Chapter 16.

4 Answer: \(x^2 + (1/2)x - (1/4)\), found by using the identities \(\sin^2 x + \cos^2 x = 1\) and \(\cos(a + b) = \cos(a) \cos(b) - \sin(a) \sin(b)\) multiple times. (In fact, we get something that is not irreducible over \(\mathbb{Q}\) in this way, so then we factor to find the answer.)

5 Note that \([\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6\), so we need a \(\zeta\) that has a minimal polynomial of degree 6 over \(\mathbb{Q}\). We suppose \(\zeta = 3\sqrt[3]{2} + \omega\) will work, so we ask Mathematica to look at its powers to find the least \(n\) satisfying \(\{1, \zeta, \zeta^2, \ldots, \zeta^n\}\) is linearly dependent.

Answer: \(9 + 9x + 3x^3 + 6x^4 + 3x^5 + x^6\).

6 Let \(\omega\) be a primitive 8th root of unity. Certainly, \(E_8 \subseteq \mathbb{Q}(i, \sqrt{2})\), since \(\omega = (\sqrt{2}/2) + i(\sqrt{2}/2)\).

Conversely, note that \(\omega^2 = i\) and \(\omega + \omega^{-1} = i(\sqrt{2}/2)\), so the reverse inclusion also holds.

7 First, find the roots of \(u^2 - 2u - 2\), then the roots are the squares roots of these. Or, ask Mathematica for the roots: \((\zeta_1, \zeta_2, \zeta_3, \zeta_4) = (i\sqrt{3} + 1, i\sqrt{3} - 1, -i\sqrt{3} + 1, -i\sqrt{3} - 1)\).

Evidently, any field containing \(\zeta_1\) also contains \(\zeta_3\); ditto for \(\zeta_2, \zeta_4\), hence \([E : \mathbb{Q}]\) is either 4 or 8. It doesn’t take too long to convince yourself that \(\zeta_2\) cannot be written as a rational function of \(\zeta_1\), so \([E : \mathbb{Q}] = 8\).

Note that \(\zeta_1 / \zeta_2 = \sqrt{2 + \sqrt{3}}\) and \(\zeta_2 \sqrt{2 + \sqrt{3}} = \sqrt{1 + \sqrt{3}}\). Thus \(i \in E\), so \(E \supseteq \mathbb{Q}(i, \sqrt{1 + \sqrt{3}}, \sqrt{1 - \sqrt{3}})\).

9 Proved in class, using the intermediate value theorem.

16 Look at factorization of \(x^n - 1\) in terms of \(\Phi_n(x)\). Since degrees are additive under products of polynomials, and \(\deg \Phi_n(x) = \varphi(n)\), the result follows.

Chapter 17.

1 After Exercise 16.9, we know that \([\mathbb{C} : \mathbb{R}] = 2\). There is only one group with order two, so \(\text{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}_2\). Specifically, it is generated by the automorphism \(\alpha\) of \(\mathbb{C}\) sending \(i\) to \(-i\).

2 This exercise essentially asks us to prove that complex conjugation is a ring automorphism of \(\mathbb{C}\). I’ll leave that to you (or see your notes, as I talked about it once). Let \(E = \mathbb{R}(\zeta_1, \ldots, \zeta_n)\).

We need only show that, \(\overline{\zeta}_k \in E\) for all \(k\). But, since \(0 = \overline{0} = f(\overline{\zeta}_k) = f(\zeta_k)\), this follows from the automorphism fact: \(\zeta_1\) is another root \(\zeta_{k'}\).

4 First figure out its order by computing \([E : \mathbb{Q}]\ldots 8\) (see Exercise 16.7). Then determine which permutations of \(\mathfrak{S}_4\) are allowed as automorphisms of \(E\). Conclude that \(\text{Gal}(f) = D_4\).
7 For part (a), note that the group is $V$, as found in the introduction, 17.1. There are three nontrivial subgroups of $V$, corresponding (in the notation of the introduction) to $\langle \alpha_2 \rangle$, $\langle \alpha_3 \rangle$, $\langle \alpha_4 \rangle$. What are the related fixed subfields? How about $Q(\sqrt{3})$, $Q(\sqrt{2})$, and $Q(\sqrt{6})$?

8 Given any two roots, $\zeta_1$ and $\zeta_2$, we need an automorphism $\alpha \in \text{Gal}(E/F)$ sending $\zeta_1$ to $\zeta_2$. We know that the evaluation map $\text{ev}_\zeta$ defines an automorphism between $F[x]/(f)$ and $F(\zeta)$ for any $\zeta$ that is a root of an irreducible polynomial $f$. Each such map lifts to an automorphism of the splitting field $E$, by Lemma 17.5. Compose the two, one in the forward direction and one in the reverse direction to build an automorphism $\alpha: E \rightarrow E$ that fixes $F$ and sends $\zeta_1$ to $\zeta_2$.

