Problem 1. (20 points) Compute the degree of the splitting field of each of the following polynomials over \( \mathbb{Q} \). Explain briefly why your answer is correct.

(a) \( x^3 - 17 \)
(b) \( x^4 - 1 \)
(c) \( x^4 + 1 \)
(d) \( x^9 - 8 \)

Solution.

(a) This polynomial is irreducible by Eisenstein, so adjoining one root gives a degree 3 extension. But then to get the other roots we need a cube root of 1, so the splitting field contains \( \sqrt[3]{-3} \), so has degree divisible by 2. Hence the degree of the splitting field is \( 6 \).

(b) This polynomial factors as
\[
x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i),
\]
so the splitting field is \( \mathbb{Q}(i) \), which has degree \( 2 \).

(c) A root \( \zeta \) of \( x^4 + 1 \) is a primitive 8'th root of unity, so the splitting field \( \mathbb{Q}(\zeta) \) is a cyclotomic field. It's the splitting field of \( x^8 - 1 = (x^4 + 1)(x^4 - 1) \). We proved in class that the degree of this field is equal to \( \phi(8) = \#\{0 \leq a < 8 : \gcd(a, 8) = 1\} \). Alternatively, the map \( \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/8\mathbb{Z})^* \) is an isomorphism. Hence the degree is \( 4 \).

(d) The splitting field is generated by \( 3\sqrt{2} \) and a primitive 9'th root of unity \( \zeta \). This gives a tower of fields
\[
\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(3\sqrt{2}),
\]
where the bottom extension is a cyclotomic extension of degree 6 and the top extension is a Kummer extension of degree 3, so the total degree is \( 18 \). Note that if instead it had been \( x^9 - 10 \), say, then the Kummer extension would have degree 9, so the total degree would have been 54, not 18.

Problem 2. (10 points)

(a) Let \( K/F \) be a separable field extension with \( [K : F] = 2 \). Prove that \( K/F \) is Galois.

(b) Give an example of fields \( F \subset K \subset L \) with the property that \( K/F \) is Galois and \( L/K \) is Galois, but \( L/F \) is not Galois. Be sure to explain why.

Solution. (a) We know that \( K = F(\alpha) \) for some \( \alpha \) by the primitive element theorem. Further \( \alpha \) is the root of a (monic) quadratic polynomial since \( [F(\alpha) : F] = 2 \). Say \( \alpha \) is a root of \( x^2 + bx + c \) with \( b, c \in F \).
Let $\beta$ be the other root. Then $\alpha + \beta = -a$, so $\beta = a + \alpha \in F(\alpha)$. Hence $F(\alpha)$ is the splitting field of the polynomial $x^2 + bx + c$, so it is Galois over $F$. (If $F$ doesn’t have characteristic 2, then another way to see that both roots are in $F(\alpha)$ is to use the quadratic formula $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$.)

(b) Take $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt[4]{2})$. Then $K/F$ has degree 2 and $L/F$ has degree 2, so from (a) we know that both $K/F$ and $L/K$ are Galois. On the other hand, note that $L$ contains one of the roots of $x^4 - 2$, namely $\sqrt[4]{2}$, but it doesn’t contain all of the roots, since it doesn’t contain $i\sqrt[4]{2}$. (If it did, then $L$ would contain $i$, which it can’t, since $L$ is a subfield of $\mathbb{R}$.) We proved in class that if a Galois extension contains one root of an irreducible polynomial, then it contains all the roots. This proves that $L/F$ is not Galois.

Another proof, which is similar, is to note that we have a homomorphism

$$L = \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{C}$$

that sends $\sqrt[4]{2}$ to $i\sqrt[4]{2}$. Since the image is not equal to $L$ (since $L \subset \mathbb{R}$), therefore $L$ is not Galois over $F$.

