Appendix A

Hints

Below are some hints, which should be interpreted as possible (but not the only!) ways to get started.

Hint (Theorem 2.4)**.** You are solving $x^2 + bx + c = 0$. Try "completing the square" first; then solve for x.

Hint (Problem 3.9)**.** Multiplying a fraction by the complex conjugate of the denominator can be an effective way to simplify an expression.

Hint (Theorem 3.11)**.** Think back to changing from polar to rectangular coordinates (or parametrizing circles or solving triangles).

Hint (Theorem 3.12)**.** Try using Theorem 3.11 + trigonometric identities.

Hint (Problem 3.20)**.** You want to find a z such that $z^4 = \zeta_3$. You are working with powers (hence multiplication), so try writing z in the form $z = r\cos\theta + ir\sin\theta$. Now you can use Corollary 3.14 to simplify z^4 and compare with ζ_3. What can you deduce about r and θ?

Hint (Lemma 3.22)**.** Similar to Problem 3.20, try writing z in the form $z = r\cos\theta + ir\sin\theta$. Now, what does $z^n = 1$ imply about r and θ?

Hint (Lemma 3.23)**.** It may be helpful to draw some pictures first. Try plotting ζ_8, $(\zeta_8)^2$, $(\zeta_8)^3$, ..., $(\zeta_8)^8$, $(\zeta_8)^{14}$, $(\zeta_8)^{85}$. Now, you know by a previous problem that $(\zeta_n)^n = 1$, so also $(\zeta_n)^{2n} = 1$ and so on. Try (using the division algorithm) to write $k = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r \le n-1$ and plug that into $(\zeta_n)^k$.

Hint (Theorem 3.24)**.** You may want to view this as the following "if and only if" statement: z is an n^{th} root of $1 \iff z = (\zeta_n)^k$ for some $0 \le k \le n-1$. Now make use of the previous lemma and theorems you proved. Don't forget to explain why each of $1, \zeta_n, (\zeta_n)^2, \ldots, (\zeta_n)^{n-1}$ are all different.

Hint (Theorem 3.28)**.** Suppose that z is a root of $p(x)$. Then $p(z) = 0$, so $a_n z^n + a_{n-1} z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0 = 0$. This last equation is is just comparing two complex numbers—try taking the conjugate of both sides. Fact 3.5 is helpful.

Hint (Problem 3.40). You are trying to find $(a+b\sqrt{5})^{-1} = \frac{1}{a+b\sqrt{5}}$. Try multiplying top and bottom by the conjugate: $a-b\sqrt{5}$.

Hint (Theorem 3.50). For the first part, notice that $x \cdot 0 = x(0+0)$. For the last part, remember that the definition of a field ensures that F has at least two elements, so there is some $a \in F$ with $a \neq 0$. Now, what happens if $0 = 1$?

Hint (Theorem 3.53). The crux is to show that every nonzero element has a multiplicative inverse when n is prime. Let $a \in (\mathbb{Z}_n)^*$. You need to find some integer b such that $ab = 1$ modulo n. Now, since $a \in (\mathbb{Z}_n)^*$ and n is prime, $\gcd(a,n) = 1$. By Bézout's Lemma, there exist $k,l \in \mathbb{Z}$ such that $1 = ka + ln$. What happens when you consider the equation $1 = ka + lp$ modulo n?

Hint (Problem 3.57). If T_3 is a subfield, then, in particular, it is closed under multiplication, so it must be that $\alpha^2 \in T_3$. That means that $\alpha^2 = a + b\alpha$ for some $a, b \in \mathbb{Q}$. What does this imply?

Hint (Problem 3.64). Try following the approach in Example 3.60. First show $\{a+bi \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{Q}(i)$ by showing that every subfield that contains $\mathbb{Q}$ and i must also contain $\{a+bi \mid a,b \in \mathbb{Q}\}$. To show the reverse containment, use the fact that $\{a+bi \mid a,b \in \mathbb{Q}\}$ is a subfield, by a previous problem.

