MATH 830 FALL 2021: HOMEWORK 2, SOLUTIONS

You may work together on these homework problems, but each student in the class must write up the solutions to this assignment entirely on their own. You may use the class notes, previous homework or class supplements, but you may not consult any other sources, including, any algebra textbook, the internet, graduate students not in this class, or any professor except your Math 830 instructor. Please upload a pdf copy of your solutions to Blackboard no later than 10pm on Monday October 5.

1. Let x, y be independent variables over $\mathbb{Z}_p$, $p > 0$ a prime. Set $F := \mathbb{Z}_p(x^p, y^p)$ and $K := \mathbb{Z}_p(x, y)$. Give a *rigorous* proof that $[K : F] = p^2$ and use this fact to show that K is not a simple extension of F. Hint: Take p^{th} powers!

Solution. Let us assume first that $[K : F] = p^2$. If K is a simple extension of F, then we can write $K = F(u)$, for some $u \in K$. By definition of K, $u = \frac{f(x,y)}{g(x,y)}$ for $f(x, y), g(x, y) \in \mathbb{Z}_p[x, y]$. Now $u^p \in F$, so u satisfies a monic polynomial of degree p with coefficients in F, which implies $[K : F] \leq p$, a contradiction.

To see that $[K : F] = p^2$, note that $K = F(x, y)$. We first prove that $[F(x) : F] = p$. Certainly $x^p \in F$, so x is a root of $h(t) := t^p - x^p \in F[t]$. We now argue that $h(t)$ is the minimal polynomial of x over F. Suppose not. Then, let $c(t)$ denote the minimal polynomial of x over F, and assume $c(t)$ is a proper factor of $h(t)$. Over K, we can write $f(t) = (t - x)^p$, which means $c(t) = (t - x)^r$, with $r < p$. Thus, $c(t) = t^r - rxt^{r-1} + \cdots + (-1)^r x^r \in F[t]$. Since $r \neq 0$ in $\mathbb{Z}_p$, we have $x \in F$. Intuitively, this clearly cannot happen.

To see formally that $x \notin F$, suppose $x = \frac{a(x^p,y^p)}{b(x^p,y^p)}$, for $a(x^p, y^p)$, $b(x^p, y^p)$ polynomials in x^p and y^p. Then $xa(x^p, y^p) = b(x^p, y^p)$ as polynomials in x, y. This is a contradiction, since wherever x appears in $b(x^p, y^p)$ its exponent is divisible by p, whereas no exponent of x in $xa(x^p, y^p)$ is divisible by p. Thus, $x \notin F$, so $h(t)$ is irreducible over F, giving $[F(x) : F] = p$. We now have $F \subseteq F(x) = \mathbb{Z}_p(x, y^p) \subseteq K = F(x)(y)$. If we show that $[K : F(x)] = p$, then by the multiplicative property of the degree symbol, we will have $[K : F] = p^2$. If we set $d(t) := t^p - y^p$, then $d(t)$ is a monic polynomial in $F(x)[t]$ having y as a root. If we know that $d(t)$ is irreducible over $F(x)$, then $d(t)$ will be the minimal polynomial of y over $F(x)$, and thus $[K : F(x)] = [F(x)(y) : F(x)] = p$, which is what we want. But the proof of this is almost the same as the proof that $h(t)$ is irreducible over F, so we will omit it.

2. Let F be a finite field having characteristic $p > 0$. For a field K, write K^* for the group of non-zero elements of K under multiplication.

(i) Prove that $|F| = p^n$, for some $n \geq 1$.
(ii) Prove that F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Conclude that any two finite fields with the same number of elements are isomorphic. Hint: F^* is a finite group.
(iii) Let $F \subseteq K$ be a finite extension of finite fields. Prove that K is a splitting field over F.
(iv) Recall from Problem 9 on Homework 1 that any irreducible polynomial with coefficients in $\mathbb{Z}_p$ is separable. Use a similar proof to show that any irreducible polynomial with coefficients in F is separable. Thus, every finite extension of a finite field is a separable extension.

Solution. For (i), since F has characteristic p, we may assume $\mathbb{Z}_p \subseteq F$. Thus, we may regard F as a vector space over $\mathbb{Z}_p$. Since F is finite, it must be finite dimensional over $\mathbb{Z}_p$. If F is n-dimensional as a vector space over $\mathbb{Z}_p$, then we have $|F| = p^n$, since as a vector space over $\mathbb{Z}_p$, $F \cong \mathbb{Z}_p^n$.

