page 30, solution to Exercise 6.1.7:** In the last sentence, replace "$\sqrt{v} + \sqrt{v}$" by "$\sqrt{u} + \sqrt{v}$".

20. **Page 30, Section 6.2 heading:** Replace "Finite and Algebraic Elements" by "Finite and Algebraic Extensions".

21. **Page 30, solution to Exercise 6.2.5:** Replace "contracts the assumption" by "contradicts the assumption".

22. **Page 31, solution to Exercise 6.2.7:** The proof notes only that $n \mid [F : K]$. It must also use $m \mid [F : K]$, since $K(u) \subseteq F$. As $\gcd(m, n) = 1$, this gives $mn \mid [F : K]$; together with $[F : K] \le mn$, it yields $[F : K] = mn$.

23. **Page 33, solution to Exercise 6.5.15:** In the characteristic 2 case, handle $u = 1$ before dividing into the two possibilities for $1 + u$. If $u = 1$, then $F^\times = \langle u \rangle = \{1\}$ and $F = \mathrm{GF}(2)$ immediately; otherwise the printed argument applies.

24. **Page 35, solution to Exercise 7.2.22:** Replace "a divisor of G" by "a divisor of $|G|$".

25. **Pages 39–40, solution to Exercise 7.5.10:** In the decomposition of H, replace "$\sum_{i=1}^{t} \beta_i = k$" by "$\sum_{i=1}^{s} \beta_i = k$".

    The induction also needs two repairs. Once we know that the number of elements of order p gives $s = t$, we conclude that multiplication by p has kernel of size p^t on both G and H. For $j \ge 2$, every element of order p^{j-1} in pG has exactly p^t preimages, all of order p^j; hence pG and pH have the same number of elements of each order. Induction therefore gives $pG \cong pH$. Uniqueness of the cyclic decomposition now shows that the multisets

    $$\{\alpha_i - 1 \mid \alpha_i > 1\} \quad \text{and} \quad \{\beta_i - 1 \mid \beta_i > 1\}$$

    agree. Since $s = t$, the number of exponents α_i equal to 1 also agrees with the number of exponents β_i equal to 1, and therefore we obtain $G \cong H$. The printed componentwise conclusion $\alpha_i - 1 = \beta_i - 1$ overlooks the cyclic factors that become trivial after multiplication by p.

26. **Page 41, solution to Exercise 7.6.7:** Replace "observing that fact K_2 has index 2" by "observing that K_2 has index 2".

27. **Pages 41–42, solution to Exercise 7.6.10(b):** In the case $p = q$, the displayed series proves solvability only after normality is checked. A subgroup H of

order p^2 has index p in G, so $H \lhd G$; moreover, H is abelian, so every subgroup K of order p is normal in H. Thus $G \supset H \supset K \supset \{e\}$ is indeed a subnormal series with abelian factors.

(Alternatively, the case $p = q$ also follows directly from Theorem 7.6.3.)

28. **Page 42, solution to Exercise 7.6.14:** After obtaining $\phi(N) \subseteq N$, add that $|\phi(N)| = |N|$ because ϕ is an automorphism. Hence $\phi(N) = N$, as required for N to be characteristic.

29. **Page 49, solution to Exercise 8.5.12:** In the congruence for $\Phi_{105}(x)$ modulo x^{25}, the final term "$-x^{24}$" is printed twice. Delete one occurrence. (The final displayed polynomial has the correct coefficient.)

30. **Pages 49–50, solution to Exercise 8.6.5:** Abstract isomorphism does not preserve transitivity: the subgroup V is isomorphic to H_1, although V is transitive and H_1 is not. Repair the argument using conjugacy. Every subgroup of order 4 lies in a Sylow 2-subgroup P, and some conjugation carries P to the displayed copy of D_4 (by the second Sylow theorem). The conjugate of the subgroup is then one of H_1, H_2, or H_3, and conjugation preserves transitivity. Here H_1 is not transitive, H_2 is cyclic and transitive, and $H_3 = V$ is transitive. The earlier order-8 case should likewise use conjugacy of Sylow 2-subgroups, rather than merely their abstract isomorphism with D_4.