Hint (Problem 3.67). Remember, in Problem 3.57(3), we saw that $\{a+b\alpha \mid a,b \in \mathbb{Q}\}$ is *not* a subfield of $\mathbb{C}$.

Hint (Problem 3.69). Use the previous theorem. To show $\mathbb{Q}\left(3-\sqrt{2}, 5+i\right) \subseteq \mathbb{Q}\left(\sqrt{2}, i\right)$, you need to show that $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}, i\right)$ and that $3-\sqrt{2}, 5+i \in \mathbb{Q}\left(\sqrt{2}, i\right)$. Then show the reverse containment in a similar way.

Hint (Theorem 4.12). Note that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$. Now use Theorem 3.24; note that $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$ should only have $n-1$ roots.

Hint (Problem 4.14). First find the roots of $z^2 - 3z - 1$. Then, for each of those roots, use Theorem 3.26 to solve for z. You should have 6 different roots in the end.

Hint (Theorem 5.20). Try a proof by contradiction. Assume that u is a unit and that u is a zero divisor. Now, what does the definition of being a zero divisor tell you about u?

Hint (Theorem 5.33). To get started, let $n = \deg p(x)$ and $m = \deg q(x)$, and then write $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ and $q(x) = b_0 + b_1 x + \cdots + b_m x^m$ with $b_m \neq 0$. You want to understand the degree of $p(x) + q(x)$, so you need to determine the largest power of x in the sum $p(x) + q(x)$.

Hint (Theorem 5.35). As with the previous theorem, let $n = \deg p(x)$ and $m = \deg q(x)$, and then write $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ and $q(x) = b_0 + b_1 x + \cdots + b_m x^m$ with $b_m \neq 0$. You need to determine the largest power of x in the product $p(x)q(x)$. What do you think is the largest power of x in the product $p(x)q(x)$? What is its coefficient, and how do you know it's not zero?

Hint (Corollary 5.37)**.** There are several things to verify to ensure that $D[x]$ is an integral domain, but we've talked about most of them already. The main thing that remains is to prove that $D[x]$ has no zero divisors—try a proof by contradiction. This is a corollary of Theorem 5.35, which means that it should be "not too hard" to prove using Theorem 5.35.

Hint (Theorem 5.43)**.** One approach is to polish up and fill in the gaps of the outline presented in the notes right before the statement of Theorem 5.43. A related, but slightly different, approach is to try using induction on the degree of $a(x)$.

Hint (Theorem 5.44)**.** Try using the division algorithm to write $a(x) = (x-c)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg r(x) < \deg(x-c)$ or $r(x) = 0$. Now show that $r(x)$ must be the zero polynomial.

Hint (Lemma 5.51)**.** First, explain why $d_1(x)$ must divide $d_2(x)$ and why $d_2(x)$ must divide $d_1(x)$. Now return to the definition of "to divide" and see what you can write down.

Hint (Theorem 5.53)**.** Follow the definitions. Since $c(x) \in I$, it can be written a particular way. Then write down what it means for $h(x)$ to divide both $a(x)$ and $b(x)$. Combine.

Hint (Theorem 5.60)**.** For the forward direction, start with the definition of a unit and apply the degree function. For the reverse direction, what does $\deg p(x) = 0$ imply about $p(x)$? Can you explicitly write down the a multiplicative inverse for $p(x)$?

Hint (Theorem 5.64)**.** Consider using Theorem 5.40.

Hint (Theorem 5.67)**.** Consider using using strong induction on the degree of the polynomial. Let $\varphi(n)$ be the statement "every polynomial in $F[x]$ of degree n can be written as a product of polynomials that are irreducible in $F[x]$."

For the base case, you want to show that $\varphi(1)$ is true. Assume that $p(x) \in F[x]$ has degree 1. Then what?

Next, assume that $\varphi(k)$ is true for all $1 \leq k \leq n$. We need to show that $\varphi(n+1)$ is true. Assume that $p(x) \in F[x]$ has degree $n+1$. There are two cases to consider: $p(x)$ is irreducible or $p(x)$ is reducible. Keep going...