For (ii), since F^* is a finite group of order $p^n - 1$, with $1 \in F$ as the identity element, we have $\alpha^{p^n-1} = 1$, for all $\alpha \in F^*$. Thus, for all such α, $\alpha^{p^n} = \alpha$ and therefore each α is a root of $f(x) := x^{p^n} - x \in \mathbb{Z}_p[x]$. Since 0 is also a root of $f(x)$, it follows that F contains p^n (distinct) roots of $f(x)$ as a polynomial with coefficients in $\mathbb{Z}_p$. Certainly we obtain F if we adjoin these elements to $\mathbb{Z}_p$, so F is the splitting field of $f(x)$ over $\mathbb{Z}_p$. The same argument would show that any other field with p^n elements is the splitting field of $f(x)$ over $\mathbb{Z}_p$,

and since any two splitting fields for the same polynomial are isomorphic, any two finite fields with the same number of elements must be isomorphic.

For (iii), suppose $|K| = p^m$. Then, by part (ii) K is the splitting field of $x^{p^m} - x$ over $\mathbb{Z}_p$, and in fact, $K = \mathbb{Z}_p(K^*)$. But then, $K = F(K^*)$, so that K is also the splitting field of $x^{p^m} - x$ over F.

For (iv), it suffices to prove that every irreducible polynomial in $F[x]$ is a separable polynomial. Suppose $f(x) \in F[x]$ is an irreducible polynomial. By problem 8 from Homework 1, $f(x)$ has distinct roots in $\overline{F}$ if $f'(x) \neq 0$, for in this case, $f(x)$ and $f'(x)$ will have no common factor. So, suppose to the contrary that $f'(x) = 0$. Then as in the proof of problem 9 from Homework 1, $f(x) = \sum_{j=0}^{r} a_j x^{pj}$, with each $a_j \in F$. Since F is finite and the map $\phi : F \to F$ given by $\phi(a) = a^p$ is one-to-one, ϕ must also be onto. Therefore, there exist $b_j \in F$ such that $a_j = b_j^p$, for all j. Thus,

$$f(x) = \sum_{j=0}^{r} a_j x^{pj} = \sum_{j=0}^{r} b_j^p x^{pj} = (\sum_{j=0}^{r} b_j x^j)^p,$$

which contradicts the irreducibility of $f(x)$. Therefore, $f'(x) \neq 0$, so $f(x)$ has distinct roots, i.e., $f(x)$ is a separable polynomial over $\mathbb{Z}_p$.

□

Important Remark. Note that, in light of Theorem 16.1, it follows from Problem 2 that any finite extension of finite fields is a Galois extension.

3. Prove that for each $n \geq 1$, there exists an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Solution. Let K denote the splitting field of $f(x) := x^{p^n} - x$ over $\mathbb{Z}_p$. Since $f'(x) \neq 0$, $f(x)$ has p^n distinct roots in $\overline{\mathbb{Z}_p}$. If we show that these p^n roots form a field, this field must be K, since it will be the smallest subfield of $\overline{\mathbb{Z}_p}$ containing the roots of $f(x)$. However, if α, β are roots of $f(x)$, then

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta, \quad (\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta, \quad (\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$$

showing that K is a subfield of $\overline{\mathbb{Z}_p}$. Since $|K| = p^n$, we have $[K : \mathbb{Z}_p] = n$. Moreover, since the extension is separable, by the Primitive Element Theorem, there exists $\alpha \in K$ such that $K = F(\alpha)$. It follows that the minimal polynomial of α over $\mathbb{Z}_p$ has degree n, which gives what we want. □

4. Let $F \subseteq K$ be a finite extension of finite fields having characteristic $p > 0$. Assume $|F| = p^n$ and $|K| = p^m$, with $n < m$. Let $\phi : K \to K$ be the Frobenius map, i.e., $\phi(\alpha) = \alpha^p$, for all $\alpha \in K$.

(i) Show that ϕ is an automorphism of K fixing $\mathbb{Z}_p$ and that $\mathrm{Gal}(K/\mathbb{Z}_p)$ is a cyclic group generated by ϕ. Which cyclic group is $\mathrm{Gal}(K/\mathbb{Z}_p)$?

(ii) Describe the intermediate fields between $\mathbb{Z}_p$ and K? Here you need to say more than the intermediate fields correspond to the subgroups of $\mathrm{Gal}(K/\mathbb{Z}_p)$.