31. **Page 50, solution to Exercise 8.6.8:** Replace "a 5-cyclic" by "a 5-cycle".

32. **Page 51, solution to Exercise 9.2.8:** The proof of the converse begins by choosing a nonzero $x_1 \in I$, which is impossible for $I = (0)$. First dispose of this case: the zero ideal is generated by 0 (or by the empty set). Then assume $I \neq (0)$ and continue as printed.

33. **Page 52, solution to Exercise 9.2.9(c):** The proposed set $\mathcal{B}$ omits the degree-zero generators. Replace "$\cup_{k=1}^{n}$" by "$\cup_{k=0}^{n}$".

    In the case $\deg f = k \geq n$, the "repeat the argument using the generators of I_n" argument is somewhat underexplained. In more detail, this argument proceeds as follows: We have $a \in I_k = I_n$ (by part (b), since $k \geq n$), and thus $a = \sum_{j=1}^{m(n)} r_j a_{jn}$ for some $r_j \in R$, where each a_{jn} is the x^n-coefficient of $p_{jn}(x)$. Hence, the polynomial $f(x) - \sum_j r_j x^{k-n} p_{jn}(x)$ has lower degree than $f(x)$, and still cannot be expressed as a linear combination of elements of $\mathcal{B}$.

34. **Page 52, Sarges's proof of the Hilbert basis theorem:** Replace "for $1 \leq i < k-1$" by "for $1 \leq i < k$" when describing the polynomials already chosen before f_k.

35. **Page 52, Sarges's proof of the Hilbert basis theorem:** Replace "be the degree f_i" by "be the degree of f_i".

36. **Page 54, solution to Exercise 9.3.5(i):** Replace "such that $x = k^2$" by "such that $s = k^2$".

    Replace "a solution $\left(a^2, b^2, k\right)$" by "a solution (a, b, k)".

37. **Page 54, Exercise 9.3.6(b):** Replace "show this it *suffices*" by "show that it *suffices*".

38. **Page 55, solution to Exercise 10.1.5(b):** The proof of the converse reads rather confusingly when $k = 0$ or $k = 1$; in these cases, the ascending central series stabilizes either immediately or after one step, and some of the arguments given do not apply. It is probably better to explain things more rigorously: Any $j \in \{1, 2, \ldots, k\}$ satisfies

    $$D_{2^j m} / Z(D_{2^j m}) \cong D_{2^{j-1} m}$$

    (by the Lemma and by what was said just before it). Thus, by induction over i, we can easily see that the ascending central series of D_n satisfies

    $$D_n / Z_i\left(D_n\right) \cong D_{2^{k-i} m} \qquad \text{for each } i \in \{0, 1, \ldots, k\},$$

    and thus in particular $D_n / Z_k\left(D_n\right) \cong D_m$. If $m > 1$, then $Z\left(D_m\right) = \{e\}$, which entails $Z_{k+1}\left(D_n\right) = Z_k\left(D_n\right)$. Thus, if $m > 1$ (equivalently, if n is not a power of 2), the ascending central series of D_n stabilizes at $Z_k(D_n)$ and never reaches D_n.

39. **Page 57, Exercise 10.2.8:** Replace "isomorpic" by "isomorphic".

40. **Page 58, solution to Exercise 10.3.7:** Replace both occurrences of "identity" in "We can identity ..." by "identify".

41. **Page 59, solution to Exercise 10.3.8(b):** The matrix

    $$\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$$

    has order 4 for $a = 2, 3$, but has order 2 for $a = 4 = -1$ (unless it is the identity, which cannot occur here since $a \neq 1$). Thus replace "has order 4 for $a = 2, 3, 4$" by "has order 4 for $a = 2, 3$ and order 2 for $a = 4$". The conclusion that F_{20} has no element of order 10 remains valid.

