Section 1.2

Theorem 1.5 The theorem should say, "Every Pythagorean triple (a, b, c) is similar to a Pythagorean triple of the form $(q^2 - p^2, 2qp, q^2 + p^2)$, where p and q are positive integers with $q > p > (\sqrt{2} - 1)q$."

Exercise 1.19(i) The answer should be $q = 4$, $p = 3$.

Exercise 1.21 The definition of **rational line** must be broadened to include the case of a line of the form $x = a$, where a is a rational number. (Otherwise we must assume that the points P and Q have distinct x-coordinates.)

Exercise 1.22 Assume also, as part of the set-up, that the point Q is in the first quadrant. At the end of your proof, you may use the following fact: If c^2 is an integer, then either c is an integer or c is irrational.

Exercise 1.31 This is a challenging problem. First show that there are no positive rational numbers x and y so that $x^4 + 1 = y^2$, using Theorem 1.7. To prove that there are no positive rational numbers x and y so that $x^4 - 1 = y^4$, you will need to prove an analogous result to Theorem 1.7, namely that there is no triple (x, y, z) of positive integers with $x^4 - y^4 = z^2$.

Exercise 1.33 Use the fact that 1 and 2 are not congruent numbers.

Theorem 1.9 Near the end of the proof, the sentence beginning with "When we clear denominators . . . " should say, "When we clear denominators, we get $a^4 + 2^4c^4 = (ab)^2$, . . . "

Theorem 1.11 The phrase "if and only of" should be replaced by "if and only if." Also (as is made clear by the discussion preceding the theorem), the perfect squares in the arithmetic sequence are perfect *rational* squares, namely squares of rational numbers, not necessarily squares of integers.

Section 1.3

How to Think About It, p 34 After the computation, in the second sentence, in which the gcd, 4, is being written as a linear combination of 124 and 1028, the 0 digit is omitted from 1028.

1.3 Extra Exercise 1 Prove that an integer $m > 1$ is prime if and only if it has no factorization $m = ab$, where $|a| < m$ and $|b| < m$.

1.3 Extra Exercise 2 Prove that there are no integers a, b such that $(\frac{a}{b})^2 = 3$.

Exercise 1.41(i) This is a more general version of the Division Algorithm, which is very useful. Make sure you understand how this version of the Division Algorithm works by trying several examples. For example, try $a = 5$, $b = 23$, then $a = 5$, $b = -23$, and $a = -5$, $b = 23$, and finally $a = -5$, $b = -23$. You can try to prove this general version of the Division Algorithm as a challenge problem.

Exercise 1.46 After proving the "two out of three" rule, deduce the following handy fact: for integers a, b, c, if c is a common divisor of a and b (meaning $c|a$ and $c|b$), then c divides every integer linear combination of a and b, i.e. for any integers s and t, $c|(sa + tb)$.

Exercise 1.47 There are eight parts to this problem; just pick two or three to do. The point of this problem is to help you understand the proof of Theorem 1.19.

Exercise 1.49 Study the proof of Theorem 1.19 and make a similar argument. Define a subset C of I to be the set of positive elements in I, and let d be the smallest element in C. Then prove that all other elements of I are multiples of d, and all multiples of d are elements of I. As in the case of Theorem 1.19,

there is also a trivial case, which needs to be treated separately. Note, however, that the set I given in this exercise is not defined *explicitly* but *implicitly*. Instead of being told exactly what is in I (as in the proof of Theorem 1.19), we are given three *properties* of I. We cannot assume anything about what is in I, except what is implied by the three listed properties.

Exercise 1.71 The numbers a, b, and c are real numbers. Modify part (ii) to say,

"In proving Corollary 1.35, we need the fact that

$$ab + a\big((-1)c\big) \;=\; ab - ac.$$

Prove this fact."

Section 1.4

1.4 Extra Exercise 1 Prove the uniqueness of multiplicative inverses in $\mathbb{R}$. In other words, prove: Given any real number $a \neq 0$, if there are real numbers b_1 and b_2 with $ab_1 = 1$ and $ab_2 = 1$, then $b_1 = b_2$. This justifies the use of the notation a^{-1} to refer to *the* multiplicative inverse (reciprocal) of a; without the uniqueness property the notation a^{-1} would be ambiguous.