(iii) Determine $\mathrm{Gal}(K/F)$.

(iv) What are the intermediate fields between F and K?

(v) Conclude that if F and K are finite fields, with $|F| = p^n$ and $|K| = p^m$ and $n < m$, then (up to isomorphism) $F \subseteq K$ if and only if $n|m$.

Solution. For part (i), we have already been using the fact that when K is a field of characteristic p, then, for all $a, b \in K$, $(a + b)^p = a^p + b^p$, which follows since each binomial coefficient $\binom{p}{j}$ with $j \neq 1$ or p equals zero in K. This means $\phi(a + b) = \phi(a) + \phi(b)$. Also $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$. Therefore ϕ is a field homomorphism, and thus also injective. Since K is finite, ϕ must also be surjective, so that ϕ is an automorphism of K. Finally $\phi(a) = a^p = a$, for all $a \in \mathbb{Z}_p$, which shows that ϕ fixes $\mathbb{Z}_p$, i.e., $\phi \in \mathrm{Gal}(K/\mathbb{Z}_p)$.

Now consider ϕ^2. For all $a \in K$, $\phi^2(a) = \phi(a^p) = (a^p)^p = a^{p^2}$. An easy induction argument shows that $\phi^i(a) = a^{p^i}$, for all $a \in K$ and $i \geq 1$. By part (ii) of the previous problem, $\phi^m(a) = a^{p^m} = a$, for all $a \in K$, so that ϕ^m is the identity map. Suppose $\phi^j = id$, for some $j < m$. Then for all $a \in K$, $a = \phi^j(a) = a^{p^j}$, so that every element of K is a root of $x^{p^j} - x \in \mathbb{Z}_p[x]$. But a polynomial cannot have more roots that its degree. Thus, as an element of $\mathrm{Gal}(K/\mathbb{Z}_p)$, ϕ has order m. On the other hand, by the previous problem, K is a simple, Galois extension of $\mathbb{Z}_p$, and thus $|\mathrm{Gal}(K/\mathbb{Z}_p)| = [K : \mathbb{Z}_p] = m$, which implies that $\mathrm{Gal}(K/\mathbb{Z}_p) = \langle\phi\rangle$, the cyclic group of order m.

For (ii), since the extension $\mathbb{Z}_p \subseteq K$ is Galois, the intermediate fields between $\mathbb{Z}_p$ and K are in 1-1 correspondence with the subgroups of $\mathrm{Gal}(K/\mathbb{Z}_p)$. Now, since $\mathrm{Gal}(K/\mathbb{Z}_p) \cong \mathbb{Z}_m$, the subgroups of $\mathrm{Gal}(K/\mathbb{Z}_p)$ are of the form $\langle \phi^r \rangle$ with $r|m$. For each such r, there is a corresponding subfield of the fixed field of $\langle \phi^r \rangle$. It is easy to check that an element a of K is fixed by $\langle \phi^r \rangle$ if and only if it is fixed by ϕ^r, i.e., if and only if $a^{p^r} = a$. In other words, the fixed field of $\langle \phi^r \rangle$ is the splitting field of $x^{p^r} - x$ over $\mathbb{Z}_p$.

For (iii), from problem 2 we know that F is the splitting field of $x^{p^n} - x$, and thus $a \in K$ belongs to F if and only of $\phi^n(a) = a$. In other words, F is the fixed field of $\langle \phi^n \rangle$. By the Galois correspondence theorem, $\mathrm{Gal}(K/F) = \langle \phi^n \rangle$, a cyclic group of order r, where $m = rn$.

For (iv), since the intermediate fields between F and K correspond to the subgroups of $\mathrm{Gal}(K/F)$, we want the subgroups of $\langle \phi^n \rangle$. Now, $\langle \phi^n \rangle$ is a cyclic subgroup of $\langle \phi \rangle$ of order r, where $m = rn$, , so its subgroups are of the form $\langle \phi^{ns} \rangle$, with $s|r$. It follows from (iii) that the intermediate fields between F and K are the splitting fields of $x^{p^{ns}} - x$, with s dividing r.

