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.

Extra 6.2 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.)

Extra 6.2 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 $\Phi_n(x)$, $n = 2, 3, 4, 6, 12$, using long division of polynomials.

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

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) $\mathrm{im}\varphi = \mathbb{Q}[\omega]$. 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 $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

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

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 on the Unit 2 Corrections and Modifications.) (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 $\lambda \nmid yz \ldots$".

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: "$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$".