(1) [2 pts] What does it mean for an algebraic field extension $L/K$ to be normal?

$$\forall \alpha \in L, \quad \alpha \text{ splits over } L \uparrow \text{min polynomial } / K$$

(b) [2 pts] What is the splitting field of $x^4 - 2$ over $\mathbb{Q}$? Identify explicitly a non-normal subfield.

$$\mathbb{Q}(i, \sqrt[4]{2})$$

$$\mathbb{Q}(\sqrt[4]{2}) \quad \text{[since this is the fixed field of a } \mathbb{Z}_2 \leq D_4, \text{ which is not a normal subgroup]}$$

(c) [3 pts] What is the Galois group? Define “soluble” (for finite groups), and explicitly demonstrate its solubility.

$$D_4 = \langle r, h \mid h^4 = e, r^4 = e, r^2 = h \rangle$$

$$G \text{ soluble } \iff \exists S_{\text{pgps.}}, \{1 \leq G_n \leq G_{n-1} \leq \cdots \leq G_1 = G \text{ s.t. } G_i \text{ abelian quotient of } G_i \}$$

$$1 \leq \mathbb{Z}_4 \leq \langle r \rangle \leq D_4 \text{ quotient of } \mathbb{Z}_2$$

(2) [3 pts] The polynomials $P(x) = x^3 + x + 1$ and $Q(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{Z}_2$. Let $K$ (resp. $K'$) be a field obtained from $\mathbb{Z}_2$ by adjoining a root of $P$ (resp. $Q$). Describe explicitly an isomorphism from $K$ to $K'$.

$$K \cong \frac{\mathbb{Z}_2[x]}{(P(x))} \quad \xrightarrow{\cong} \quad \frac{\mathbb{Z}_2[x]}{(Q(x))} \quad \xrightarrow{\text{check well-deft}} \quad P(x) \mapsto P(x+1) = (x+1)^3 + (x+1) + 1 = x^3 + x^2 + x + 1 \cong Q(x).$$
(3) [6 pts] Compute the Galois group of \( f(x) := x^3 + 4x + 1 \) over \( \mathbb{Q} \), over \( \mathbb{Z}_7 \), and over \( \mathbb{Z}_5 \).

By formula a la care, \( \Delta = -4(4)^3 - 27(1)^2 = -283 \) is prime.

\[ \mathbb{Q} : \quad f'(x) > 0, \quad f(-1) < 0 < f(0) \quad \text{\& Gross's lemma} \Rightarrow \text{no roots in } \mathbb{Q} \quad \Rightarrow \text{irred. over } \mathbb{Q} \]

\[ \Delta \neq \text{square} \]
\[ \Rightarrow G \cong S_3 \]

\[ \mathbb{Z}_7 : \quad \text{no roots} \Rightarrow \text{irred.} \]
\[ \Delta = -283 \equiv -3 \equiv 4 \equiv 2 \pmod{7} \]
\[ \Rightarrow G \cong \mathbb{Z}_3 \]

\[ \mathbb{Z}_5 : \quad 3 \equiv -2 \equiv 3 \pmod{5} \text{ is a root (only one)}, \quad f \equiv (x+2)(x^2-2x+3) \]
\[ \Rightarrow G \cong \mathbb{Z}_2 \]

(4) [4 pts] Let \( f \) be an irreducible cubic polynomial over \( K \) with \( \text{char}(K) \neq 2 \), and let \( \delta \) be a square root of the discriminant of \( f \). Show that \( f \) remains irreducible over \( K(\delta) \).

\( L := \text{SFE for } f/K \) contains \( \delta \), hence also \( K(\delta) \). Suppose \( f \) reducible over \( K(\delta) \). Then we have

\[ L \]
\[ \begin{array}{c}
\leftrightarrow 2 \times 1 \\
(3 \times 6)
\end{array} \]

\[ K \]

which is clearly impossible by the tower law.
(5) (a) [8 pts] Use the Galois correspondence to find all subfields of \( \mathbb{Q}(\zeta_7) \), and express them in the form \( \mathbb{Q}(\alpha) \). Which are Galois over \( \mathbb{Q} \)?

\[
\text{Aut}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3
\]

\[
\{\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6\} = \text{basis of } \mathbb{Q}(\zeta_7)/\mathbb{Q}
\]

Basis of fixed field of \( \mathbb{Q}_2 \): \( \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6 \)

\( \Rightarrow \) fixed field is \( \mathbb{Q}(\zeta_7) \)

Basis of fixed field of \( \mathbb{Q}_2 \): \( \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6 \)

\( \Rightarrow \) fixed field is \( \mathbb{Q}(\beta) \)

\( \mathbb{Z}_7^* \) abelian \( \Rightarrow \) all subfields normal

\( \Rightarrow \) all subfields of \( \mathbb{Q}(\zeta_7) \) normal over \( \mathbb{Q} \)

\( \Rightarrow \) all subfields of \( \mathbb{Q}(\zeta_7) \) Galois over \( \mathbb{Q} \)

(b) [2 pts] Using a criterion from class, show that a regular 7-gon is not constructible with straightedge and compass.

\[
[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6 \quad \text{which is not of the form } 2^e.
\]
(6) (a) [5 pts] Let $K$ be a finite field, of order $q = p^m$. Show that $K$ is a splitting field for $x^q - x$.

\[ K^* \text{ gen., } \left| K^* \right| = q - 1 \Rightarrow x^q - x = 1 \\forall x \in K \]

\[ \Rightarrow \alpha^2 - \alpha = 0 \\forall \alpha \in K. \]

Repeatedly applying div. algorithm gives

\[ x^q - x = \prod_{\alpha \in K} (x - \alpha) \]

so that $x^q - x$ splits over $K$ and $K$ is generated by its roots.

\[ \Rightarrow K \text{ is SFE}. \]

(b) [5 pts] Let $f \in K[x]$ be irreducible of degree $n > 1$. Use (a) to give a direct proof that $f$ is separable. [Hint: given one root, what are the others?]

Let $L$ be an SFE over $K$ for $f$, $\sigma = p^m$ the $(p^m = q^k)$ power Frobenius map $\in \text{Aut}(L/K)$.

Since $x^q - x$ cannot have $q$ distinct roots, and the $q$ elements of $K$ are all roots, $K$ is precisely the fixed field of $\sigma$.

Now let $\alpha \in L$ be a root of $f$, and suppose $\sigma^k(\alpha) = \alpha$.

Then $\alpha$ is in the fixed field of $\sigma^k$, which has order $\leq p^mk = \left| K \right|^k$

hence degree $\leq k/K$. Since $m \in K[x]$ has degree $n$,

\[ \left[ K(\alpha) : K \right] = n \text{ and so } k \geq n. \]

Hence the $\{ \alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha) \}$ are distinct, and by the fresherman's dream are also roots of $f$.

\[ \Rightarrow f \text{ has no repeated roots}. \]