For (v), it follows from (iii) that if $F \subseteq K$ are finite fields with $F = \mathbb{Z}_{p^n}^n$ and $K = \mathbb{Z}_{p^m}$, then $n|m$. Conversely, suppose $n|m$ and F and K are finite fields satisfying $|F| = p^n$ and $|K| = p^m$, with $n < m$. Then by problem 2, K is a splitting field of $x^{p^m} - x$ and over $\mathbb{Z}_p$ and F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Fix K. Then by (ii), since $n|m$, there is a subfield F_0 of K whose order is p^n and it is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Since splitting fields for the same polynomials over the same base field are isomorphic, F is isomorphic to F_0. Thus, up to isomorphism, F is contained in K. □

5. Let $F := \mathbb{Q}$ and K denote the splitting field of $x^7 - 1$ over $\mathbb{Q}$. Find (with proof) $\mathrm{Gal}(K/F)$ and then use the Galois Correspondence Theorem to find (with proof) all intermediate fields between F and K. You may use the fact that $x^6 + x^5 + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Solution. Set $\epsilon := e^{\frac{2\pi i}{7}}$, a primitive 7th root of unity, so that $1, \epsilon, \epsilon^2, \ldots \epsilon^6$ are the roots of $x^7 - 1$. Thus, $K := \mathbb{Q}(\epsilon)$ is the splitting field of $x^7 - 1$ over $\mathbb{Q}$. Since ϵ is a root of $f(x) := x^6 + x^5 + \cdots + x + 1$, which is irreducible over $\mathbb{Q}$, $f(x)$ is the minimal polynomial of ϵ over $\mathbb{Q}$ and thus $[K : \mathbb{Q}] = 6$. Since $K = \mathbb{Q}(\epsilon)$ is Galois over $\mathbb{Q}$, $\mathrm{Gal}(K/F)$ is a group of order six. We will show that $\mathrm{Gal}(K/F) \cong \mathbb{Z}_6$. Since ϵ^3 is also a root of $f(x)$, there is a field isomorphism $\sigma : K \to \mathbb{Q}(\epsilon^3) \subseteq K$ such that $\sigma(\epsilon) = \epsilon^3$. Moreover, $[\mathbb{Q}(\epsilon^3) : \mathbb{Q}] = 6$, therefore $\mathbb{Q}(\epsilon^3) = K$, so that $\sigma \in \mathrm{Gal}(K/F)$. If we show that the values $\epsilon, \sigma(\epsilon), \ldots, \sigma^5(\epsilon)$ are distinct, this will show that $1, \sigma, \ldots, \sigma^5$ are distinct elements of $\mathrm{Gal}(K/F)$ and it will follow that $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ is cyclic of order six.

Now,

$$
\begin{aligned}
&id(\epsilon) = \epsilon.\\
&\sigma(\epsilon) = \epsilon^3.\\
&\sigma^2(\epsilon) = \sigma(\epsilon^3) = \sigma(\epsilon)^3 = (\epsilon^3)^3 = \epsilon^9 = \epsilon^2.\\
&\sigma^3(\epsilon) = \sigma(\sigma^2(\epsilon)) = \sigma(\epsilon^2) = \sigma(\epsilon)^2 = \epsilon^6.\\
&\sigma^4(\epsilon) = \sigma(\epsilon^6) = \sigma(\epsilon)^6 = \epsilon^{18} = \epsilon^4.\\
&\sigma^5(\epsilon) = \sigma(\epsilon^4) = \sigma(\epsilon)^4 = \epsilon^{12} = \epsilon^5,
\end{aligned}
$$

which gives what we want. It now follows that $H_1 := \langle \sigma^2 \rangle$ and $H_2 := \langle \sigma^3 \rangle$ are the only proper subgroups of $\mathrm{Gal}(K/F)$, so that the fixed fields K^{H_1} and K^{H_2} are the only intermediate fields between $\mathbb{Q}$ and K.

To find K^{H_1}, it suffices to find the elements of K fixed by σ^2. We first calculate σ^2 on the basis $1, \epsilon, \ldots, \epsilon^5$, for K over $\mathbb{Q}$.

$$
\begin{aligned}
&\sigma^2(1) = 1.\\
&\sigma^2(\epsilon) = \epsilon^2.\\
&\sigma^2(\epsilon^2) = \sigma^2(\epsilon)\sigma^2(\epsilon) = \epsilon^2\epsilon^2 = \epsilon^4.\\
&\sigma^2(\epsilon^3) = \sigma^2(\epsilon)^3 = \epsilon^6 = 1 - \epsilon - \epsilon^2 - \epsilon^3 - \epsilon^4 - \epsilon^5.\\
&\sigma^2(\epsilon^4) = \sigma^2(\epsilon)^4 = \epsilon^8 = \epsilon.\\
&\sigma^2(\epsilon^5) = \sigma^2(\epsilon)^5 = \epsilon^{10} = \epsilon^3.
\end{aligned}
$$