1.4 Extra Exercise 2 The proof of Corollary 1.35 has a few gaps. The purpose of this exercise is to fill in the gaps. First recall the definition of subtraction: for real numbers a and b, we define $a - b = a + (-b)$, where $-b$ is the unique real number with the property that $-b + b = 0$. (See Addition Axiom (iii) and Proposition 1.33.) Second, recall Corollary 1.34, which says that, given a real number a, its (unique) negative can be obtained from a by multiplying by the (unique) negative of the multiplicative identity, namely: $-a = (-1)a$. Consider $a(b - c)$. Rewrite this using the definition of subtraction. Next use distributivity. You should have $a(b - c) = ab + a(-c)$. Now use Corollary 1.34 to rewrite $-c$, and use the Law of Substitution. Next use multiplication axioms to show $a\big((-1)c\big) = (-1)(ac)$. (This takes three steps.) Finish the proof using Corollary 1.34 again and the definition of subtraction.

Exercise 1.69 Recall that, for real numbers a and b with $b \neq 0$, the notation a/b represents $a \cdot b^{-1}$ where b^{-1} is the unique real number with the property that $b \cdot b^{-1} = 1$. (See Multiplication Axiom (iii) and Proposition 1.33.) In this exercise, we aim to show that a/b is the unique real number whose product with b is a. Two things must be shown: (i) $b \cdot (a \cdot b^{-1}) = a$; and (ii) if c is a real number with the property that $b \cdot c = a$, then $c = a \cdot b^{-1}$. Give a careful proof of each of these, citing an appropriate axiom, proposition, or corollary at each step.

Section 2.1

Proposition 2.7 The proof of (i) is faulty; it shows that $a^{m+n} = a^{m+n}$, which is obviously not what is intended. The first three steps of the proof are fine, but it should finish as follows:
$a^{m-1}a^n a \;=\; a^{m-1}aa^n \;=\; a^m a^n$.

2.1 Extra Exercise Prove that, if N is a common multiple of integers m and m', then $\text{lcm}(m, m')$ divides N.

Exercise 2.3 Hint: Use Exercise 1.56 as well as Exercise 1.58.

Exercise 2.4 Modify to say, "If a is positive and $a \neq 1$, give two proofs that

$$1 + a + a^2 + \ldots + a^n \;=\; \frac{a^{n+1} - 1}{a - 1}$$

by induction on $n \geq 0$ and by multiplying the left-hand expression by $(a-1)$."

Exercise 2.8 The point of this exercise is to show that the two different ways of defining the factorial of a number are in fact equivalent. In your proof you should use the notation $n!$ to refer to the factorial as defined in the text (page 51), then use induction prove that $n!$ is always equal to $1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$, for $n \geq 1$.

Exercise 2.12(i) Modify the problem to say, "Prove that an integer $a \geq 2$ is a perfect square if and only if it can be written in the form: $a = p_1^{e_1} \dots p_n^{e_n}$ with $p_1, \dots, p_n$ distinct primes and $e_1, \dots, e_n$ positive even integers."

Exercise 2.15 "When does equality occur?" This means to find a condition on m and n that implies that $\mathcal{O}_p(m+n) = \min\{\mathcal{O}_p(m) + \mathcal{O}_p(n)\}$.

Section 2.2

Lemma 2.23 The formula for $\binom{n}{r}$ should say that $\binom{n}{r} = 1$ if $r = 0$ or $r = n$ (not, as is stated, if $n = 0$ or $n = r$.)

Example 2.27 In the expansion of $(a+b)^4$, the last term should be $+6(ab)^2$, not $-6(ab)^2$. Hence the last term in the expression for $a^4 + b^4$ should be $-6(ab)^2$.

Section 2.3

Exercise 2.44 Modify the definition of $g(n)$ so that $g(0) = 1$.

Exercise 2.49 You may assume that the limit exists and is nonzero.

