SPRING 2023: MATH 791 EXAM 3 SOLUTIONS

You will work in teams on this exam. You may use your notes, the Daily Summary, and any homework you have done, but you may not consult any other sources, including, any algebra textbook, the internet, any graduate students not on your team, or any professor except your Math 791 instructor. You may not cite without proof any facts not covered in class or the homework. All members of each team should contribute to the team's effort. The solutions should be typeset in LaTex. Each team member should also participate in the typesetting effort. Each team should upload a pdf file of its solution to Canvas no later than 5pm, Friday May 12. Note: Please do not upload solutions in any other format.

Each problem is worth 10 points. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. Good luck on the exam!

1. Prove the following statements about finite fields. You may use the following fact: Let F be a field and $f(x) \in F[x]$ a non-constant polynomial. If $f(x)$ and $f'(x)$ are relatively prime, then $f(x)$ has distinct roots in its splitting field.

(i) If F is a finite field, then F contains a subfield isomorphic to $\mathbb{Z}_p$, p prime, and $|F| = p^n$, for some n.
(ii) Given a prime p and an integer $n \geq 1$, there exists a field F with p^n elements, namely the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Prove this by showing that F turns out to be the set of distinct roots of $x^{p^n} - x$.
(iii) If F is a field with p^n elements, then F is a splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. Conclude (with justification) that any two fields with p^n elements are isomorphic.
(iv) Suppose $F \subseteq K$ are finite fields with $|F| = p^n$ and $|K| = p^m$. Then $n \mid m$. Conversely, if K is a field with p^m elements and $n \mid m$, then there exists a subfield $F \subseteq K$ with $|F| = p^n$.
(v) If K is a finite field with $|K| = p^m$, then there is a *unique* subfield F of K with $|F| = p^n$, for all n dividing m.

Solution. For (i), define $\phi : \mathbb{Z} \to F$ by $\phi(0) := 0_F$ and $\phi(n) := n_F, \phi(-n) := -n_F$, for $n > 0$, where n_F means $1_F + \cdots + 1_F$, n times. It is easy to check that ϕ is a ring homomorphism. Since F is an integral domain, the kernel of ϕ must be generated by a prime p. Thus, $\mathbb{Z}_p$ is isomorphic to a subring of F. Without loss of generality, we may assume $\mathbb{Z}_p \subseteq F$. Since F may be regarded as a vector space over the finite field $\mathbb{Z}_p$, we have $|F| = p^n$, if $n = \dim_{\mathbb{Z}_p}(F)$.

For (ii), let F denote the splitting field of $f(x) := x^{p^n} - x$ over $\mathbb{Z}_p$. Since $f(x)$ and $f'(x)$ are relatively prime in $\mathbb{Z}_p[x]$, $f(x)$ has p^n distinct roots in F. Now, if $\alpha, \beta \in F$ are roots of $f(x)$, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ and $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, hence $\alpha + \beta$ and $\alpha\beta$ are roots of $f(x)$. Similarly, 0, $-\alpha$ and α^{-1} ($\alpha \neq 0$) are roots of $f(x)$ Thus, the set of p^n distinct roots of $f(x)$ form a subfield of F, and since F is the smallest field containing the roots of $f(x)$, the elements of F are the roots of $f(x)$. Thus, $|F| = p^n$.

For (iii), 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 (iv) and (v) first suppose we have $\mathbb{Z}_p \subseteq F \subseteq K$. Then $m = [K : \mathbb{Z}_p] = [K : F] \cdot [F : \mathbb{Z}_p] = [K : F] \cdot n$, showing n divides m. Conversely, suppose $n \mid m$, and $|K| = p^m$. Since K is Galois over $\mathbb{Z}_p$ with Galois group $G := \text{Gal}(K/\mathbb{Z}_p)$ generated by the Frobenius map ϕ (by problem 2), $|G| = m$ since $\phi^m(\alpha) = \alpha^{p^m} = \alpha$, for all $\alpha \in K$. Write $m = nc$ and let H be the subgroup of G generated by ϕ^n and $F := K^H$. Then

$[F : \mathbb{Z}_p] = [G : H] = n$, so $|F| = p^n$. Since H is the unique subgroup of G having index n, F is the unique subfield of K with p^n elements (by the Galois Correspondence Theorem).