It follows that if $\gamma = a + b\epsilon + c\epsilon^2 + c\epsilon^3 + e\epsilon^4 + f\epsilon^5 \in K$, then

$$\begin{aligned}\sigma^2(\gamma) &= a + b\epsilon^2 + c\epsilon^4 + d(-1 - \epsilon - \epsilon^2 - \epsilon^3 - \epsilon^4 - \epsilon^5) + e\epsilon + f\epsilon^3 \\ &= (a-d) + (e-d)\epsilon + (b-d)\epsilon^2 + (f-d)\epsilon^3 + (c-d)\epsilon^4 + -d\epsilon^5\end{aligned}$$

If $\gamma \in K^{H_1}$, then $\gamma = \sigma^2(\gamma)$. This yields the system of equations

$$\begin{aligned}a &= a - d \\ b &= e - d \\ c &= b - d \\ d &= f - d \\ e &= c - d \\ f &= -d\end{aligned}$$

It follows that $d = 0$, $f = 0$, $b = c = e$. Thus, $\gamma = a + b\epsilon + b\epsilon^2 + b\epsilon^4 = a + b(\epsilon + \epsilon^2 + \epsilon^4)$. Moreover, the equations above for σ^2, show that $\epsilon + \epsilon^2 + \epsilon^4$ is fixed by σ^2, and thus any expression of the form $a + b(\epsilon + \epsilon^2 + \epsilon^4)$ is fixed by σ^2. It follows that $K^{H_1} = \{a + b(\epsilon + \epsilon^2 + \epsilon^4) \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\epsilon + \epsilon^2 + \epsilon^4)$.

To find K^{H_2}, we will argue indirectly. Note that to find K^{H_2}, we need to find the elements of K fixed by σ^3. An easy calculation shows that:

$\sigma^3(1) = 1$.
$\sigma^3(\epsilon) = \epsilon^6 = -1 - \epsilon - \epsilon^2 - \epsilon^3 - \epsilon^4 - \epsilon^5$.
$\sigma^3(\epsilon^2) = \epsilon^{12} = \epsilon^5$.
$\sigma^3(\epsilon^3) = \epsilon^{18} = \epsilon^4$.
$\sigma^3(\epsilon^4) = \epsilon^{24} = \epsilon^3$.
$\sigma^3(\epsilon^5) = \epsilon^{30} = \epsilon^2$.

Note that $\sigma^3(\epsilon^3 + \epsilon^4) = \sigma^3(\epsilon^3) + \sigma^3(\epsilon^4) = \epsilon^4 + \epsilon^3$, so that $\epsilon^3 + \epsilon^4$ belongs to K^{H_2}, and thus $\mathbb{Q}(\epsilon^3 + \epsilon^4) \subseteq K^{H_2}$. Now, since $|H_2] = 2$, $[K^{H_2} : \mathbb{Q}] = 3$. Thus, there are no fields between $\mathbb{Q}$ and K^{H_2}. It follows that $K^{H_2} = \mathbb{Q}(\epsilon^3 + \epsilon^4)$.

Finally, since $\mathrm{Gal}(K/F)$ is abelian, every subgroup is normal in $\mathrm{Gal}(K/F)$, so that $\mathbb{Q}(\epsilon + \epsilon^2 + \epsilon^4)$ and $\mathbb{Q}(\epsilon^3 + \epsilon^4)$ are Galois over $\mathbb{Q}$. □

6. Let $F := \mathbb{Q}$ and K denote the splitting field of $(x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$. Find (with proof) $\mathrm{Gal}(K/F)$ and then use the Galois Correspondence Theorem to find (with proof) all intermediate fields between F and K.