Hint (Problem 5.79)**.** Use the division algorithm to write $a(x) = (x^2+1)q(x) + r(x)$. What does this tell you?

Hint (Theorem 5.86)**.** Using Fact 5.76, you know that R/I is ring. So, for the first part, assume R is commutative, and use this to show R/I is commutative. The starting point is to choose two arbitrary elements of R/I, which would be something like $a+I$ and $b+I$ for $a, b \in R$. Now show that $(a+I)(b+I) = (b+I)(a+I)$ using the definition of multiplication in Fact 5.76.

Hint (Problem 5.80)**.** For the second part, remember that $a \equiv_6 b \iff a - b$ is a multiple of 6. For the last, use the division algorithm to write $a = 6q + r$. What does this imply?

Hint (Theorem 5.83)**.** By definition of an ideal, $I \subseteq R$, so what we really need to show is that $R \subseteq I$. Remember that I is closed under multiplication by elements of R. So, if $a \in I$, then $ra \in R$. Try to first show that $1 \in R$.

Hint (Theorem 5.85)**.** Theorem 5.83 should help with the forward direction. For the backward direction, let $a \in R^*$; you need to show a has an inverse. Try using Theorem 5.82: the set $I = \{ar \mid r \in R\}$ is an ideal. By assumption, $I = \{0\}$ or $I = R$. Which is it? Notice that if $I = R$, then $1 \in I$.

Hint (Problem 5.96)**.** Use Theorem 5.94. Theorem 5.83 may also be helpful.

Hint (Theorem 5.99)**.** Try using Theorem 5.91.

Hint (Theorem 5.119)**.** Assume $\phi : R \to S$ is a ring homomorphism. We need to define a suitable homomorphism from $R/\ker\phi$ to $\phi(R)$, and then check that it is bijective. Let's let $K := \ker\phi$. Try defining $\hat{\phi} : R/K \to \phi(R)$ via $\hat{\phi}(a+K) = \phi(a)$. A very important point, is that we don't actually know that $\hat{\phi}$ is a well-defined function. We know that a coset $a+K$ might be equal to $a'+K$, so we'd better make sure that if $a+K = a'+K$ then $\hat{\phi}(a+K) = \hat{\phi}(a'+K)$. Do that first. Then, verify that $\hat{\phi}$ is a homomorphism that is also surjective and injective. For injectivity, it may be useful to use Theorem 5.117 and instead show that $\ker\hat{\phi} = \{0+K\}$.

Hint (Theorem 5.121)**.** We want to show that $\phi(I)$ is an ideal of S. Elements of $\phi(I)$ look like $\phi(a)$ for some $a \in I$. To show that $\phi(I)$ is a subring of S, let $\phi(a_1), \phi(a_2) \in \phi(I)$ for some $a_1, a_2 \in I$. Now explain why $\phi(a_1) + \phi(a_2)$, $\phi(a_1)\phi(a_2)$, and $-\phi(a_1)$ are all in $\phi(I)$. You also should say why $\phi(I)$ is nonempty. Finally, you also need to show that for all $s \in S$, $s\phi(a_1)$ is in $\phi(I)$. Remember that ϕ maps *onto* S, so $s = \phi(r)$ for some $r \in R$. Now keep going.

Hint (Theorem 5.122)**.** We want to show that $\phi^{-1}(J)$ is an ideal of R. Let $a_1, a_2 \in \phi^{-1}(J)$. This means that $\phi(a_1), \phi(a_2) \in J$. To show that $a_1 + a_2$, $a_1 a_2$, and $-a_1$ are in $\phi^{-1}(J)$, you just need to show that $\phi(a_1) + \phi(a_2)$, $\phi(a_1)\phi(a_2)$, and $-\phi(a_1)$ are all in J (using that $a_1, a_2 \in \phi^{-1}(J)$ and J is an ideal). You also need to show that $ra_1 \in \phi^{-1}(J)$, and to do that, you need to show that $\phi(ra_1) \in J$.