2. Let p be a prime and $\mathbb{Z}_p \subseteq K$ be a finite extension. Prove that K is Galois over $\mathbb{Z}_p$ with Galois group generated by the Frobenius map $\phi(\alpha) = \alpha^p$, for all $\alpha \in K$. Conclude that any finite extension $F \subseteq K$ of finite fields is a Galois extension with cyclic Galois group.

Solution. Suppose $|K| = p^m$, so that every element $\alpha \in K$ has the property that $\phi^m(\alpha) = \alpha^{p^m} = \alpha$. Thus ϕ^m is the identity element in $G := \mathrm{Gal}(K/\mathbb{Z}_p)$. Suppose ϕ^r is the identity, for some $r < m$. Then for all $\alpha \in K$, $\alpha = \phi^r(\alpha) = \alpha^{p^r}$, which implies that $x^{p^r} - x$ has p^m roots, a contradiction. Thus

$$m = \langle \phi \rangle \leq G \leq [K : \mathbb{Z}_p] = m.$$

It follows that $G = \langle \phi \rangle$ and $|G| = [K : \mathbb{Z}_p]$, so K is a Galois extension of $\mathbb{Z}_p$ whose Galois group is generated by ϕ. For the second statement, if $F \subseteq K$ is a finite extension of fields, then we have $\mathbb{Z}_p \subseteq F \subseteq K$, for some prime p, and since K is Galois over $\mathbb{Z}_p$, it is also Galois over F, by the Galois Correspondence Theorem. Since $\mathrm{Gal}(K/F) \subseteq \mathrm{Gal}(K/\mathbb{Z}_p)$, and the latter group is cyclic, $\mathrm{Gal}(K/F)$ is also cyclic.

3. Let p be a prime and x, y indeterminates over $\mathbb{Z}_p$. Set $F := \mathbb{Z}_p(x^p, y^p)$ and $K := \mathbb{Z}_p(x, y)$. Find (with proof) infinitely may intermediate fields between F and K. Hint: Review the proof of the existence of primitive elements.

Solution. The same proof from class when $p = 2$ will show that there is no primitive element for the extension $F \subseteq K$. We claim the fields $F(x + x^{p^n}y)$ are distinct, for $n \geq 1$. Suppose $E := F(x + x^{p^n}y) = F(x + x^{p^m}y)$, with $n \neq m$. Then $(x + x^{p^n}y) - (x + x^{p^m}y) = (x^{p^n} - x^{p^m})y \in E$. Since $x^{p^n} - x^{p^m} \in F$, we have $y \in E$. Thus, $x^{p^n}y \in E$, and hence $x \in E$. It follows that $K = E = F(x + x^{p^n}y)$, a contradiction. Thus, the fields $F(x + x^{p^n}y)$ are distinct, and hence there are infinitely many intermediate fields between F and K.

4. Construct a field with K with 32 elements, find $\mathrm{Gal}(K/\mathbb{Z}_2)$ and show that K is Galois over $\mathbb{Z}_2$. Then exhibit the one-to-one correspondence between the intermediate fields between $\mathbb{Z}_2$ and K and the subgroups of $\mathrm{Gal}(K/\mathbb{Z}_2)$.

Solution. By problem 1, if K denotes the splitting field of $x^{32} - x$ over $\mathbb{Z}_2$, then K is a field with 32 elements, and by problem 2, K is Galois over $\mathbb{Z}_2$. Moreover, $[K : \mathbb{Z}_2] = 5$ and $\mathrm{Gal}(K/\mathbb{Z}_2) \cong \mathbb{Z}_5$. Since there are no proper subgroups of $\mathbb{Z}_5$, by the Galois Correspondence Theorem there are no intermediate fields between $\mathbb{Z}_2$ and K.