42. **Page 62, solution to Exercise 10.4.10:** Delete the duplicated "and" in "and and $10 \cdot 2$"; replace "sybgroup" by "subgroup"; replace "which isomorphic" by "which is isomorphic"; and replace "G is belongs" by "G belongs".

F. Corrections to the student study guide

In this section, page numbers refer to the printed page numbers in the booklet *Abstract Algebra: A Study Guide for Beginners* (downloadable from `https://www.johnabeachy.com/abstractalgebra`); the roman-numbered front matter is cited in the same way.

1. **Page 5:** Replace "then are certainly congruent" by "then they are certainly congruent".

2. **Pages 6 and 94, Problem 1.2.39:** Replace "module 20" by "modulo 20".

3. **Page 9:** Replace "if has an element" by "if it has an element".

4. **Pages 9 and 98, Problem 1.4.45:** In part (a), replace "for not" by "but not". In part (c), replace "such $(p-1)/2$ is even" by "such that $(p-1)/2$ is even".

5. **Pages 15 and 108, Problem 2.1.35:** Replace "such a that" by "such that".

6. **Pages 19 and 113, Problem 2.3.21:** Delete the trailing comma in the cycle $(2,4,9,7,)$.

7. **Page 23:** Replace "The process the ended" by "The process that ended".

8. **Pages 26 and 121, Problem 3.1.39:** For $c \neq 0$, the expression $(az+b)/(cz+d)$ has a pole, so it does not define a function $\mathbf{C} \to \mathbf{C}$. Replace $\mathbf{C}$ by the Riemann sphere $\widehat{\mathbf{C}}$ and interpret the formula at the pole and at infinity, or reformulate the problem with appropriate domains.

9. **Page 28, Problem 3.1.50:** Replace "definied" by "defined".

   More importantly, the displayed operation is not closed on the stated set: its first component ad can vanish when $d = 0$. Replace "$(a,b) * (c,d) = (ad, bc+d)$" by "$(a,b) * (c,d) = (ac, bc+d)$" in order to avoid this issue (and obtain a more meaningful operation, too). This is the operation obtained by identifying (a,b) with the matrix $\left[\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right]$.

10. **Pages 29 and 125, Problem 3.2.38(a):** Replace "a subgroup of G" by "a subgroup of $\mathrm{Sym}(S)$".

    In the hint, replace "$\sigma(V) = V$ for all $\sigma \in \mathrm{Sym}(S)$" by "$\sigma(V) = V$ for all $\sigma \in H$".

11. **Page 36:** Replace "and the transferred" by "and then transferred".

12. **Pages 39 and 146, Problem 3.5.34:** Replace "Use the the result" by "Use the result".

13. **Pages 44 and 153, Problem 3.7.32:** Replace "$\phi : G_1 \to G_2$" by "$\phi : G \to G$".