Hint (Problem 6.4)**.** Notice that $\alpha^2 = 2 + 2\sqrt{2}i - 1$, so $\alpha^2 - 1 = 2\sqrt{2}i$. What happens if you square both sides?

Hint (Lemma 6.5)**.** Towards a contradiction, assume that $m(x)$ is reducible. By Theorem 5.61, $m(x) = a(x)b(x)$ for some $a(x), b(x) \in F[x]$ with $\deg a(x)$ and $\deg b(x)$ both smaller than $\deg m(x)$. Now, $m(x) \in I$, so $0 = m(\alpha) = a(\alpha)b(\alpha)$. Explain why this implies that $a(x)$ or $b(x)$ is in I. But $I = (m(x))$, so by Theorem 5.91, $m(x)$ divides $a(x)$ or $b(x)$. What's the contradiction?

Hint (Problem 6.9)**.** Theorem 4.12 might provide some inspiration.

Hint (Problem 6.22)**.** To see why the degree of $m(x)$ can not be 3, suppose it is. Then $x^4 - 2x^2 + 9 = m(x)q(x)$ for some $q(x) \in \mathbb{Q}[x]$ with $\deg q(x) = 1$. Explain why $q(x)$ has a root that lies in $\mathbb{Q}$. But the root of $q(x)$ is a root of $x^4 - 2x^2 + 9$, so find the roots of $x^4 - 2x^2 + 9$ (and thus a contradiction).

Hint (Theorem 6.58)**.** Consider using Theorem 5.111 and remember that $c = c \cdot 1$.

Hint (Theorem 7.8)**.** Let $p(x) = x^n - r^n$. Why is $p(x) \in F[x]$? Can you show that $F(r) = F^{p(x)}$?

Hint (Theorem 7.19)**.** First use Theorem 6.61 to show that γ maps R to itself, then make use of the fact that γ is an injective function.

Next, use results from Chapter 5 (including the First Isomorphism Theorem for rings) to show that γ is an isomorphism from $\mathbb{Q}^{p(x)}$ to $\gamma(\mathbb{Q}^{p(x)})$ and that γ fixes $\mathbb{Q}$. Then, to show that $\gamma \in \mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$, it only remains to show that $\mathbb{Q}^{p(x)} = \gamma(\mathbb{Q}^{p(x)})$. Let $r_1, \ldots, r_n$ be the roots of $p(x)$ so that $\mathbb{Q}^{p(x)} = \mathbb{Q}(r_1, \ldots, r_n)$. Using the definition of $\mathbb{Q}(r_1, \ldots, r_n)$, it is not to hard to see that $\gamma(\mathbb{Q}(r_1, \ldots, r_n)) = \gamma(\mathbb{Q})(\gamma(r_1), \ldots, \gamma(r_n))$. Now explain why $\gamma(\mathbb{Q})(\gamma(r_1), \ldots, \gamma(r_n)) = \mathbb{Q}(r_1, \ldots, r_n)$.

Hint (Theorem 7.23)**.** Let γ be complex conjugation. By Theorem 7.19, $\gamma \in \mathrm{Aut}(\mathbb{Q}^{p(x)}/\mathbb{Q})$. What does γ do to the real roots of $p(x)$? What about to those that are not real?

Hint (Lemma 8.6)**.** You want to show that $x^{-1}y^{-1}xy \in N$, which is the same as $(x^{-1}y^{-1}xy)N = N$ in the quotient group H/N. Work in H/N, and compute $(x^{-1}N)(y^{-1}N)(xN)(yN)$. Don't forget that H/N is abelian.

Hint (Theorem 8.13)**.** Let σ be an element of order 5 and τ a transposition. First explain why σ must be a 5-cycle. Then notice that we can write $\sigma = (a, b, c, d, e)$ and $\tau = (a, x)$ where $x \in \{b, c, d, e\}$. Try to use Fact 8.12. If $x = b$, you can directly apply Fact 8.12; if not, consider σ^2, σ^3,...