5. Let $\gamma \in \mathbb{C}$ be a primitive 8th root of unity, e.g., $e^{\frac{2\pi i}{8}}$. Set $\alpha := \gamma + \gamma^2$. Find $p(x)$, the minimal polynomial of α over $\mathbb{Q}$, and all of its roots.

Solution. Since γ satisfies $x^8 - 1 = (x^4 - 1)(x^4 + 1)$, and does not satisfy $x^4 - 1$, γ satisfies $x^4 + 1$. To see that $x^4 + 1$ is irreducible over $\mathbb{Q}$, since it is a primitive polynomial, it suffices to show that $x^4 + 1$ is irreducible over $\mathbb{Z}$. $x^4 + 1$ clearly has no roots in $\mathbb{Z}$, so one has to show that there is not an equation of the form $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$, with $a, b, c, d \in \mathbb{Z}$. This polynomial equation yields a system of four equations in the unknowns a, b, c, d which is easily seen to not have a solution in $\mathbb{Z}$, so that $x^4 + 1$ is irreducible over $\mathbb{Q}$. Thus, $x^4 + 1$ is the minimal polynomial of γ over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$ and $1, \gamma, \gamma^2, \gamma^3$ is a basis for $\mathbb{Q}(\gamma)$ over $\mathbb{Q}$. Multiplying each basis element by α yields the following system of equations

$$\begin{aligned}
\alpha \cdot 1 &= 0 \cdot 1 + 1 \cdot \gamma + 1 \cdot \gamma^2 + 0 \cdot \gamma^3 \\
\alpha \cdot \gamma &= 0 \cdot 1 + 0 \cdot \gamma + 1 \cdot \gamma^2 + 1 \cdot \gamma^3 \\
\alpha \cdot \gamma^2 &= -1 \cdot 1 + 0 \cdot \gamma + 0 \cdot \gamma^2 + 1 \cdot \gamma^3 \\
\alpha \cdot \gamma^3 &= -1 \cdot 1 + -1 \cdot \gamma + 0 \cdot \gamma^2 + 0 \cdot \gamma^3.
\end{aligned}$$

We may rewrite this sytem of equation as a matrix equation

$$\begin{pmatrix} \alpha & -1 & -1 & 0 \\ 0 & \alpha & -1 & -1 \\ 1 & 0 & \alpha & -1 \\ 1 & 1 & 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Since the corresponding system of equations has a non-trivial solution, the determinant of the coefficient matrix equals zero. This shows that α is a root of the polynomial $p(x) = x^4 + 2x^2 + 4x + 2$. By Eisenstein's criterion, $p(x)$ is irreducible over $\mathbb{Q}$, so that $p(x)$ is the minimal polynomial for α over $\mathbb{Q}$.

There are several ways to find the other roots of $p(x)$. Here is one way. Set $K := \mathbb{Q}(\gamma)$ and compute $\mathrm{Gal}(K/\mathbb{Q})$. Since $[K : \mathbb{Q}] = 4$ and K is Galois over $\mathbb{Q}$ (its a simple extension that is the splitting field of $x^4 + 1$ over $\mathbb{Q}$ - see the April 24 Daily Update), there are three non-trial elements in $\mathrm{Gal}(K/F)$. If we apply these automorphisms to α, we will obtain the other roots of $p(x)$. Now, $\gamma, \gamma^3, \gamma^5, \gamma^7$ are the four primitive 8^{th} roots of unity, and hence are the roots of $x^4 + 1$. It follows that the non-trivial automorphisms of $\mathrm{Gal}(K/\mathbb{Q})$ take γ to the elements $\gamma^3, \gamma^5, \gamma^7$, respectively. If we call these automorphisms, σ, τ, δ, we have:

(i) $\sigma(\alpha) = \sigma(\gamma) + \sigma(\gamma)^2 = \gamma^3 + \gamma^6$.

(ii) $\tau(\alpha) = \tau(\gamma) + \tau(\gamma)^2 = \gamma^5 + \gamma^{10} = \gamma^2 + \gamma^5$.

