Exercise 1 (14.4: 2)**.** Find a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

The Galois group of $K \doteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ is clearly all 8 distinct maps determined by

$$\sqrt{2} \mapsto \pm\sqrt{2}$$
$$\sqrt{3} \mapsto \pm\sqrt{3}$$
$$\sqrt{5} \mapsto \pm\sqrt{5}.$$

Since K is a degree 8 extension over $\mathbb{Q}$, this means K is Galois over $\mathbb{Q}$. Now Consider $\theta = \sqrt{2} + \sqrt{3} + \sqrt{5}$. It is not fixed by any nontrivial element of the above Galois group, so by the Fundamental Theorem of Galois Theory, $\mathbb{Q}(\theta)$ cannot lie in any proper subfield of K. But since $\theta \in K$, we know $\mathbb{Q}(\theta)$ is a subfield of K. Thus $K = \mathbb{Q}(\theta)$.

Exercise 2 (14.5: 7)**.** Complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)$ of the cyclotomic field of n-th roots of unity. The field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the maximal real subfield of K.

Complex conjugation: Using the definitions of roots of unity on page 539 of DF, any primitive n-th root of unity ζ_n can be written

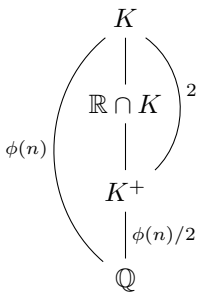
$$\zeta_n = e^{2\pi k i/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$

for some $0 \leq k \leq n-1$ (not all k in this range will give a primitive root of unity, but the actual value of k won't be needed in this proof). Then using the trigonometirc identities $\sin(-x) = -\sin(x)$ and $\cos(-x) = \cos(x)$, complex conjugation gives

$$\begin{aligned}
\overline{\zeta_n} &= \cos\left(\frac{2\pi k}{n}\right) - i\sin\left(\frac{2\pi k}{n}\right) \\
&= \cos\left(-\frac{2\pi k}{n}\right) + i\sin\left(-\frac{2\pi k}{n}\right) \\
&= e^{-2\pi k i/n} \\
&= \zeta_n^{-1}.
\end{aligned}$$

Since the elements of $\mathbb{Q}$ have no imaginary component, $\mathbb{Q}$ is fixed by complex conjugation. Thus it restricts to $\sigma_{-1} \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$.

Maximal Real Subfield: Since $\zeta_n + \zeta_n^{-1} = \zeta_n + \overline{\zeta_n} = 2\cos(2\pi k/n)$ (the imaginary components cancel out), the extension $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is real. This shows $K^+ \subset K \cap \mathbb{R}$. This gives us the tower



where $[K^+ : \mathbb{Q}] = \phi(n)/2$ was proven on the first midterm and $[K : K^+] = 2$ follows from degrees multiplying in towers. This forces one of $[K : \mathbb{R} \cap K]$ and $[\mathbb{R} \cap K : K^+]$ to be 1. But the former cannot be 1, as K contains complex elements and $\mathbb{R} \cap K$ does not. Thus $[\mathbb{R} \cap K : K^+] = 1$, so $\mathbb{R} \cap K = K^+$.

Exercise 3 (14.5: 10)**.** $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Because it was easier to type out, I denote $\sqrt[3]{2}$ by θ.

First we show that $\mathbb{Q}(\theta)$ is not Galois over $\mathbb{Q}$. We know that θ is the root of the minimal polynomial $x^3 - 2$ over $\mathbb{Q}$ (this shows that $\mathbb{Q}(\theta)$ is a degree 3 extension of $\mathbb{Q}$). But this polynomial has roots

$$\theta, \theta\zeta_3, \theta\zeta_3^2,$$

and $\theta\zeta_3, \theta\zeta_3^2$ aren't real (this follows from the explicit form of ζ_3 on page 540 of DF). Since θ, on the other hand, *is* real, this means that θ is the only one of these roots contained in $\mathbb{Q}(\theta)$. Thus the Galois group can only map θ to itself, i.e. the group is trivial. Since the Galois group is order 1 but $\mathbb{Q}(\theta)$ is a degree 3 extension over $\mathbb{Q}$, this means $\mathbb{Q}(\theta)$ is not Galois over $\mathbb{Q}$.

Now we can show the desired result. We know $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong \mathbb{Z}_n^\times$, which in particular shows that it is abelian. And every subgroup of an abelian group is necessarily normal, so by the Fundamental Theorem of Galois Theory, all subfields of $\mathbb{Q}(\zeta_n)$ must be Galois over $\mathbb{Q}$. But we just showed that $\mathbb{Q}(\theta)$ is not Galois over $\mathbb{Q}$, so it cannot be one of these subfields.