Solution. Note that $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. By Examples 12.2 and 15.2 (a), $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree four over $\mathbb{Q}$ and has intermediate fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$. It is easy to see that $\sqrt{5}$ does not belong to any of these fields, therefore $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (since $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ cannot equal $\mathbb{Q}(\sqrt{5})$). Therefore $[K : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$, and thus, $[K : \mathbb{Q}] = 8$. We argue that $\mathrm{Gal}(K/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The proof is similar to the proof that the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$, as given in Example 12.2. Now, if $\sigma \in \mathrm{Gal}(K/F)$, $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{3}) = \pm\sqrt{3}, \sigma(\sqrt{5}) = \pm\sqrt{(5)}$. There are eight possible such automorphisms and they all exist. For example, to see that there is $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = -\sqrt{3}, \sigma(\sqrt{5}) = -\sqrt{5}$, we start with the automorphism $\phi : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ that takes $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$, which exists by Example 12.2. Now the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is $x^2 - 5$. Thus, by Homework 1, problem 7, there exists a field isomorphism $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5})$ such that σ extends ϕ and $\sigma(\sqrt{5}) = -\sqrt{5}$. Thus, $\sigma \in \mathrm{Gal}(K/F)$ has the required properties. It is easy to see that $\sigma^2 = id$. In a similar way, we can create six other non-identity elements that take any combination of roots to $x^2 - 2, x^2 - 3, x^2 - 5$ to any other combination of corresponding roots. In fact, the easiest way to see this is to take ϕ to be any one of the four elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ found in Example 12.2 and to apply problem 7 on Homework to extend each of these to K by sending $\sqrt{5}$ to $\sqrt{5}$ or $\sqrt{5}$ to $-\sqrt{5}$.

We can easily identify $\mathrm{Gal}(K/F)$ as $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ if we write $\mathbb{Z}_2 = \{1, -1\}$ as a multiplicative group. Then the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are:

$$(1,1,1), (-1,1,1), (1,-1,1), (1,1,-1), (-1,-1,1), (1,-1,1), (1,1,-1), (-1,-1,-1).$$

Clearly, σ as defined above corresponds to $(-1,-1,-1)$. And likewise, the element $\tau \in \mathrm{Gal}(K/F)$ that takes $\sqrt{2}$ to $\sqrt{2}$, $\sqrt{3}$ to $-\sqrt{3}$, $\sqrt{5}$ to $-\sqrt{5}$ is identified with $(1,-1,-1)$. If one identifies the elements of $\mathrm{Gal}(K/F)$ with the triples above, and writes out the two groups tables, one can see the required isomorphism of groups.

As for the subgroups of $\mathrm{Gal}(K/F) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, one has to be a bit careful, since if A, B are groups, then the subgroups of $A \times B$ are not only the subgroups $H \times K$, where H is a subgroup of A and K is a subgroup of B. While the $H \times K$ are certainly subgroups of $A \times B$, not every subgroup of $A \times B$ has this form. (FWIW: It is true for rings with identity that if $J \subseteq R_1 \times R_2$ is an ideal in the product of rings, then $J = I_1 \times I_2$, for ideals $I_1 \subseteq R_1$ and $I_2 \subseteq R_2$.) However, if $L \subseteq A \times B$ is a subgroup, then L_1 the set of first components of the elements of L forms a subgroup of A and similarly, L_2, the second components of the elements of L form a subgroup of B, and $L \subseteq L_1 \times L_2$. This latter fact will still help us identity the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathrm{Gal}(K/F)$. The first thing to note is that every non-identity element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order two, hence they each generate a subgroup of order two and account for all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ of order two. Let us identify each of these subgroups by their generators:

$$
\begin{aligned}
C_1 &\leftrightarrow (-1,1,1)\\
C_2 &\leftrightarrow (1,-1,1)\\
C_3 &\leftrightarrow (1,1,-1)\\
C_4 &\leftrightarrow (-1,-1,1)\\
C_5 &\leftrightarrow (1,-1,-1)\\
C_6 &\leftrightarrow (-1,1,-1)\\
C_7 &\leftrightarrow (-1,-1,-1)
\end{aligned}
$$

Since each of these subgroups has index four in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, their fixed fields have degree four over $\mathbb{Q}$. For ease of notation, we will write C_i' instead of K^{C_i} for the fixed field of C_i. With the identification of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with $\mathrm{Gal}(K/F)$ above, it is clear, say, that C_1 fixes $\sqrt{3}, \sqrt{5}$, and therefore $\mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq C'$ and since $\mathbb{Q}(\sqrt{3},\sqrt{5})$ has degree four over $\mathbb{Q}$, we must have $C_1' = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Another case: C_4 clearly fixes $\sqrt{6}$ and $\sqrt{5}$, so that $C_4' = \mathbb{Q}(\sqrt{6},\sqrt{5})$. Thus, we obtain