9 If $E/F$ is a simple extension, then $E = F(\zeta)$ for some root $\zeta$ of some irreducible polynomial $f \in F[x]$. Moreover, $[E:F] = \deg(f) = n$. Any automorphism of $E$ that fixes $F$ must send $\zeta$ to another root of $f$. (Since $E = F(\zeta)$, any such automorphism $\alpha$ is uniquely determined by where $\alpha$ sends $\zeta$.) If $|\text{Gal}(E/F)| = [E:F] = n$, then there are $n$ distinct places to send $\zeta$. That is, there are as many distinct roots of $f$ as its degree, $n$. Conclude that $f$ is separable.

10 For part (a), note that $\theta = \omega + \omega^{-1}$ is real. (Look at the unit circle. It is $2 \cos(2\pi/n)$.) This means that $Q(\omega)$ is strictly bigger than $Q(\theta)$, since it contains $\omega - \omega^{-1}$, which is imaginary. On the other hand, $\omega \theta = \omega^2 + 1$, or $\omega^2 - \omega \theta + 1 = 0$, so $\omega$ satisfies a degree two polynomial over $Q(\theta)$. Conclude that $[Q(\omega):Q(\theta)] \leq 2$. Equality then follows.

11 For part (b), recall that $\text{Gal}(Q(\omega)/Q)$ is a cyclic group of order $\varphi(n)$. Using the correspondence $H = \text{Gal}(E/K) \iff \text{Fix}(H) = K$ and the identity $[K:F] = [G:H]$, we see that we need to find a subgroup of order two. If it is generated by $\alpha$, then $\text{Gal}(Q(\omega)/Q(\theta))$ is generated by $\alpha^2$.

13 The group is $V$, as found in the introduction, 17.1. There are three nontrivial subgroups of $V$, corresponding (in the notation of the introduction) to $\langle \alpha_2 \rangle$, $\langle \alpha_3 \rangle$, $\langle \alpha_4 \rangle$. What are the related fixed subfields? How about $Q(\sqrt{3})$, $Q(\sqrt{2})$, and $Q(\sqrt{6})$?

15 Let $E$ be the splitting field of $f(x) = x^4 - 2$, with roots $\zeta_{1,3} = \pm \sqrt{2}$ and $\zeta_{2,4} = \pm i \sqrt{2}$. May check that $\delta = -i32\sqrt{2} \notin Q$, so $\text{Gal}(f) \nleq A_4$. Conclude that it’s $C_4$, $D_4$, or $S_4$. Can’t be $S_4$, since the permutation (12) is not allowed. (Only the permutation (12)(34).) Can’t be $C_4$, because there is more than one element of order 2 in $\text{Gal}(f)$: (13) and (24).

Now, figure out what subfields correspond to the subgroups on page 325.

$D_4 \overset{\text{Fix}}{\rightarrow} Q.$

$\langle 12\rangle, \langle 34 \rangle, \langle 14 \rangle, \langle 23 \rangle \overset{\text{Fix}}{\rightarrow} Q(i \sqrt{2})$

$\langle (12)(34) \rangle \overset{\text{Fix}}{\rightarrow} Q(\zeta_1 + \zeta_2)$

$\langle (12)(34) \rangle \overset{\text{Fix}}{\rightarrow} Q(\zeta_1)$

$\langle (12)(34), (14)(23) \rangle \overset{\text{Fix}}{\rightarrow} Q(i)$

$\langle (13)(24) \rangle \overset{\text{Fix}}{\rightarrow} Q(\sqrt{2})$

$\langle (13) \rangle \overset{\text{Fix}}{\rightarrow} Q(\zeta_1 - \zeta_2)$

$\langle (13) \rangle \overset{\text{Fix}}{\rightarrow} Q(\sqrt{2})$

$\langle (13) \rangle \overset{\text{Fix}}{\rightarrow} Q(\zeta_2)$

$\langle (24) \rangle \overset{\text{Fix}}{\rightarrow} Q(\zeta_1)$

$\langle (11) \rangle \overset{\text{Fix}}{\rightarrow} E = Q(i, \sqrt{2}).$

16 Let $E$ be the splitting field for $f$, so $Q \subseteq E \subseteq \overline{Q}$. We follow elements of the proof of Theorem 17.17, though the theorem itself doesn’t directly apply. Claim:

$\text{Gal}(f) = \text{Gal}(E/Q) \simeq \text{Gal}(\overline{Q}/Q)/\text{Gal}(\overline{Q}/E).$
Then the homomorphism would simply be \( \alpha \in \text{Gal}(\overline{Q}/Q) \mapsto \alpha|_E \). First, convince yourself that \( \text{Gal}(Q/E) \subseteq \text{Gal}(\overline{Q}/Q) \). Next, consider \( \beta \in \text{Gal}(Q/E) \) and \( \alpha \in \text{Gal}(\overline{Q}/Q) \). Note that \( \alpha \) must permute the roots of \( f \), since \( f \) is irreducible over \( Q \). This means \( \alpha(E) \subseteq E \), since \( E \) is built from \( Q \) by adding the roots of \( f \). Conclude that \( \alpha^{-1} \beta \alpha(e) = e \) for all \( e \in E \). That is, \( \text{Gal}(\overline{Q}/E) \) is a normal subgroup. Now follow the proof of (ii) to see that the quotient is \( \text{Gal}(E/Q) \).

17 Put \( aK = L \). Fix \( \beta \in H, \ell \in L, \) and \( k = \alpha^{-1}(\ell) \). Then, \( \alpha \beta \alpha^{-1}(\ell) = \alpha \beta (k) = \alpha (k) = \ell \), so \( \ell \in \text{Fix}(\alpha \beta \alpha^{-1}) \). The inclusion \( \text{Fix}(\alpha \beta \alpha^{-1}) \subseteq aK \) is similar. (First step: \( \alpha \beta \alpha^{-1}(e) = e \) implies \( \beta \alpha^{-1}(e) = \alpha^{-1}(e) \), so \( \beta \) fixes \( \alpha^{-1}(e) \) for all \( e \in \text{Fix}(\alpha \beta \alpha^{-1}) \).

Second part is similar. Note: everything fixes \( F \), so for first inclusion, need only show that \( \alpha \eta \in \text{Fix}(\alpha \beta \alpha^{-1}) \).

Chapter 18.

2 Let \( f \) be the quartic, here are the possible factorizations into irreducibles (degrees indicated below):

\[
\begin{align*}
(1) &\quad (x - \zeta) h_3(x) & 1 & 3 \\
(2) &\quad (x - \zeta')(x - \zeta'') h_2(x) & 1 & 1 & 2 \\
(3) &\quad h_2'(x) h_2''(x) & 2 & 2 \\
(4) &\quad \prod (x - \zeta^{(i)}) & 1, 1, 1, 1
\end{align*}
\]

In (4), all roots already lie in \( F \), so \( \text{Gal}(f) \) is trivial. In (2), a single degree two extension completes the factorization into irreducibles, so \( \text{Gal}(f) = Z_2 \). In (3), there may be a second degree two extension necessary (iff \( h_2' \neq h_2'' \)). In this case, no roots of \( h_2'' \) can be sent to roots of \( h_2'' \) by elements of \( \text{Gal}(f) \), so \( \text{Gal}(f) = Z_2 \) or \( V \). In (1), look back at Section 16.5. \( |\text{Gal}(f)| \) is 3 or 6, i.e., \( A_3 \) or \( S_3 \).

4 Note that \( g(x) = (x - \frac{-a + \sqrt{a^2 - 4b}}{2})(x - \frac{-a - \sqrt{a^2 - 4b}}{2}) \). Thus, the roots of \( g \) are \( \zeta_1 = \sqrt{\frac{a + \sqrt{a^2 - 4b}}{2}} \), \( \zeta_2 = \sqrt{\frac{a - \sqrt{a^2 - 4b}}{2}} \), and their negatives.

It is easy to check that the cubic resolvent is reducible: \( r(x) = x (x^2 - 2ax + (a^2 - 4b)) \).

With some work, we have \( \delta(g) = 4(a^2 - 4b) (8a^3 + 4b) \). Let \( \partial = \sqrt{a^2 - 4b} \). Since \( g \) is irreducible, \( \partial \notin F \), but this doesn’t necessarily mean that \( \partial \notin F \). So we are left to look at the table on page 347: \( \text{Gal}(f) \) is among: \( V, D_4 \), and \( C_4 \).

To get the first case, make \( \text{Gal}(r) = \{1\} \), so make \( \sqrt{\partial} \in F \), e.g., \( g(x) = x^4 + 9 \). For the others, you need a bit of trial and error. The roots of \( g(x) = x^4 - 5 \) are \( i^k \sqrt{5} \) for \( k = 0, 1, 2, 3 \). If \( \alpha \in \text{Gal}(g) \) takes \( i^k \sqrt{5} \) to \( i^k \sqrt{5} \), there seems to still be a choice for where to send \( i^k \sqrt{5} : \pm \sqrt{5} \), so \( \text{Gal}(g) = D_4 \). Finally, if \( \text{Gal}(g) = C_4 \), then \( [E : F] = 4 \), meaning once you have one root you have them all. Try \( x^4 + 5x^2 + 5 \), whose roots are \( \zeta_1 = \frac{1}{\sqrt{2}} \sqrt{5 + \sqrt{5}} \), \( \zeta_2 = \frac{1}{\sqrt{2}} \sqrt{5 - \sqrt{5}} \), and their negatives. Notice that \( \zeta_1 \zeta_2 = 10 \in Q \). That is, \( \zeta_2 \in Q(\zeta_1) \), hence \( [E : F] = 4 \) and we are done.