(iii) $\delta(\alpha) = \delta(\gamma) + \delta(\gamma)^2 = \gamma^7 + \gamma^{14} = \gamma^6 + \gamma^7$.

Thus, the roots of $p(x)$ are $\gamma, \gamma^3 + \gamma^6, \gamma^2 + \gamma^5, \gamma^6 + \gamma^7$.

6. Let K denote the splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$. Find (with proof) $\mathrm{Gal}(K/\mathbb{Q})$ and then use the Galois correspondence theorem to find (with proof) all intermediate fields between $\mathbb{Q}$ and K. Hints: (i) The Galois group in question will be abelian. It may be more convenient to write this group multiplicatively, rather than additively. (ii) If A, B are abelian groups, there may be more subgroups of $A \times B$ than just subgroups of the form $H \times K$, where H is a subgroup of A and K is a subgroup of B.

Solution. Note that $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. From the lecture of April 24 we have $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 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 $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. 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 the April 24 lecture. Now, if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{3}) = \pm\sqrt{3}, \sigma(\sqrt{5}) = \pm\sqrt{(5)}$. There are eight possible such automorphisms and they all exist. For example, to see that there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ 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 the lecture of April 14. Now the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is $x^2 - 5$. Thus, by the crucial proposition from April 14 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 on April 14 and to apply the crucial proposition from April 14 to extend each of these to K by sending $\sqrt{5}$ to $\sqrt{5}$ or $\sqrt{5}$ to $-\sqrt{5}$.

We can easily identify $\mathrm{Gal}(K/\mathbb{Q})$ 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 $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ 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 $\mathrm{Gal}(K/\mathbb{Q})$ with the triples above, and writes out the two groups tables, one can see the required isomorphism of groups.

As for the subgroups of $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, 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. [1] 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 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathrm{Gal}(K/\mathbb{Q})$. 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

[1] For what it's worth: 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 $I_2 \subseteq R_2$.

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 $\mathrm{Gal}(K/\mathbb{Q})$ 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 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathrm{Gal}(K/\mathbb{Q})$, 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 $\sigma_2, \sigma_3, \sigma_4$ in G be the automorphisms satisfying: $\sigma_2(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{3}) = -\sqrt{3}$; $\sigma_3(\sqrt{2}) = -\sqrt{2}$ and $\sigma_3(\sqrt{3}) = \sqrt{3}$; $\sigma_4(\sqrt{2}) = -\sqrt{2}$ and $\sigma_4(\sqrt{3}) = -\sqrt{3}$ and set $H_2 := \langle\sigma_2\rangle$, $H_3 := \langle\sigma_3\rangle$, $H_4 := \langle\sigma_4\rangle$ to be the corresponding subgroups, then $K_2 := H_2 \times \mathbb{Z}_2, K_3 := H_3 \times \mathbb{Z}_2, K_4 := H_4 \times \mathbb{Z}_2$ 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. Set $F := \mathbb{Q}(i)$ and $K = F(\sqrt[8]{2})$. Show that K is Galois over F with $\mathrm{Gal}(K/F) \cong \mathbb{Z}_8$ and find (with proof) all intermediate fields between F and K. Hint: Show that K contains a primitive 8th root of unity.

Solution. Set $\epsilon := e^{\frac{2\pi i}{8}}$, a primitive 8th root of unity, and $\gamma := \sqrt[8]{2}$, a real 8th root of 2. Note that $\gamma^2 = \sqrt[4]{2}$ and $\gamma^4 = \sqrt{2}$. Note also that $\epsilon = \frac{\gamma^4}{2} + i\frac{\gamma^4}{2} \in K$. Now $K = F(\gamma)$ is the splitting field for $f(x) := x^8 - 2$ over F, since the roots of $f(x)$ are $\gamma\epsilon^i$, with $0 \le i \le 7$. Thus, K is Galois over F. Now, $[K : \mathbb{Q}] = [\mathbb{Q}(i,\gamma) : \mathbb{Q}] = 16$, since $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 8$ and $i \notin \mathbb{Q}(\gamma)$. It follows that $[K : F] = 8$ and $f(x)$ is irreducible over F. Therefore, $|\mathrm{Gal}(K/F)| = 8$.