Exercise 2.50(i) Modify to say: "Let r be a nonzero real number. Consider the sequence $\{s_n\}$ defined by $s_n = r^n$ for $n \geq 0$, so $\{s_n\}$ is $\{1, r, r^2, r^3, \dots\}$. Suppose that s_n satisfies the recurrence relation $s_n = s_{n-1} + s_{n-2}$ for $n \geq 2$. Show that r must be either $\gamma = \frac{1}{2}(1+\sqrt{5})$ or $\delta = \frac{1}{2}(1-\sqrt{5})$."

Section 3.1

Exercise 3.2 Modify (i) to say, "Show, for all positive integers n, that the value of i^n is one of $1, i, -1, i$."

Exercise 3.3 Modify (i) to say, "Show, for all positive integers n, that the value of ω^n is one of $1, \omega, \omega^2$."

Section 3.2

Proposition 3.14 At the end of the proof, it is stated that $\sin\theta = \frac{a}{|z|}$, but it should say that $\sin\theta = \frac{b}{|z|}$.

Corollary 3.19 The imaginary unit is missing in the definitions of z and w. The corollary should begin, "If $z = |z|(\cos\alpha + i\sin\alpha)$ and $w = |w|(\cos\beta + i\sin\beta)$, then $z \cdot w = \dots$"

Exercise 3.21 The point of this exercise is to take advantage of the fact that we have proven that $\mathbb{C}$ satisfies the nine "fundamental properties" of the real numbers discussed in Section 1.4. In particular, the

proofs of the relevant results in Section 1.4 can be very easily modified to prove the corresponding results for complex numbers. Use this as an opportunity to write proofs that use only the laws of substitution and the nine fundamental properties, making sure to cite what law or property you use at each step.

Exercise 3.23 The imaginary unit is missing from the formula for $z - \bar{z}$. The exercise should say, "If $z \in \mathbb{C}$ show that $z + \bar{z} = 2(\Re z)$ and $z - \bar{z} = 2(\Im z) \cdot i$."

Exercise 3.26 Nonnegative integer powers of complex numbers are defined in a way analogous to the definition for nonnegative integer powers of real numbers; see page 51. A negative integer power of a nonzero real or complex number is defined as the corresponding positive power of the multiplicative inverse: if $-n$ is a negative integer and $a \neq 0$ is a real or complex number, then $a^{-n} = (a^{-1})^n$.

Exercise 3.39 The sentence should begin "Let $n \geq 0$ be an integer ...".

Exercise 3.41 For (ii), you may use the following fact about polynomials: If $r_1, r_2, \ldots, r_n$ are distinct roots of a degree n polynomial $f(x)$, then $f(x) = C(x - r_1)(x - r_2)\ldots(x - r_n)$ for some constant C. (This follows from induction and Proposition 6.15, stated at the beginning of Section 3.1, on page 82.)

Exercise 3.42 The integer n should be positive, not merely nonnegative. Also, in part (i) of the question, there is unnecessary repitition of the definition of ζ.

Section 3.3

Example 3.31 As stated, the 8^{th} roots of unity are shown in Figure 3.7. Notice that there are eight of them. The four *primitive* 8^{th} roots of unity are listed: $\cos(\frac{2\pi}{8}) + i\sin(\frac{2\pi}{8})$, $\cos(\frac{6\pi}{8}) + i\sin(\frac{6\pi}{8})$, $\cos(\frac{10\pi}{8}) + i\sin(\frac{10\pi}{8})$, and $\cos(\frac{14\pi}{8}) + i\sin(\frac{14\pi}{8})$.

Theorem 3.32(i) The term ζ is missing from the left-hand side of the equation. The equation should be $1 + \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{n-1} = 0$. Also, for this to be true, we need $\zeta \neq 1$. The rest of the theorem holds for any nth root of unity ζ, including $\zeta = 1$.

Exercise 3.50 For (i), you may use the following fact: If $r_1, r_2, \ldots, r_n$ are distinct roots of a degree n polynomial $f(x)$, then $f(x) = C(x - r_1)(x - r_2)\ldots(x - r_n)$ for some constant C.