14. **Pages 44 and 153, Problem 3.7.33:** Replace "$\phi^2 = \phi^2$" by "$\phi^2 = \phi$".
15. **Pages 57 and 172, Problem 4.2.33:** Insert the missing closing parentheses in "deg$(f(x)$" and "deg$(g(x)$", and replace "such f" by "such that f".
16. **Pages 65 and 187, Problem 5.1.37(a):** Replace "a an idempotent" by "a is an idempotent".
17. **Pages 65 and 187, Problems 5.1.38 and 5.1.39:** Replace "an unit" by "a unit".
18. **Page 69, Answers and Hints:** Replace "R is an field" by "R is a field".
19. **Pages 72 and 203, Problem 5.3.48(e):** Replace "If L is and ideal" by "If L is an ideal".
20. **Page 72, Problem 5.3.54:** The strict inclusion "$I_n \subset I_m$" cannot hold whenever $n \leq m$, since equality of the indices is allowed. Either replace $n \leq m$ by $n < m$, or replace $\subset$ by $\subseteq$.
21. **Page 73, Problem 5.3.60(b):** Delete the unmatched opening parenthesis on the left-hand side. The assertion should read
$$I(J \cap K) \subseteq IJ \cap IK.$$
22. **Page 80:** Delete the duplicated "to" in "one way to to construct", and replace "passing though" by "passing through".
23. **Page 80, Theorem:** Replace "$n = 2^k p_2 \cdots p_m$" by "$n = 2^k p_1 p_2 \cdots p_m$".
24. **Page 86, solution to Problem 1.1.38:** Replace "$3 = (1)\,(n^2+n+1) + (-n-2)(n+1)$" by "$3 = (1)\,(n^2+n+1) + (-n-2)(n-1)$".
25. **Page 86, solution to Problem 1.1.40:** After writing $m = 2k+1$ and $n = 2q+1$, the expansion should use powers of k and q, not powers of m and n. In particular,
$$(2k+1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1,$$
and similarly with q.
26. **Page 90, solution to Problem 1.2.37:** Replace "Theorem 2.6" by "Theorem 1.1.6".
27. **Page 92, solution to Problem 1.3.32:** Replace "if an only if" by "if and only if".
28. **Page 93, alternate solution to Problem 1.3.35:** "substitute for x in the second congruence" should be "substitute for x in the first congruence".

29. **Page 94, solution to Problem 1.3.39:** In the sentence introducing the additive order of [5], replace "the solution of $4x \equiv 0 \pmod{20}$" by "the solution of $5x \equiv 0 \pmod{20}$".

30. **Page 98, solution to Problem 1.4.45(c):** Replace "$x \equiv k \pmod{p}$" by "$x \equiv k! \pmod{p}$".

31. **Page 99, solution to Problem 1.4.46:** The multiplicative argument takes place in the group of units. Replace each relevant occurrence of "$\mathbf{Z}_{35}$" by "$\mathbf{Z}_{35}^{\times}$".

32. **Page 101, review solutions:** In the solution to Problem 3, replace "$\text{lcm}[1275, 495)$" by "$\text{lcm}(1275, 495)$".

    In the solution to Problem 5, dividing the congruence by 8 gives $3x \equiv 21 \pmod{25}$, not the original congruence $24x \equiv 168 \pmod{200}$.

    In the solution to Problem 6, delete the duplicated "the".

33. **Page 104, solution to Problem 2.1.27:** Replace "$[2x_1]_8 = [x_2]_8$" by "$[2x_1]_8 = [2x_2]_8$".

    Also delete the duplicated "but".

34. **Page 105, solution to Problem 2.1.29(c):** Repair the malformed bracket and extraneous parenthesis in the verification.

35. **Page 106, solutions to Problems 2.1.31–2.1.32:** In the solution to Problem 2.1.31, replace $\{f(x_1\}$ by $\{f(x_1)\}$. In parts (a) and (c) of the solution to Problem 2.1.32, replace $f(x)$ by $f(s)$ where the element under discussion is denoted by s.

36. **Page 107, solution to Problem 2.1.34:** The composite KL is the identity transformation on $\mathbf{R}^n$, not on $\mathbf{R}^m$.

37. **Page 112, solution to Problem 2.2.22:** Replace "$f^{-1}(P_\alpha \cap (P_\beta)$" by "$f^{-1}(P_\alpha \cap P_\beta)$".

38. **Page 113, solution to Problem 2.3.23:** Replace "cannot be less than n" by "cannot be less than m".

39. **Page 116, solution to Review Problem 7:** Delete the parenthetical sentence "You could use $P = A$ instead of $P = I$". This is not valid for a singular matrix A.

40. **Page 118, solution to Problem 3.1.29:** The calculation of

    $$(x_1, y_1, z_1) * ((x_2, y_2, z_2) * (x_3, y_3, z_3))$$

    has a missing operation symbol $*$ (on the second line, between the two triples), a missing plus sign (on the third line, in "$z_3x_2y_3$") and a missing closing parenthesis (at the end of the third line).