We now let $\sigma : K \to K$ be the automorphism of K fixing F satisfying $\sigma(\gamma) = \epsilon^5\gamma$. Then

$$\sigma(\epsilon) = \frac{\sigma(\gamma^4)}{2} + \frac{\sigma(\gamma^4)}{2} = \frac{\sigma(\gamma)^4}{2} + i\frac{\sigma(\gamma)^4}{2} = \frac{\epsilon^{20}\gamma^4}{2} + i\frac{\epsilon^{20}\gamma^4}{2} = \epsilon^4 \cdot \{\frac{\gamma^4}{2} + i\frac{\gamma^4}{2}\} = \epsilon^5.$$

From the equations $\sigma(\gamma) = \epsilon^5\gamma$ and $\sigma(\epsilon) = \epsilon^5$, we readily obtain

$$\begin{aligned} \sigma^2(\gamma) &= \epsilon^6\gamma \\ \sigma^3(\gamma) &= \epsilon^3\gamma \\ \sigma^4(\gamma) &= \epsilon^4\gamma \\ \sigma^5(\gamma) &= \epsilon\gamma \\ \sigma^6(\gamma) &= \epsilon^2\gamma \\ \sigma^7(\gamma) &= \epsilon^7\gamma \\ \sigma^8(\gamma) &= \gamma. \end{aligned}$$

This shows that σ has order eight as an element of $\mathrm{Gal}(K/\mathbb{Q})$, which gives $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_8$. Thus, $\langle\sigma^4\rangle$ and $\langle\sigma^2\rangle$ are the only proper subgroups of $\mathrm{Gal}(K/\mathbb{Q})$. Again, the equations $\sigma(\gamma) = \epsilon^5\gamma$ and $\sigma(\epsilon) = \epsilon^5$ yield $\sigma^2(\gamma^4) = \gamma^4 = \sqrt{2}$. Moreover, since $[\mathrm{Gal}(K/F) : \langle\sigma^2\rangle] = 2$, we have $[K^{\sigma^2} : F] = 2$. It follows that $K^{\sigma^2} = F(\sqrt{2})$. Similarly, $\sigma^4(\gamma^2) = \gamma^2 = \sqrt[4]{2}$. And, so, in similar fashion, $K^{\sigma^4} = F(\sqrt[4]{2})$. Thus, the diagram of intermediate fields between F and K is:

$$F \subsetneq F(\sqrt{2}) \subsetneq F(\sqrt[4]{2}) \subsetneq K.$$

8. Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$. Use Zorn's lemma to prove that there exists a subfield F of $\overline{\mathbb{Q}}$ maximal with respect to the property of **not** containing $\sqrt{2}$. Then show that $[K : F]$ is even for every finite extension of fields $F \subseteq K$.

Solution. Let S denote the subfields of $\overline{\mathbb{Q}}$ containing $\mathbb{Q}$, but not containing $\sqrt{2}$. If $\{E_\alpha\}_{\alpha\in A}$ is a chain in S, then, as we have seen before, $L := \bigcup_{\alpha\in A} E_\alpha$ is a field, certainly contained in $\overline{\mathbb{Q}}$ and it clearly does not contain $\sqrt{2}$. Thus, L is an upper bound for the chain in S. Therefore, S has a maximal element, F. Now, if K is a finite extension of F, then $\sqrt{2} \in K$, and thus $F \subsetneq F(\sqrt{2}) \subseteq K$. Since $[F(\sqrt{2}) : F] = 2$, using the multiplicative property of the degree symbol, it follows that $[K : F]$ is even.

9. Suppose $F \subseteq K$ is a finite extension and K is the splitting field of $p(x) \in F[x]$ over F. Follow the ideas from the Lecture 36 in class to show that if $f(x) \in F[x]$ is irreducible and has a root in K, then it splits over K. The key idea is to show that if $\tau : K \to \overline{F}$ is a field isomorphism fixing F, then $\tau(K) = K$. Here we do not assume that $p(x)$ is irreducible.