$$
\begin{aligned}
C_1' &= \mathbb{Q}(\sqrt{3},\sqrt{5})\\
C_2' &= \mathbb{Q}(\sqrt{2},\sqrt{5})\\
C_3' &= \mathbb{Q}(\sqrt{2},\sqrt{3})\\
C_4' &= \mathbb{Q}(\sqrt{6},\sqrt{5})\\
C_5' &= \mathbb{Q}(\sqrt{2},\sqrt{15})\\
C_6' &= \mathbb{Q}(\sqrt{3},\sqrt{10})\\
C_7' &= \mathbb{Q}(\sqrt{6},\sqrt{15}).
\end{aligned}
$$

It might seem that we have omitted some subfields of degree four over $\mathbb{Q}$, say $E := \mathbb{Q}(\sqrt{10},\sqrt{15})$. But $\sqrt{10}\cdot\sqrt{15} = 5\sqrt{6} \in E$, and thus $\sqrt{6} \in E$. Therefore, E contains $\mathbb{Q}(\sqrt{6},\sqrt{15})$, which forces $E = C_7'$. This shows the power of the Galois Correspondence Theorem. We have accounted for all of the subgroups of $\mathrm{Gal}(K/F)$ of order two, and have therefore accounted for all of the intermediated field having degree four over $\mathbb{Q}$, even though there may be multiple ways to represent each intermediate field.

We now identify seven subgroups of order four, $K_1, \ldots, , K_7$. Since these subgroups have index two in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathrm{Gal}(K/F)$, it will follow that their fixed fields K_i' (using the same notation as before) will have degree two over $\mathbb{Q}$. Note that a basis for K over F is $1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}$. If we adjoin each of the basis elements, except 1, to $\mathbb{Q}$ this will give us seven of the expected fixed fields of degree two over $\mathbb{Q}$. But we also need to see which fixed field corresponds to which subgroup of order four and that there are no other intermediate fields having degree two over $\mathbb{Q}$.

We first identify the subgroups of order four having the form $H \times K$. Let $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. Then $K_1 := G \times \{1\}$ is a subgroup of order four. If we let $\sigma_2, \sigma_3, \sigma_4$ be as in Example 12.2, and set $H_2 := \langle \sigma_2 \rangle$, $H_3 := \langle \sigma_3 \rangle$, $H_4 := \langle \sigma_4 \rangle$ be the corresponding subgroups, then $K_2 := H_2 \times \mathbb{Z}_2, K_3 := H_3 \times \mathbb{Z}_2, K_3 := H_4 \times \mathbb{Z}_2$ are the remaining subgroups of $\mathrm{Gal}(K/F)$ of the form $H \times K$. Note that in terms of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ we have

$$\begin{aligned}
K_1 &= \{(1,1,1), (-1,1,1), (1,-1,1), (-1,-1,1)\} \\
K_2 &= \{(1,1,1), (1,1,-1), (1,-1,1), (1,-1,-1)\} \\
K_3 &= \{(1,1,1), (1,1,-1), (-1,1,1), (-1,1,-1)\} \\
K_4 &= \{(1,1,1), (1,1,-1), (-1,-1,1), (-1,-1,-1)\}.
\end{aligned}$$

We can now see that the corresponding fixed fields are

$$\begin{aligned}
K_1' &= \mathbb{Q}(\sqrt{5}) \\
K_2' &= \mathbb{Q}(\sqrt{2}) \\
K_3' &= \mathbb{Q}(\sqrt{3}) \\
K_4' &= \mathbb{Q}(\sqrt{6}).
\end{aligned}$$

We now list three more subgroups of order four:

$$\begin{aligned}
K_5 &= \{(1,1,1), (-1,-1,1), (-1,1,-1), (1,-1,-1)\} \\
K_6 &= \{(1,1,1), (-1,-1,-1), (1,-1,1), (-1,1,-1)\} \\
K_7 &= \{(1,1,1), (-1,-1,-1), (-1,1,1), (1,-1,-1)\}.
\end{aligned}$$

For these subgroups, we clearly have

$$\begin{aligned}
K_5' &= \mathbb{Q}(\sqrt{30}) \\
K_6' &= \mathbb{Q}(\sqrt{10}) \\
K_7' &= \mathbb{Q}(\sqrt{15}).
\end{aligned}$$