5 \( h(x) = (x^2 + a_1 x + a_0)(x^2 + b_1 x + b_0) \) with neither \( a_1^2 - 4a_0 \) nor \( b_1^2 - 4b_0 \) in \( F \), and with the latter a purely imaginary number. Suppose the roots of the first factor are \( \zeta_{1,2} \) and the second factor are \( \eta_{1,2} \). With some ingenuity, one sees that \( \delta(h) = (\zeta_1 - \zeta_2)(\eta_1 - \eta_2) \prod_i (\zeta_i^2 + b_1 \zeta_i + b_0) \).

This is clearly not real, since the first and last factors are, but the second one is clearly not (in fact, it’s purely imaginary). Conclude that \( \text{Gal}(h) \) is a transitive group not contained in \( A_4 \), i.e., it is among: \( S_4, D_4, C_4 \). If it were the latter case, then there would be only one element of order two. But we can permute the real roots and leave the complex ones alone, and vice versa, so there are at least two elements of order two in \( \text{Gal}(h) \).
According to the table on page 347, \( \text{Gal}(f) = V \). \( E = \mathbb{Q}(\sqrt{5}, i\sqrt{3}) \). Need three subfields of degree 2 over \( \mathbb{Q} \): \( \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i\sqrt{3}), \) and \( \mathbb{Q}(i\sqrt{15}) \). Watch-Out: \( \mathbb{Q}(\sqrt{5} + i\sqrt{3}) = E \).

**Chapter 19.**

3 Put \( E = \mathbb{Q}(x_1, \ldots, x_n), K = L(\delta) = \mathbb{Q}(s_1, \ldots, s_n, \delta), \) and \( L = \mathbb{Q}(s_1, \ldots, s_n) \). By Theorem 17.18, we know that \( \text{Gal}(E/K) \subseteq A_n \). Note that \( X^2 - \Delta \) is defined in \( L[X] \), with splitting field equal to \( K \). Use Theorem 17.17(i): \( \text{Gal}(E/K) \trianglelefteq \text{Gal}(E/L) = S_n \). If \( n \neq 4 \), then the only nontrivial normal subgroup of \( S_n \) is \( A_n \). Done. What about for \( n = 4 \)? Looks like you have a bit more work to do. (Hint: check that \( \alpha = (123) \in \text{Gal}(E/K) \).

**Chapter 20.**

4 Put \( \theta = \omega + \omega^{-1} \) and \( \omega = e^{2\pi i/11} \). Then \( c = \cos(2\pi/11) = \theta/2 \) has the same splitting field, etc., as \( \theta \) does. Following Theorem 17.18(ii), we see that \( \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\theta)) \trianglelefteq \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \), since the larger group is cyclic (and hence abelian). Then the quotient (isomorphic to \( \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})) \) is the quotient of a cyclic group and hence is cyclic. We have seen that \( |\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\theta))| = 2 \) and \( |\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 10 \), so the quotient has order 5.

To prove that \( \cos(2\pi/11) \) may be found by taking radicals, use the comments after Corollary 20.9 (an indirect argument about composition series for cyclic groups), or use the following direct argument: Add the radical \( \omega \) first. Then, \( \theta = \omega + \omega^{-1} \Rightarrow \theta = (\omega^2 + 1)/\omega \Rightarrow \theta^{11} = \sum_k \binom{11}{k} \omega^{2k} \). Call this last quantity \( \alpha \). Then \( c \) is a solution to the equation \( X^{11} - \alpha/2^{11} \), so you can solve \( c \) by radicals.

5 \( \mathbb{Q} \to \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{1 + \sqrt{3}}) \to \mathbb{Q}(i, \sqrt{1 + \sqrt{3}}) \).

7 For first part, need generalization of the fact that \( \mathbb{Z}/(p^k q^\ell)\mathbb{Z} \) and \( \mathbb{Z}/p^k \mathbb{Z} \times \mathbb{Z}/q^\ell \mathbb{Z} \) are isomorphic, plus facts about subgroups of Sylow \( p \)-subgroups. For second part, need classification theorems of abelian groups.