Exercise 3.56 In this exercise you will construct a cubic polynomial with "nice" real coefficients that has three non-obvious real roots. This is similar to Example 3.34, which constructs a quadratic polynomial. Both this exercise and the example use Exercise 3.23 (that the sum of a complex number and its conjugate is real) and Theorem 3.32 (especially that the nth roots of unity sum to zero: make sure you are using the corrected version of this theorem, stated above). Exercise 3.15 will be helpful for the last part of this exercise.

Section 3.4

Exercise 3.72 In this exercise, a and b are real numbers.

Section 4.1

Proposition 4.3 The last sentence of the proof should begin, "Finally, $(a-b)+(b-c)=a-c\ldots$"

Page 137 At the bottom of the page, the last clause of the last sentence describing casting out 9s should read, "for the variation of Proposition 4.11 for 9 says that $r(a)$ is the remainder after dividing a by 9." (The text has $\Sigma(a)$ instead of $r(a)$; while $\Sigma(a)$ is congruent to $r(a)$ mod 9, we do not necessarily have $\Sigma(a)<9$, so $\Sigma(a)$ is not necessarily the remainder after dividing by 9.)

4.1 Extra Exercise 1 (a) Find the smallest positive integer solution of the linear congruence $3x \equiv 4$ mod 5. (b) Characterize all integer solutions of the linear congruence in (a).

4.1 Extra Exercise 2 (a) Find the smallest positive integer solution of the following system of linear congruences:

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 3 \mod 7 \end{aligned}$$

(b) Characterize all integer solutions of the system in (a).

4.1 Extra Exercise 3 (a) Find the smallest positive integer solution of the following system of linear congruences:

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 3 \mod 6 \end{aligned}$$

(b) Characterize all integer solutions of the system in (a).

Exercise 4.4 There are certainly several ways to do this, but one is to use Lemma 4.15.

Exercise 4.14 Justify all of your steps carefully, citing definitions or propositions proven in this section, as appropriate.

Exercise 4.18 Notice that this is the example (adapted from a problem in Qin Jiushao's *Nine Chapters on the Mathematical Art*) discussed on page 146-147. Try solving it using the method used in Example 4.22: write out each congruence as an equation (for example, $x \equiv 32 \mod 83$ becomes $x = 83k + 32$ for some integer k) and go from there.

Exercise 4.19 You may find it helpful to use the extra exercise for Section 2.1.

Exercise 4.22 There is a typo in this exercise: instead of finding s and t, find v and w.

Section 4.2

Page 151 Near the end of the description of how to find a private key, "Proposition 4.17" is cited. The correct citation is Theorem 4.17.

How to Think About It, p 152 There is a typo in the third expression in the computatation of 4^{103} modulo 13. It should read $4^{103} = 4^{12\cdot 8+7} = \left(4^{12}\right)^8 4^7$. The text has 10 instead of 8.

Section 4.3

Page 154 The second sentence of the last paragraph, which reminds us how addition and multiplication are compatible with congruence, should conclude by saying, "if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then $a + b \equiv a' + b' \bmod m$ and $ab \equiv a'b' \bmod m$."

Theorem 4.43 In the second part of the proof (beginning with "Conversely ...") there is an unfortunate line break. We are taking $m = ab$ where $0 < a, b < m$, i.e. $0 < a < m$ and $0 < b < m$, not merely $0 < a$ and $b < m$.

Proposition 4.46 Condition (ii) is stated incorrectly. It should say, "if $a, b \in S$, then $a - b \in S$." The proof is also missing some important steps. Please see the supplemental notes for a complete proof.

Extra 4.3 Exercise Let R be a ring. Let $0 \leq n, m \in \mathbb{Z}$ and $a \in R$. (a) Show that $(n + m)a = na + ma$. Why is this not distributivity? (b) Show that $n(ma) = (nm)a$. Why is this not associativity? (Hint: Remember that this is "hybrid" notation; see the definitions and discussion at the top of page 160.)

Exercise 4.45 Hint: as in the proof of Propositions 4.41 and 4.42, use the norm; see p 116-117 and p 121.

Exercise 4.54 Note that M_2 is a subset of the (non-commutative!) ring of 2-by-2 matrices with entries in $\mathbb{R}$. (See the "How to Think About It" box on page 156.) Therefore several properties are inherited from that ring. (Which ones?) In particular, note that commutativity of multiplication must be proven explicitly because it does not hold in the ring of 2-by-2 matrices with entries in $\mathbb{R}$.