41. **Page 120, solution to Problem 3.1.36:** The formula "$x^{-1} = (axa)^{-1}$" at the end confuses the original group inverse with the inverse for the new operation. Replace it by: "The inverse of x with respect to $*$ is $(axa)^{-1}$."

42. **Page 120, solution to Problem 3.1.37:** Replace "Note the $e \cdot e$" by "Note that $e \cdot e$".

43. **Page 121, solution to Problem 3.1.39:** In the displayed matrix product, replace its lower-right entry "$c_2b_1 + d_2d_2$" by "$c_2b_1 + d_2d_1$".

44. **Page 123, answer to Problem 3.1.42(b):** The stated set $\mathbf{R}^2$ is not a group under
$$(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1x_2 + y_2),$$
since an element whose first component is 0 has no inverse. Restrict the set to $\{(x, y) \in \mathbf{R}^2 \mid x \neq 0\}$.

45. **Page 124, solution to Problem 3.2.34:** Replace "each nonzero element" by "each nonidentity element".

46. **Page 124, solution to Problem 3.2.35:** In the final paragraph of the solution to Problem 3.2.35, replace the two erroneous occurrences of "H" by "K".

47. **Page 125, solution to Problem 3.2.37:** "If $\sigma, \tau \in \mathrm{Sym}(S)$" should be "If $\sigma, \tau \in H$".

48. **Page 125, solution to Problem 3.2.38:** After proving $\sigma(V) = V$ for $\sigma \in H$, verify closure and inverses directly; "substitute V for x" in the preceding solution is not a valid argument (as the analogy to Problem 3.2.37 is somewhat thin).

49. **Page 131, solution to Problem 3.3.31:** Replace the final "BA^3" by "AB^3".

50. **Page 136, solution to Problem 3.3.42:** Replace the final "$[H : H \cap N]$" by "$[H : H \cap K]$".

51. **Page 136, solution to Problem 3.3.50:** Delete the duplicated "Answer:".

52. **Page 139, solution to Problem 3.4.38:** Replace "$z_1 + z_2 + x_1y + 2$" by "$z_1 + z_2 + x_1y_2$".

53. **Page 140, solution to Problem 3.4.41:** In the homomorphism calculation, the second components of all values of ϕ lie in $\mathbf{Z}_6$, not in $\mathbf{Z}_2$. Replace the relevant subscripts "2" on those second components by "6".

54. **Page 141, solution to Problem 3.4.43:** Replace the false equality "$\langle p^{n-1} \rangle = (p^n - 1)\mathbf{Z}_{p^n}$" by "$\langle p^{n-1} \rangle = p^{n-1}\mathbf{Z}_{p^n}$".

55. **Page 142, solution to Problem 3.4.46:** In the matrix factorization, replace

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}$$

by

$$\begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}.$$

In the alternate solution, replace "$\mathrm{GL}_2(\mathbf{Z}_p) = HK$" by "the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbf{Z}_p)$ is HK and we have".

56. **Page 147, answer to Problem 3.5.40:** Replace "One possibility it to" by "One possibility is to".

57. **Page 149, solution to Problem 3.6.38:** Replace "elments" by "elements".

58. **Page 153, solution to Problem 3.7.31:** Replace "for every divisor of k" by "for every divisor k of m".

59. **Page 153, solution to Problem 3.7.32(b):** "Let $y \in G$" should be "Let $g \in G$".

60. **Page 153, solution to Problem 3.7.33:** Replace

$$\begin{bmatrix} \det(A) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \det(A) & 0 \\ 0 & 1 \end{bmatrix}$$

by

$$\begin{bmatrix} \det(A) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \det(B) & 0 \\ 0 & 1 \end{bmatrix}.$$

61. **Page 154, solution to Problem 3.7.34:** In the alternate solution to Problem 3.7.34, replace "$\psi(G)$" by "$\psi(G_2)$".