Solution. Suppose $p(x)$ has degree d and $p(x) = (x - \alpha_1)\cdots(x - \alpha_d)$, with each $\alpha_j \in K$, not necessarily distinct. Thus, $K = F(\alpha_1, \ldots, \alpha_d)$. Suppose $\tau : K \to \overline{F}$ is a field isomorphism fixing F. Then $\{\alpha_1, \ldots, \alpha_d\} = \{\tau(\alpha_1), \ldots, \tau(\alpha_d)\}$, since τ permutes the roots of $p(x)$. Since τ fixes F, we have $\tau(K) = F(\tau(\alpha_1), \ldots, \tau(\alpha_d)) = K$.

Now let $f(x) \in F[x]$ be irreducible and have a root $\gamma \in K$. Let $\beta \in \overline{F}$ be any other root of $f(x)$. Then there exists an isomorphism $\sigma : F(\gamma) \to F(\beta)$ fixing F such that $\sigma(\gamma) = \beta$ (by the crucial proposition of April 14). Now, $K = F(\gamma)(\alpha_1, \ldots, \alpha_d)$ is the splitting field of $p(x)$ over $F(\beta)$. By the first application of the crucial proposition (see the April 19 Daily Update), we may extend σ to a field isomorphism $\hat{\sigma} : K \to \hat{\sigma}(K)$. By the first paragraph above, $\hat{\sigma}(K) = K$. Since $\hat{\sigma}(\gamma) = \beta$, we have $\beta \in K$. Since β was arbitrary, K contains all of the roots of $f(x)$, and thus $f(x)$ splits over K.

10. Consider $f(x) = x^3 - 4x + 2$.

(i) Show that $f(x)$ is irreducible over $\mathbb{Q}$.

(ii) Prove that $f(x)$ has three real roots. (Hint: Use calculus!)

(iii) Let ϵ be a primitive 3rd root of unity and set $\alpha := \sqrt[3]{\frac{\sqrt{111}i}{9} - 1}$. Show that the three roots of $f(x)$ are:

$$\alpha + \frac{4}{3\alpha}, \qquad \alpha\epsilon + \frac{4}{3\alpha\epsilon}, \qquad \text{and} \qquad \alpha\epsilon^2 + \frac{4}{3\alpha\epsilon^2}.$$

Comment. Recall that any degree three polynomial with coefficient in $\mathbb{Q}$ is solvable by radicals, which means that its roots, or equivalently, its splitting field, can be obtained by adjoining sequences of square roots, cube roots of elements to $\mathbb{Q}$ that are already obtained from elements of $\mathbb{Q}$ by taking a sequence of roots of elements from $\mathbb{Q}$, etc, as is the case for the roots of $f(x)$ above.[2] This problem is an illustration of the classical result known as *Casus irreducibilis* states that no irreducible cubic polynomial in $\mathbb{Q}[x]$ has its splitting field contained in a *real radical extension*. In other words, even though the roots of $f(x)$ are real numbers, that can be extracted by taking sequences of square roots and cube roots, this process of root taking cannot be done entirely within the real number system.

Solution. For (i), that $f(x)$ is irreducible over $\mathbb{Q}$ follows from Gauss's Lemma and Eisenstein's criterion.

[2] The formal definition is as follows: $f(x) \in F[x]$ is *solvable by radicals* if its splitting field is contained in an extension of the form $F(\alpha_1, \ldots, \alpha_r)$, where for each $1 \le i \le r$, $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$, for some $n_i \ge 1$.

The famous theorem of Galois concerning solvability by radicals asserts: Let $f(x) \in F[x]$ and write K for the splitting field of $f(x)$ over F. Then $f(x)$ is solvable by radicals if and only if $\mathrm{Gal}(K/F)$ is a solvable group.

Part (ii) is essentially a calculus problem. $f(x)$ has two critical points, one a minimum below the x-axis, and the other a maximum, above the x-axis. This together with the fact that $f(x)$ is a polynomial of degree 3 insures that the graph of $f(x)$ crosses the x-axis exactly three times.