Exercise 4.57 In this problem, we have a field F and a subring k of F. We aim to show that k is a subfield of F if and only if the following condition $(*)$ holds: for all nonzero $a \in k$, $a^{-1} \in k$. Note that "a^{-1}" must refer to the multiplicative inverse of a in F (because we do not know whether or not a has a multiplicative inverse in k.) So "a^{-1}" refers to an element of F with the property that $aa^{-1} = 1_F$, where multiplication is multiplication in F and 1_F is the multiplicative identity in F. Proposition 4.35 ensures that there is only one element of F that is a multiplicative inverse for a. So the condition $(*)$ is that: for every element a of the subring k, the multiplicative inverse of a (when considering a as an element of F) is contained in the subring k.

Exercise 4.58 Modify (i) to say, "Show that $\{0, 3\} \subset \mathbb{Z}_6$ has the same addition and multiplication tables as $\mathbb{Z}_2$." Modify (ii) to say, "Is $\mathbb{Z}_2$ a subring of $\mathbb{Z}_6$?"

Section 5.1

Exercise 5.2 Hint: Use a result proven in this section.

Exercise 5.3 You are asked to prove that $\mathbb{Z}_m$ is a domain if and only if $\mathbb{Z}_m$ is a field. You may assume $m \geq 2$ (although the result is also true for $m = 1$.) One direction follows immediately from a result in this section. For the other direction, use Theorem 4.43 to prove the contrapositive.

Section 5.2

Page 196, bottom There is a space missing after the comma in the first sentence after the "How to Think About It" box.

Corollary 5.9(i) This should say, "If R is a commutative ring, then $R[x]$ and R' are subrings of $R[[x]]$." (It is R' (not R) that is a subring of $R[x]$.)

Exercise 5.9 The elements r and s should be in the ring R not $\mathbb{R}$.

Exercise 5.28 The formatting is misleading. Only part (i) of this exercise is a true/false question.

Section 5.3

Definition of evaluation homomorphism, top of page 215 We should have $e_a(f) = f^{\#}(a)$ not $e_a(f) = f(a)$.

Exercise 5.45 Although we have not formally defined the root of a polynomial, it is what you think it should be, namely, if f is a polynomial in $R[x]$, then an element $a \in R$ is a root of f if $f^{\#}(a) = 0$.

Section 6.1

Lemma 6.1 In the hypothesis, we should specify that $g \neq 0$, in order for the degree of g to be defined. (This implies $f \neq 0$, but $f \neq 0$ does not imply $g \neq 0$.)

Proposition 6.13 To be explicit, in this proposition m and n are positive integers.

Page 243 The last sentence on this page mentions that gcds are unique in $k[x]$, incorrectly citing Corollary 6.29. The correct citation is Theorem 6.30(ii).

Theorem 6.25 The ideal I consists of multiples of $d(x)$ in $k[x]$, not simply constant multiples of $d(x)$, with constants in k, so the correct description is: $I = (d) = \{rd : r \in k[x]\}$. It would be even clearer if it was written as $I = \big(d(x)\big) = \{r(x)d(x) : r(x) \in k[x]\}$.

Theorem 6.28, Corollary 6.29, and Theorem 6.30 The statement of Theorem 6.28 is true, but the proof given shows only that *there is* a gcd of f and g that is a linear combination of f and g; it does not show that *any* gcd of f and g is a linear combination of f and g. The statements of Corollary 6.29 and Theorem 6.30 are also true, but their proofs rely critically on the fact that *any* gcd of f and g is a linear combination of f and g, which is not actually proven in the text. Please see the supplemental notes for proofs of these three results.

6.1 Extra Exercise 1 Consider the map $\varphi : \mathbb{Q}[x] \to \mathbb{C}$ given by $f \mapsto f^{\#}(\omega)$, where $\omega = \frac{1}{2}(-1 + \sqrt{3}\,i)$, as usual. (i) Prove that φ is a homomorphism. (ii) Prove that $\ker(\varphi) = (x^2 + x + 1)$.