To see that we have accounted for all of the subgroups, and hence, all of the intermediate fields, we just have to see that there are no more subgroups of order four. Let us do so by examining the last coordinates of the elements of a subgroup of order four. If all of the last coordinates are 1, there is clearly one such subgroup, namely, K_1. If at least one element, say a has last coordinate -1, there has to be at least two such elements, because, if b is a non-identity element with 1 as last coordinate, ab is a non-identity element with -1 as a last coordinate. On the other hand, if a, b are non-identity elements, with -1 as the last coordinate, ab has last coordinate 1. Thus, except for K_1, any subgroup of order four has two elements with last coordinate 1 and two elements with last coordinate -1. Now, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements with -1 in the last coordinate. There are six ways to choose two of them, say a, b. Then it is not hard to see that $\{(1,1,1), a, b, ab\}$ forms a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Since there are six ways to do this, and we have found six such subgroups above, we have accounted for all possible subgroups of order four, and therefore all intermediate fields having degree two over $\mathbb{Q}$. □

7. Suppose $F \subseteq K$ is a finite extension of fields and $K = F(\alpha_1, \ldots, \alpha_n)$. Give a proof by induction on n that $|\mathrm{Gal}(K/F)| \leq [K : F]$. Hint: First get a good understanding of the case $n = 2$. For this, find the number of field homomorphisms $F(\alpha_1) \to F(\alpha_1, \alpha_2)$ fixing F. Now work out how to use problem 7 from Homework 1 to count the number of automorphisms of $F(\alpha_1, \alpha_2)$ that fix F. Once you have done this, you should be able to do the general case.

Solution. Since K is finite over F, we can assume $K = F(\alpha_1, \ldots, \alpha_n)$. We may further assume that no α_{i+1} belongs to $F(\alpha_1, \ldots, \alpha_i)$. We induct on i to show that the number of field homomorphisms from $F(\alpha_1, \ldots, \alpha_i)$ to K fixing F is less than or equal to $[F(\alpha_1, \ldots, \alpha_i) : F]$. The case $i = 1$ is covered by Proposition 2.1, for if $f(x)$ denotes the minimal polynomial of α_1 over F, and $\phi : F(\alpha_1) \to K$ is a homomorphism fixing F, then $\phi(\alpha_1)$ must be a root of $f(x)$. Since there are at most $\deg(f(x)) = [F(\alpha_1) : F]$ roots of $f(x)$ in K, this gives what we want.

Now suppose $i > 1$ and there are s field homomorphisms from $E := F(\alpha_1, \ldots, \alpha_i)$ to K fixing F with $s \leq [F(\alpha_1, \ldots, \alpha_i) : F]$. Let $g(x)$ denote the minimal polynomial of α_{i+1} over E. Let $\phi : E \to K$ be a field homomorphism fixing F. Set $E' := \phi(E)$, so that ϕ is field isomorphism from E to E'. As in problem 7 in Homework 1, we let $g^\phi(x)$ denote the polynomial in $E'[x]$ obtained by applying ϕ to the coefficients of $g(x)$. Suppose $d := \deg(g(x))$ and $\sigma : E(\alpha_{i+1}) \to K$ is a field homomorphism extending ϕ. Then $\sigma(\alpha_{i+1})$ must be a root of $g^\phi(x)$ in K. Since there are at most d such roots, the number of field homomorphisms $\sigma : E(\alpha_{i+1}) \to K$ extending ϕ is less than or equal to $d = [E(\alpha_{i+1}) : E]$. Now, suppose $\tau : E(\alpha_{i+1}) \to K$ is a field homomorphism fixing F. Then $\tau_{|_E} : E \to K$ is a field homomorphism from E to K fixing F. In other words, any field homomorphism from $E(\alpha_{i+1}) \to K$ fixing F is the extension of a field homomorphism from E to K fixing F. Now, there are s field homomorphisms $\phi : E \to K$ and at most d extensions of each ϕ to $E(\alpha_{i+1})$, therefore there are at most

$$sd \leq [E : F] \cdot [E(\alpha_{i+1}) : E] = [F(\alpha_1, \ldots, \alpha_{i+1}) : F],$$

homomorphisms from $F(\alpha_1, \ldots, \alpha_{i+1})$ to K fixing F. Thus, by induction on i, when $i = n$, we have that the number of field homomorphisms from $K \to K$ fixing F is less than or equal to $[K : F]$, which completes the proof. $\square$