Exercise 4 (14.5: 13)**.**

1. Since a is relatively prime to n, it is relatively prime to the components of the prime decomposition. Then we have

$$\sigma_a(\zeta_{p_i^{a_i}}) = \sigma_a(\zeta_n^{d_i}) = \sigma_a(\zeta_n)^{d_i} = (\zeta_n^a)^{d_i} = (\zeta_n^{d_i})^a = \zeta_{p_i^{a_i}}^a.$$

   It is also an automorphism of $\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}$ since it still fixes $\mathbb{Q}$ and also maps $\mathbb{Q}(\zeta_{p_i^{a_i}})$ onto itself. It depends only on where $\zeta_{p_i^{a_i}}$ is mapped to, and this is determined by $a \pmod{p_i^{a_i}}$.

2. Then by Theorem 26, $\sigma_{a \pmod{p_i^{a_i}}}$ defines an isomorphism

$$(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times \to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{p_i^{a_i}})).$$

   When we apply these isomorphisms componentwise to the decomposition of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$, we get that the two products in Corollary 27 are isomorphic.

Exercise 5 (14.6: 2)**.** Determine the Galois groups of the following polynomials.

1. $x^3 - x^2 - 4$.
2. $x^3 - 2x + 4$.
3. $x^3 - x + 1$.
4. $x^3 + x^2 - 2x - 1$.

In all these, I denote the current polynomial's Galois group by G.

1. $x^3 - x^2 - 4$ factors into $(x-2)(x^2+x+2)$, and since $2 \in \mathbb{Q}$, its splitting field is determined by the second factor. The second factor's discriminant is $b^2 - 4ac = -7$. Since this isn't a rational square, DF Proposition 34 says that G isn't a subgroup of A_2. Since S_2 has no proper subfields containing A_2, this means $G \cong S_2$.

2. $x^3 - 2x + 4$ factors into $(x+2)(x^2-2x+2)$, and since $-2 \in \mathbb{Q}$, its splitting field is determined by the second factor. The second factor's discriminant is $b^2 - 4ac = -4$, so by the same logic as in part (a), $G \cong S_2$.

3. This polynomial is irreducible by the rational root test. Then by DF Equation 14.18', the discriminant of this polynomial is

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc,$$

   where $a = 0, b = -1, c = 1$. This comes out to $D = -23$, and since this isn't a square, G is not a subgroup of A_3. Once again, S_3 has no proper subsets containing A_3, so $G \cong S_3$.

4. This polynomial is irreducible by the rational root test. Then again by Equation 14.18', for $a = 1, b = -2, c = -1$, we get $D = 49$. This is a square in $\mathbb{Q}$, so G is a subgroup of A_3. But $|A_3| = 3$, so its only proper subgroup is the trivial group. But since our polynomial's roots are not contained in $\mathbb{Q}$, its Galois group cannot be trivial, so $G \cong A_3$.

Exercise 6 (14.6: 6)**.** Determine the Galois group of $x^4 + 3x^3 - 3x - 2$.

This polynomial is irreducible by Eisenstein's Criterion for $p = 2$. By the long ugly formula on the bottom of DF page 614, for $a = 3, b = 0, c = -3, d = -2$, we calculate the discriminant to be $D = -2183$. This isn't a square in $\mathbb{Q}$, so by DF Proposition 34, the polynomial's Galois group G is not a subgroup of A_4.

Additionally, we can manually calculate the resolvent cubic to be

$$h(x) = \frac{1}{64}\left(x^3 + 432x^2 + 908x + 9\right).$$

This is irreducible by the rational root test, so now we're in case (a) of DF page 615. This means $G \cong S_4$.

Exercise 7 (14.6: 11)**.** Let F be a non-Galois degree 4 extension of $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4, A_4, or D_8. Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.

First bit: By the primitive element theorem, since F is a finite extension of a character 0 field, F must be simple, i.e. $F = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{Q}$. Since it's a degree 4 extension, this means the minimal polynomial $m_\alpha(x)$ of α is quartic. Denote the splitting field of $m_\alpha(x)$ by K.

Since K is a splitting field, it's Galois over $\mathbb{Q}$. Since there are 4 roots of $m_\alpha(x)$, this means $G \doteq \text{Gal}_{\mathbb{Q}}(K)$ is a subgroup of S_4.

Since F is not Galois, we know $K \neq F$, so we have the following tower.

$$\begin{array}{c} K \\ | \\ F \\ |{\scriptstyle 4} \\ \mathbb{Q} \end{array}$$

Since $|S_4| = 24$ and the order of a subgroup divides the order of the group, this means $[K : \mathbb{Q}] = |\text{Gal}_{\mathbb{Q}}(K)|$ divides 24. Then since degrees multiply in towers, this means $[K : F]$ divides 6 (and isn't 1, since $K \neq F$). This means $[K : \mathbb{Q}] = 8, 12$, or 24. Using the list at the top of DF page 614, the only possible subgroups of S_4 of these sizes are D_8, A_4, and S_4.

Second bit: Suppose F contains a quadratic extension $\mathbb{Q}(\sqrt{D})$. We then know $[F : \mathbb{Q}(\sqrt{D})] = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$. Since A_4 has no subgroups of index 2, we know $G \neq A_4$. The only index 2 subgroup of S_4 is A_4, but since A_4 has no index 2 subgroups, we can't get 2 index 2 subgroups in a row, as required by the Galois correspondence. Thus $G = D_8$.