6.1 Extra Exercise 2 Consider the map $\varphi : \mathbb{Q}[x] \to \mathbb{C}$ given by $f \mapsto f^{\#}(\zeta)$, where $\zeta = \frac{1}{2}(1 + \sqrt{3}\,i)$. (i) Prove that φ is a homomorphism. (ii) Prove that $\ker(\varphi) = (x^2 - x + 1)$.

6.1 Extra Exercise 3 Let R be a domain, and let p be a nonzero element of R that is also not a unit. Suppose p has the property that if $p|ab$ for some $a, b \in R$, then $p|a$ or $p|b$. (In this case, we say that p is a "prime element" of R.) Show that p is irreducible in R.

Exercise 6.1 Hint: Look back at Exercise 5.14, page 202.

Exercise 6.6 Modify to say, "Let k be a domain and let $f(x) \in k[x]$. If $a(x)$ is an associate of $f(x)$, prove that either $f = a = 0$ or $\deg(f) = \deg(a)$. Give an example to show that the statement may be false if k is not a domain."

Exercise 6.10 *For number theory students who have omitted Sections 4.2-7.3:* You may prove this result in the context of $\mathbb{Z}[i]$, rather than an abstract commutative ring.

Exercise 6.13 Use the Euclidean Algorithm I and II, pages 249-251.

Exercise 6.17 Part (i) relies on the definition of relatively prime and the surrounding discussion, which occur on page 248, after the statement of the exercise. Hint: Look back at Exercise 1.58.

Exercise 6.23 Just do the first part of this problem, the part about gcds, generalizing Exercise 5.50(ii).

Exercise 6.26 Modify to say, "Let f and g be relatively prime polynomials in $k[x]$, where k is a field. If $h \in k[x]$ is an irreducible polynomial, and $h^2|fg$, prove that $h^2|f$ or $h^2|g$."

Exercise 6.30 Hint: Aiming for a contradiction, suppose $f(x)$ factors. Then one of its factors is linear, giving a root in $\mathbb{Q}$. Let $\frac{p}{q}$ be the root, where p, q are relatively prime integers. Then $f(\frac{p}{q}) = 0$, i.e. $(\frac{p}{q})^3 + 5(\frac{p}{q})^2 - 10(\frac{p}{q}) + 15 = 0$. Muliply both sides of this equation by q^3 to get an equation in integers. ...

Example 6.44 The triangle symbol used to indicate the end of the example appears prematurely.

Section 6.2

Proposition 6.55 Though called a proposition when stated, it is called a theorem when referenced. See, for example, the three references to "Theorem 6.55" in the paragraphs following the proof.

Figure 6.1 The cyclotomic polynomials Φ_5, Φ_7, and Φ_{11} are all missing their linear terms, as is clear from looking at Proposition 6.62.

Page 264 At the beginning of the subsection, "Roots of Unity," a definition is given for a primitive nth root of unity; this is not the same as the definition given in Chapter 3 (page 111), but it is equivalent to it.

Lemma 6.59 The proof of the lemma is incomplete; there is no discussion of how to prove uniqueness of the divisor d. Exercise 6.52 completes the proof.

6.2 Extra Exercise 1. Show that the following polynomials are irreducible in $\mathbb{Q}[x]$: (a) $x^3 + 5x^2 + 21$ (Hint: Use Proposition 6.51 and Theorem 6.55.) (b) $x^4 + 7x^3 + 11x^2 - 3x - 105$ (Hint: Use Theorem 6.55 and Example 6.56.) (c) $x^3 + 7x^2 + 5x + 28$ (Hint: Use Theorem 6.55 and Example 6.57.)

