Section 7.2

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 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.) We show that E is closed under subtraction as follows. Take $a, b \in E$; then $0 = g(a) = a^q - a$, so $a^q = a$, and similarly $b^q = b$. By Proposition 7.17(ii), $(a-b)^q = (a + (-b))^q = a^q + (-b)^q$. If q is odd, then clearly $(-b)^q = -b^q$, so $(a-b)^q = a^q - b^q$, which implies $g(a-b) = 0$, i.e. $a - b \in E$. If q is even, $(-b)^q = b^q$, but since q is a power of a prime, we must have $q = 2^n$ and $k = \mathbb{F}_2$. Thus $-1 = 1$, and $(-b)^q = b^q = -b^q$, implying, as argued above, that $g(a-b) = 0$ and $a - b \in E$. 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!) Let $a \neq 0$ be in E. Then, $0 = g(a) = a^q - a$, so $a^q = a$, and, since E is a subring of K, it is a domain, and we may cancel to obtain $a^{q-1} = 1$. Since $q \geq 2$, we have $a \cdot a^{q-2} = 1$ in K, i.e. $a^{-1} = a^{q-2}$ in K. Since E is closed under multiplication and $a \in E$, we have $a^{q-2} \in E$, and thus $a^{-1} \in E$.

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 $p(x) \in k[x]$ 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: "$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$".