62. **Page 154, solution to Problem 3.7.36:** Replace "$gag^{-1} \in G$" by "$gag^{-1} \in N$".

63. **Page 155, solution to Problem 3.7.37:** In the computation of the conjugacy class of a^2, replace "xax^{-1}" by "xa^2x^{-1}".

64. **Page 158, solution to Problem 3.8.43:** Replace "cosets of N" by "cosets of H".

65. **Page 158, solution to Problem 3.8.45:** Replace "$Nb = \{ab, a^3b, a^6b, a^9b\}$" by "$Nb = \{b, a^3b, a^6b, a^9b\}$".

66. **Page 160, solution to Problem 3.8.50:** The question concerns conjugates of a, but the proof switches to x. Use one fixed element throughout; for example,
$$gag^{-1} = hah^{-1} \iff h^{-1}g \in C(a).$$

67. **Page 160, solution to Problem 3.8.52:** Also replace "classses" by "classes".

68. **Page 172, alternate solution to Problem 4.2.31:** Replace "This give" by "This gives".

69. **Page 174, solution to Problem 4.3.28:** In the multiplication calculation, replace
$$(ac - 3bd) + (ad + bc)\sqrt{3}$$
by
$$(ac - 3bd) + (ad + bc)\sqrt{3}\,i.$$

70. **Page 175, solution to Problem 4.3.30:** Delete the final comment. It refers to $\mathbf{Z}_3[x]/\langle x^2 + x - 1\rangle$, whereas the field just constructed is $\mathbf{Z}_5[x]/\langle x^2 + x + 1\rangle$; moreover, the claim about all nonzero powers of $[x]$ is incompatible with the order-3 calculation on the same page.

71. **Page 176, solution to Problem 4.3.34:** Replace "$x^2 + bc + 1$" by "$x^2 + bx + 1$".

72. **Page 178, answer to Problem 4.4.35:** Replace "Problems 34 and 35" by "Problems 33 and 34".

73. **Page 181, solution to Review Problem 7(b):** In the back-substitution, replace
$$(x + 1)(x^3 + x^2 + 2x + 1)$$
by
$$(x + 1)(x^3 + 2x^2 + x + 1).$$

74. **Page 185, solution to Problem 5.1.35:** In part (a), the list of units of $\mathbf{Z}_{24}$ omits 17. The complete list is
$$\{1, 5, 7, 11, 13, 17, 19, 23\}.$$
In part (b), the conditions modulo 3 and modulo 8 must both hold, so replace "or else" by "and furthermore".

75. **Page 186, solution to Problem 5.1.36(a):** In the lower-left entry of the first displayed matrix product, replace "$cd + bd + af$" by "$cd + be + af$".

76. **Page 186, solution to Problem 5.1.36(b):** The displayed inverse of the matrix with diagonal entries -1 should be

$$\begin{bmatrix} -1 & 0 & 0 \\ b & -1 & 0 \\ c & b & -1 \end{bmatrix}^{-1} = \begin{bmatrix} -1 & 0 & 0 \\ -b & -1 & 0 \\ -c-b^2 & -b & -1 \end{bmatrix}.$$

77. **Page 186, solution to Problem 5.1.36(e):** The product in part (e) has the same erroneous term "bd" as the one in part (a); replace it by "be".

78. **Page 187, solution to Problem 5.1.36(e):** This uses the convention that zero divisors must be nonzero. But the book does allow 0 to count as a zero divisor (unless the ring is trivial). Some work is needed to square this conflict of definitions.

79. **Page 188, solution to Problem 5.1.40(a):** Delete the extra closing parenthesis after "$= ab + ac - 2a^2bc$", and replace "S is Boolean ring" by "S is a Boolean ring".

80. **Page 189, solution to Problem 5.1.43:** Delete the extra x in "$b_{n-1}x^{n-1}x + \cdots$".