Conversely, suppose $G = D_8$. All subgroups in the subgroup lattice of D_8 has index 2, so by the Galois correspondence and the fact that F is degree 4 over $\mathbb{Q}$ instead of degree 2, F must contain a proper subfield. This proper subfield must then be degree 2 over $\mathbb{Q}$, i.e. it is a quadratic extension.

Exercise 8 (14.6: 44)**.** Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of a quartic $f(x)$ over $\mathbb{Q}$. Show that the quantities $\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\alpha_1\alpha_4 + \alpha_2\alpha_3$ are permuted by the Galois group of $f(x)$. Conclude that these elements are the roots of a cubic polynomial over $\mathbb{Q}$.

The Galois group G of $f(x)$ permutes the α_i, so if $\sigma \in G$, then

$$\sigma(\alpha_1\alpha_2 + \alpha_3\alpha_4) = \sigma(\alpha_1)\sigma(\alpha_2) + \sigma(\alpha_3)\sigma(\alpha_4)$$

must be one of the other two expressions (note that since the roots all lie in some field, they commute under multiplication). Using similar logic for applying σ to the other two expressions, we get that all three are permuted by G.

If we denote these three expressions by a, b, c, then they're the roots of the polynomial

$$(x - a)(x - b)(x - c).$$

We just showed that this polynomial is symmetric, so by DF Corollary 31 it is a rational function, i.e. it is a cubic polynomial over $\mathbb{Q}$.

Exercise 9 (14.7: 3)**.** Let $\text{char}(F) \neq 2$. State and prove a necessary and sufficient condition on $\alpha, \beta \in F$ so that $F(\sqrt{\alpha}) = F(\sqrt{\beta})$. Use this to determine whether $\mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$.

First bit: There are two trivial cases:

1. If α and β are both squares in F, then $\sqrt{\alpha}, \sqrt{\beta} \in F$, so $F(\sqrt{\alpha}) = F = F(\sqrt{\beta})$.
2. If one is a square and the other isn't, then one of the extensions is equal to F and the other isn't, so the extensions aren't equal.

The final case is when neither α nor β is a square in F, i.e. $\sqrt{\alpha}, \sqrt{\beta} \notin F$. Supposing $F(\sqrt{\alpha}) = F(\sqrt{\beta})$, we can write $\sqrt{\alpha}$ as $\sqrt{\alpha} = c + d\sqrt{\beta}$ for some $c, d \in F$. Squaring gives $\alpha = c^2 + 2cd\sqrt{\beta} + d^2\beta$. Since $\alpha \in F$ but $\sqrt{\beta} \notin F$, this forces $2cd = 0$. Since $\text{char}(F) \neq 2$, this means either c or d is 0. If $d = 0$, then $\sqrt{\alpha} = c \in F$, but $\sqrt{\alpha} \notin F$ by assumption, so it must be the case that $c = 0, d \neq 0$. This gives $\alpha = d^2\beta$, or

$$\frac{\alpha}{\beta} = d^2.$$

So if $F(\sqrt{\alpha}) = F(\sqrt{\beta})$, then α/β is a square in F. This condition is also sufficient: if $\alpha/\beta = d^2$ for some $d \in F$, then $\sqrt{\alpha} = d\sqrt{\beta}$, so $F(\sqrt{\alpha}) = F(\sqrt{\beta})$.

Second bit: Let $F = \mathbb{Q}(\sqrt{2})$, $\alpha = 1 - \sqrt{2}, \beta = -1$, then

$$\begin{aligned} F(\sqrt{\alpha}) &= \mathbb{Q}(\sqrt{1-\sqrt{2}}, \sqrt{2}) = \mathbb{Q}(\sqrt{1-\sqrt{2}}), \\ F(\sqrt{\beta}) &= \mathbb{Q}(i, \sqrt{2}). \end{aligned}$$

Note that the last equality on the first line above comes from this extension being of degree higher than 2, so $((1-\sqrt{2})^{1/2})^2 = 1 - \sqrt{2}$ is a basis element of that extension, so $\sqrt{2} \in \mathbb{Q}((1-\sqrt{2})^{1/2}$.

Suppose $\alpha/\beta = \sqrt{2} - 1$ is a square in $F = \mathbb{Q}(\sqrt{2})$, then

$$\sqrt{2} - 1 = (c + d\sqrt{2})^2 = c^2 + 2cd\sqrt{2} + 2d^2$$

for some $c, d \in \mathbb{Q}$. Since $c, d, c^2, d^2 \in \mathbb{Q}$ and $\sqrt{2} \neq \mathbb{Q}$, this implies

$$\begin{aligned} c^2 + 2d^2 &= -1, \\ 2cd &= 1. \end{aligned}$$

The first equality in this system is impossible, though, so the two extensions are not equal.