6.2 Extra Exercise 2. Fill in the details of Example 6.61 for $n = 1, 2, 3, 4, 6, 12$, as follows. For $n = 1$, we define $\Phi_1(x) = x - 1$. (No computation necessary.) For $n > 1$, we define $\Phi_n(x)$ in terms of $\Phi_d(x)$, where d ranges over proper divisors of n. In particular, for $n = 2$, the only proper divisor is $d = 1$, so $\Phi_2(x) = (x^2 - 1)/\Phi_1(x) = (x^2 - 1)/(x - 1)$. Similarly for $n = 3$, $\Phi_3(x) = (x^3 - 1)/(x - 1)$. For $n = 4$, we now have two proper divisors, $d = 1, 2$, so we need to divide $x^4 - 1$ by $\Phi_1(x)$ and $\Phi_2(x)$) to get $\Phi_4(x)$. For $n = 6$, the proper divisors are $1, 2, 3$, so we divide $x^6 - 1$ by $\Phi_1(x)$, $\Phi_2(x)$, and $\Phi_3(x)$ to get $\Phi_6(x)$, and for $n = 12$, we divide $x^{12} - 1$ by $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_4(x)$, and $\Phi_6(x)$. Compute each of these $\Phi_n(x)$, $n = 2, 3, 4, 6, 12$, cancelling common factors if possible, and using long division of polynomials, as needed.

Exercise 6.42(i) Hint: Reduce modulo 3 and check for linear and irreducible quadratic factors.

Exercise 6.50 The definition of a squarefree integer is given on page 34.

Exercise 6.52 For this exercise, use the definition of primitive dth root of unity given in this section (page 264), rather than the definition from Chapter 3 (page 111).

Section 7.1

Exercise 7.12 Imitate the proof of Theorem 7.11, making sure to look up all references and references of references. Consider the map $\varphi : \mathbb{Q}[x] \to \mathbb{C}$ given by $\varphi(f) = f(\omega)$. Show (1) φ is a homomorphism, (2) $\ker\varphi$ is the ideal generated by the polynomial $x^2 + x + 1$. (Two inclusions to show here!), and (3) $\text{im}\varphi = \mathbb{Q}[\omega]$. The use the First Isomorphism Theorem.

Section 7.2

Example 7.28 At the end of the second paragraph, the cyclotomic polynomial Φ_7 is missing its linear term. It should be $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

7.2 Extra Exercise 0 Let $K = \mathbb{F}_2[x]/(x^2 + x + 1)$, and let $z = x + (x^2 + x + 1)$ in K. (a) Show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. (b) According to Proposition 7.20(v), K is a 2-dimensional vector space over $\mathbb{F}_2$ with basis $\{1, z\}$, i.e. $K = \{a_0 + a_1 z : a_i \in \mathbb{F}_2, 0 \leq i \leq 1\}$. List the elements in K (there are four) and write out addition and multiplication tables for K. (c) What is the characteristic of K? (This will be clear from looking at the addition table.) (d) Find two distinct roots of $x^2 + x + 1$ in K.

7.2 Extra Exercise 1 Let $\zeta = \cos(2\pi/5) + i\sin(2\pi/5)$. (i) Show that ζ is algebraic over $\mathbb{Q}$. (ii) What is the minimal polynomial for ζ over $\mathbb{Q}$? (iii) What is the degree of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$? (iv) Describe $\mathbb{Q}(\zeta)$ explicitly as a subfield of $\mathbb{C}$. ("All complex numbers of the form ...".) (v) Let $\alpha = \zeta + \zeta^4$. Show that $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{Q}(\zeta)$, and find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]$. **Hint**: Let $\beta = \zeta^2 + \zeta^3$. Calculate $\alpha + \beta$ and $\alpha\beta$ to find the minimal polynomial for α over $\mathbb{Q}$.

Exercise 7.30 Hint: Look back at Exercise 3.15 and Exercise 7.22.

Exercise 7.33 You may use the result of 1.3 Extra Exercise 2.

Exercise 7.36 The end of the hint should say, "... the polynomial p may factor in $F[x]$."

Theorem 7.38 There are three issues with this proof. (1) To show that $g'(x) = -1$ in $K[x]$, we need to show that in K, $1 + \cdots + 1$ (q times) is zero. This is not stated explicitly in Proposition 7.17, but is a consequence of Proposition 7.17(i). (2) To prove that E is a subring of K, it is necessary to show that $1 \in E$, that E is closed under *subtraction*, and that E is closed under multiplication. (See correction of Proposition 4.46, above.) (3) To prove that E is a subfield of K, it is necessary to show that for every nonzero $a \in E$, the multiplicative inverse of a in K, namely a^{-1}, also lies in E. This is straightforward and does not rely on Lemma 7.37 (nor is is appropriate to invoke Lemma 7.37, since Lemma 3.37 presumes that we are working in a field with q elements!) See the online notes for an outline of a correct proof.