**Problem 3.** (10 points) Let $F = \mathbb{Q}$ and let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Write down all of the intermediate fields, that is, all fields $E$ with $F \subseteq E \subseteq K$, and indicate how they match up with subgroups of the Galois group of $K/F$.

**Solution.** The Galois group $G = \text{Gal}(K/F)$ is a product of three cyclic groups of order 2, generated by the three elements $\sigma, \tau, \lambda$ with the property that

$$\sigma(\sqrt{2}) = -\sqrt{2} \quad \text{and} \quad \sigma \text{ fixes } \sqrt{3} \text{ and } \sqrt{5},$$
$$\tau(\sqrt{3}) = -\sqrt{3} \quad \text{and} \quad \tau \text{ fixes } \sqrt{2} \text{ and } \sqrt{5},$$
$$\lambda(\sqrt{5}) = -\sqrt{5} \quad \text{and} \quad \lambda \text{ fixes } \sqrt{2} \text{ and } \sqrt{3}.$$  

It’s then easy to what products of elements do. For example

$$\sigma \tau(\sqrt{2}) = -\sqrt{2}, \quad \sigma \tau(\sqrt{3}) = -\sqrt{3}, \quad \sigma \tau(\sqrt{5}) = \sqrt{5},$$

so $\sigma \tau$ fixes $\sqrt{6}$ (and $\sqrt{5}$). Similarly for the other products, thus

$$\sigma \tau \text{ fixes } \sqrt{5} \text{ and } \sqrt{6}$$
$$\sigma \lambda \text{ fixes } \sqrt{3} \text{ and } \sqrt{10}$$
$$\tau \lambda \text{ fixes } \sqrt{2} \text{ and } \sqrt{15}$$
$$\sigma \tau \lambda \text{ fixes } \sqrt{6} \text{ and } \sqrt{10} \quad \text{(so also } \sqrt{15})$$
Each non-trivial element generates a subgroup of order 2, so there are 7 such subgroups
\{ e, \sigma \}, \{ e, \tau \}, \{ e, \lambda \}, \{ e, \sigma \tau \}, \{ e, \sigma \lambda \}, \{ e, \tau \lambda \}, \{ e, \sigma \tau \lambda \}.

Similarly, each pair of non-trivial elements generates a subgroup of order 4, and there are 7 such subgroups,
\{ e, \sigma, \tau, \sigma \tau \}, \{ e, \sigma, \lambda, \sigma \lambda \}, \{ e, \tau, \lambda, \tau \lambda \},
\{ e, \sigma \tau, \lambda, \sigma \tau \lambda \}, \{ e, \sigma \lambda, \tau, \sigma \tau \lambda \}, \{ e, \tau \lambda, \sigma, \sigma \tau \lambda \}, \{ e, \sigma, \lambda, \tau \lambda \}.

The fixed fields are easy enough to compute based on the actions of \( \sigma, \tau, \lambda \) and their products. So we have
\[ K^{(e)} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), \]
\[ K^{(e, \sigma)} = \mathbb{Q}(\sqrt{3}, \sqrt{5}), \]
\[ K^{(e, \tau)} = \mathbb{Q}(\sqrt{2}, \sqrt{5}), \]
\[ K^{(e, \lambda)} = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \]
\[ K^{(e, \sigma \tau)} = \mathbb{Q}(\sqrt{5}, \sqrt{6}), \]
\[ K^{(e, \sigma \lambda)} = \mathbb{Q}(\sqrt{5}, \sqrt{10}), \]
\[ K^{(e, \tau \lambda)} = \mathbb{Q}(\sqrt{2}, \sqrt{15}), \]
\[ K^{(e, \sigma \tau \lambda)} = \mathbb{Q}(\sqrt{6}, \sqrt{10}), \]
\[ K^{(e, \sigma, \tau, \sigma \tau)} = \mathbb{Q}(\sqrt{5}), \]
\[ K^{(e, \sigma, \lambda, \sigma \lambda)} = \mathbb{Q}(\sqrt{3}), \]
\[ K^{(e, \tau, \lambda, \tau \lambda)} = \mathbb{Q}(\sqrt{2}), \]
\[ K^{(e, \sigma \tau, \lambda, \sigma \tau \lambda)} = \mathbb{Q}(\sqrt{6}), \]
\[ K^{(e, \sigma \lambda, \tau, \sigma \tau \lambda)} = \mathbb{Q}(\sqrt{10}), \]
\[ K^{(e, \tau \lambda, \sigma, \sigma \tau \lambda)} = \mathbb{Q}(\sqrt{15}), \]
\[ K^{(e, \sigma \tau, \lambda, \tau \lambda)} = \mathbb{Q}(\sqrt{30}), \]
\[ K^G = \mathbb{Q}. \]