    More importantly, the final comment is false: it is not enough that each nonzero coefficient separately be a zero divisor. The correct general criterion is that $f \in R[x]$ is a zero divisor if and only if there is one nonzero $c \in R$ that annihilates every coefficient of f.

81. **Page 192, solution to Problem 5.2.30:** Replace "$\phi_1 \neq 0$" by "$\phi(1) \neq 0$".

82. **Page 193, solution to Problem 5.2.34(a):** Replace "Z_8" by "$\mathbf{Z}_8$" (twice).

83. **Page 195, solution to Problem 5.2.38:** Delete the extra closing parenthesis after "$(m_1m_2 - n_1n_2) - (m_1n_2 + m_2n_1)\, i$".

84. **Page 196, solution to Problem 5.2.44(a):** Replace "$a^b b^2$" by "a^2b^2".

85. **Page 197, solution to Problem 5.2.46:** The second paragraph of the solution omits the zero homomorphism. Add the case

$$\phi(1) = 0, \qquad \operatorname{im}\phi = \{0\}, \qquad \ker\phi = \mathbf{Z}_{120}.$$

86. **Page 198, solution to Problem 5.3.34:** Replace the malformed characterization of I by

$$I = \{f \in \mathbf{R}[x] \mid f(0) = f'(0) = 0\}.$$

87. **Page 200, solution to Problem 5.3.42(a):** Replace "since $n \equiv m \pmod 2$" by "since $a \equiv b \pmod 2$". In more detail:

$$\begin{aligned} m \underbrace{a}_{\equiv b \pmod 2} - n \underbrace{b}_{\equiv a \pmod 2} &\equiv mb - \underbrace{na}_{\equiv -na \pmod 2} \\ &\equiv mb - (-na) = na + mb \pmod 2. \end{aligned}$$

88. **Page 201, solution to Problem 5.3.44:** Replace "$a \in K$" by "$a \in I$".

89. **Page 202, solution to Problem 5.3.46(b):** Replace "Suppose that P is a prime ideal of R" by "Suppose that P is a prime ideal of S".

90. **Page 203, solution to Problem 5.3.48:** In parts (d) and (e), replace "The results holds" by "The result holds".

91. **Page 205, solution to Problem 5.4.20:** Replace "$\widehat{\phi_1\beta}\,\widehat{\phi_2\alpha} : Q(D_1) \to Q(D_2)$" by "$\widehat{\phi_1\beta}\,\widehat{\phi_2\alpha} : Q(D_1) \to Q(D_1)$".

    Replace "$\widehat{\phi_2\alpha}\,\widehat{\phi_1\beta} : Q(D_2) \to Q(D_1)$" by "$\widehat{\phi_2\alpha}\,\widehat{\phi_1\beta} : Q(D_2) \to Q(D_2)$".

92. **Page 206, review solutions:** In Problem 1(c), replace "Thus and element" by "Thus an element". In Problem 1(e), replace "nozero" by "nonzero".

93. **Page 208, solution to Review Problem 8(b):** In the comparison of products, replace "$\phi\left((c+di)\right)$" by "$\theta\left((c+di)\right)$".

    Also replace "it is clear the θ" by "it is clear that θ".

94. **Page 210, solution to Problem 6.1.21:** Replace "is a just an isomorphism" by "is just an isomorphism".

95. **Page 211, solution to Problem 6.2.19:** From $[\mathbf{Q}(u) : \mathbf{Q}] \mid 7$, it follows only that the degree is 1 or 7. To prove that it is actually 7 (not 1), argue as follows: For $\alpha = \sqrt[7]{2}$, we have $u = \alpha^4 + 3\alpha^3 \notin \mathbf{Q}$ by linear independence of $1, \alpha, \ldots, \alpha^6$. Hence the degree is indeed 7.

96. **Page 213, solution to Problem 6.3.7:** Replace "Comment We" by "Comment: We".