Example 7.41 The third sentence should begin, "By Proposition 7.20, K consists of ...".

Exercise 7.39 Modify to say, "Let $f(x)$, $g(x) \in k[x]$ be *nonconstant* monic polynomials, where k is a field. Show that, if g is irreducible and every root of f (in an appropriate splitting field) is also a root of g, then $f = g^m$ for some integer $m \geq 1$. Hint: Use *strong* induction on $\deg(f)$." (Not $\deg(h)$.) Additional Hint: For strong induction, first prove base case: i.e. that the claim is true if $\deg(f) = 1$. For the inductive step, suppose that the claim is true for every polynomial p of degree strictly less than the degree of f, and show that the claim is true for f. (To be explicit, the inductive hypothesis is: Given a nonconstant monic polynomial $p(x) \in k[x]$ with $\deg(p) < \deg(f)$ and such that every root of p is a root of g, there is an integer $m \geq 1$ such that $p = g^m$.)

Section 8.1

Exercise 8.1 Hint: Disprove the statement by providing a counterexample. Salvage the statement by proving one of the implications (either the "if" or the "only if" direction.)

Section 8.2

Lemma 8.10 In this lemma $p = 2$ or 3; it is not an arbitrary prime. So the result is true for $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, but not for arbitrary rings of cyclotomic integers.

Example 8.12 The second step of the Euclidean algorithm should be:

$$z = (3 - i)(-10 + 15i) + (-4 - 7i)$$

The text has $(3 + 3i)$ instead of z, but this is a mistake.

Exercise 8.8 This exercise references Example 8.12, which has an error, as discussed above.

Section 8.3

Proposition 8.38 There is an unmatched parentheses in the third sentence.

Proposition 8.42 The first sentence of the second paragraph of the proof should say, "It remains to settle the case where $\lambda \not| yz \ldots$".

Section 8.4

Example 8.52 The very last equation in this example should read $2r - 4t + 10s = 1$.

Exercise 8.47 Perhaps it could be modified as follows, "Referring to Example 8.52, (i) the ideal generated by the norms of *generators of* J_1 is an ideal in $\mathbb{Z}$, and hence principal. Find a generator for it. (ii) Do the same for the other ideals J_2, J_3, and J_4."

Exercise 8.48 There is a sign error. The equality should read: "$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$".

Section 9.2

9.2 Extra Exercise 1 Show that $x^3 - 15x - 126$ (from Example 3.4, page 85) is solvable by radicals by exhibiting an appropriate tower of pure extensions.

9.2 Extra Exercise 2 Show that $x^4 - 10x^2 + 1$ (from Example 3.7, page 87) is solvable by radicals by exhibiting an appropriate tower of pure extensions.

Section 9.3

9.3 Extra Exercise 1 Consider the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Determine all the automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ that fix $\mathbb{Q}$. **Hint:** Recall that $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$. Prove that an automorphism σ of $\mathbb{Q}(\sqrt[3]{2})$ is uniquely determined by $\sigma(\sqrt[3]{2})$.

9.3 Extra Exercise 2 Suppose $k = \mathbb{Q}$, $f(x) = x^3 - 2$. What is the splitting field E of $f(x)$? (It is $\mathbb{Q}(\omega, \sqrt[3]{2})$, why?) Find all possible automorphisms $\sigma : E \to E$ that fix $\mathbb{Q}$. (There are six of them. Describe them by specifying how they act on ω and $\sqrt[3]{2}$.)

Section 9.4

9.4 Extra Exercise 1 Let R be a commutative ring, and let U be the set of units in R. Show that U is an abelian group with multiplication as binary operation.

Exercise 9.12(iii) The binary operation should be multiplication, not addition.

Exercise 9.13 In this exercise $\mathbb{R}^>$ denotes the set of positive real numbers, which is a group with multiplication as its binary operation.