(These can be organized into a much nicer picture, of course, where each quadratic extension is contained in two of the degree 4 extensions; but that requires a \LaTeX\ package that I’ve never learned to use.)

**Problem 4.** (10 points)

(a) Express \( x^3 + y^3 \) as a polynomial of the elementary symmetric polynomials \( s_1 = x + y \) and \( s_2 = xy. \)
(b) Write down the elementary symmetric polynomials of the three variables \(x, y, \) and \(z\).

(c) Express \(x^3 + y^3 + z^3\) as a polynomial of the elementary symmetric polynomials of three variables. (This part is a bit messy. I'd suggest leaving it until you’ve finished working on the rest of the exam.)

Solution. (a) We have \(s_1 = x + y\) and \(s_2 = xy\). To get \(x^3 + y^3\), we need to cube \(s_1\), so

\[
s_1^3 = (x + y)^3
\]

\[
= x^3 + 3x^2y + 3xy^2 + y^3
\]

\[
= (x^3 + y^3) + (3x^2y + 3xy^2)
\]

\[
= (x^3 + y^3) + 3xy(x + y)
\]

\[
= (x^3 + y^3) + 3s_2 s_1.
\]

So

\[
x^3 + y^3 = s_1^3 - 3s_1 s_2.
\]

(b) The elementary symmetric polynomials of three variables are

\[
s_1 = x + y + z,
\]

\[
s_2 = xy + xz + yz,
\]

\[
s_3 = xyz.
\]

(c) We again start by cubing \(s_1\) in order to get \(x^3 + y^3 + z^3\) (plus some extra stuff that we’ll need to get rid of). We group the terms according to whether they look like \(a^3\) or like \(ab^2\) with \(a \neq b\) or like \(abc\) with \(a, b, c\) distinct. This gives

\[
s_1^3 = (x + y + z)^3
\]

\[
= (x^3 + y^3 + z^3) + (3x^2y + 3x^2z + 3y^2x + 3y^2z + 3z^2x + 3z^2y) + 6xyz
\]

\[
= (x^3 + y^3 + z^3) + (3x^2y + 3x^2z + 3y^2x + 3y^2z + 3z^2x + 3z^2y) + 6s_3
\]

\[
= (x^3 + y^3 + z^3) + 3 \cdot \text{(Stuff)} + 6s_3.
\]

To figure out the “Stuff”, we multiply \(s_1\) and \(s_2\) to get

\[
s_1 s_2 = (xy + xz + yz)(x + y + z)
\]

\[
= x^2 y + x^2 z + y^2 x + y^2 z + z^2 x + z^2 y + 3xyz
\]

\[
= x^2 y + x^2 z + y^2 x + y^2 z + z^2 x + z^2 y + 3s_3
\]

\[
= \text{(Same Stuff)} + 3s_3.
\]
So putting it all together, we find that
\[ x^3 + y^3 + z^3 = s_1^3 - 6s_3 - 3 \cdot \text{(Stuff)} \]
\[ = s_1^3 - 6s_3 - 3(s_1s_2 - 3s_3) \]
\[ = s_1^3 - 3s_1s_2 + 3s_3 \]