For (iii), we re-write and label the given elements as

$$r_1 := \alpha + \frac{4}{3\alpha}, \qquad r_2 := \alpha\epsilon + \frac{4\epsilon^2}{3\alpha}, \qquad \text{and} \qquad r_3 := \alpha\epsilon^2 + \frac{4\epsilon}{3\alpha}.$$

We now compute the elementary symmetric expressions in r_1, r_2, r_3.

$$\begin{aligned} r_1 + r_2 + r_3 &= \alpha + \frac{4}{3\alpha} + \alpha\epsilon + \frac{4\epsilon^2}{3\alpha} + \alpha\epsilon^2 + \frac{4\epsilon}{3\alpha} \\ &= (\alpha + \alpha\epsilon + \alpha\epsilon^2) + (\frac{4}{3\alpha} + \frac{4\epsilon^2}{3\alpha} + \frac{4\epsilon}{3\alpha}) \\ &= \alpha(1 + \epsilon + \epsilon^2) + \frac{4}{3\alpha}(1 + \epsilon + \epsilon^2) \\ &= 0 + 0 = 0. \end{aligned}$$

$$\begin{aligned} r_1 r_2 &= (\alpha + \frac{4}{3\alpha})(\alpha\epsilon + \frac{4\epsilon^2}{3\alpha}) = \alpha^2\epsilon + \frac{4}{3}(\epsilon + \epsilon^2) + \frac{16}{9\alpha^2}\epsilon^2 \\ r_1 r_3 &= (\alpha + \frac{4}{3\alpha})(\alpha\epsilon^2 + \frac{4\epsilon}{3\alpha}) = \alpha^2\epsilon^2 + \frac{4}{3}(\epsilon^2 + \epsilon) + \frac{16}{9\alpha^2}\epsilon \\ r_2 r_3 &= (\alpha\epsilon + \frac{4\epsilon^2}{3\alpha})(\alpha\epsilon^2 + \frac{4\epsilon}{3\alpha}) = \alpha^2 + \frac{4}{3}(\epsilon^2 + \epsilon) + \frac{16}{9\alpha^2} \end{aligned}$$

Thus, using $1 + \epsilon + \epsilon^2 = 0$, and simplifying, we have $r_1 r_2 + r_1 r_3 + r_2 r_3 = -\frac{4}{3} - \frac{4}{3} - \frac{4}{3} = -4$.

$$\begin{aligned} r_1 r_2 r_3 &= (\alpha + \frac{4}{3\alpha})(\alpha\epsilon + \frac{4\epsilon^2}{3\alpha})(\alpha\epsilon^2 + \frac{4\epsilon}{3\alpha}) \\ &= (\alpha^2\epsilon + \frac{4}{3}(\epsilon + \epsilon^2) + \frac{16}{9}\epsilon^2)(\alpha\epsilon^2 + \frac{4\epsilon}{3\alpha}) \\ &= \alpha^3 + \frac{4}{3}(1 + \epsilon)\alpha + \frac{16}{9\alpha}\epsilon + \frac{4}{3}\epsilon^2\alpha + \frac{16}{9\alpha}(1 + \epsilon^2) + \frac{64}{27\alpha^3} \\ &= \alpha^3 + \frac{64}{27\alpha^3} \\ &= \frac{\sqrt{111}i}{9} - 1 + \frac{64}{27(\frac{\sqrt{111}i}{9} - 1)} \\ &= \frac{\sqrt{111}i}{9} - 1 + \frac{64(\frac{\sqrt{111}i}{9} + 1)}{27(\frac{-111}{81} - 1)} \\ &= \frac{\sqrt{111}i}{9} - 1 - (\frac{\sqrt{111}i}{9} + 1) \\ &= -2. \end{aligned}$$

This gives $f(x) = (x - r_1)(x - r_2)(x - r_3)$, which shows that r_1, r_2, r_3 are the roots of $f(x)$. □