Problem 1. Consider the field extension
\[ \mathbb{Q}(\zeta) = \mathbb{Q}[x]/(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1). \]

note that \( \zeta^7 = 1 \) but \( \zeta \neq 1 \), so \( \mathbb{Q}(\zeta) \) is the result of adjoining a primitive 7th root of unity to \( \mathbb{Q} \). By assigning \( \zeta \) the complex value \( e^{2\pi i/7} = \cos \left( \frac{2\pi}{7} \right) + i \sin \left( \frac{2\pi}{7} \right) \), we observe that the points \( \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\} \) are the vertices of a regular heptagon (7-sided polygon) inscribed in the unit circle:

Since \( \zeta^6 = \cos \left( \frac{2\pi}{7} \right) - i \sin \left( \frac{2\pi}{7} \right) \), it follows that \( 2 \cos \left( \frac{2\pi}{7} \right) = \zeta + \zeta^6 \). We will find an irreducible cubic polynomial \( f(x) \) with coefficients in \( \mathbb{Q} \) that has \( 2 \cos \left( \frac{2\pi}{7} \right) \) as a root.

(a) Every element of \( \mathbb{Q}(\zeta) \) can be written in the form
\[ a_0 + a_1 \zeta + a_2 \zeta^2 + a_3 \zeta^3 + a_4 \zeta^4 + a_5 \zeta^5 + a_6 \zeta^6 \]
(though in more than one way!—the form above is just particularly convenient to work with). Express \( (\zeta + \zeta^6)^2 \) and \( (\zeta + \zeta^6)^3 \) in this form. Remember! \( \zeta^7 = 1 \).
(b) Let $v_0 = 1, v_1 = \zeta + \zeta^6, v_2 = (\zeta + \zeta^6)^2$, and $v_3 = (\zeta + \zeta^6)^3$. Consider \{\(v_0, v_1, v_2, v_3\)\} as a set of (abstract) vectors over $\mathbb{Q}$ (with seven components each) and find a linear dependence of the form

$$v_3 + b_2v_2 + b_1v_1 + b_0 = 0$$

where $b_2, b_1, b_0 \in \mathbb{Q}$ (they will actually be in $\mathbb{Z}$).

Remember! $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$.

(c) Conclude that $2 \cos \left(\frac{2\pi}{7} \right)$ is a root of the polynomial $f(x) = x^3 + b_2x^2 + b_1x + b_0$.

You should verify this with a calculator, too!

\[ \text{Solution.} \quad \text{(a) Using the binomial theorem and the fact that } \zeta^7 = 1, \text{ we have} \]

\[
(\zeta + \zeta^6)^2 = \zeta^2 + 2\zeta^7 + \zeta^{12} = 2 + \zeta^2 + \zeta^5, \]

and

\[
(\zeta + \zeta^6)^3 = \zeta^3 + 3\zeta^8 + 3\zeta^{13} + \zeta^{18} = 3\zeta + \zeta^3 + \zeta^4 + 3\zeta^6. \]

(b) We first note that from part (a), $(\zeta + \zeta^6)^2 + (\zeta + \zeta^6)^3$ is $2 + 3\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + 3\zeta^6$. This is almost $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$: we just need to subtract $2(\zeta + \zeta^6)$ and subtract 1. Hence we have

\[
(\zeta + \zeta^6)^3 + (\zeta + \zeta^6)^2 - 2(\zeta + \zeta^6) - 1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0. \]

So $b_0 = -1, b_1 = -2$, and $b_2 = 1$.

(c) From part (c), we know that $\zeta + \zeta^6$ is a root of the polynomial $f(x) = x^3 + x^2 - 2x - 1$. As explained in the problem statement, we also know that $\zeta + \zeta^6 = 2 \cos \left(\frac{2\pi}{7} \right)$. Hence $2 \cos \left(\frac{2\pi}{7} \right)$ is a root of the polynomial $f(x) = x^3 + x^2 - 2x - 1$.

(As an aside, this enables us to compute $\cos \left(\frac{2\pi}{7} \right)$ exactly using radicals: we get

\[
\cos \left(\frac{2\pi}{7} \right) = \frac{1}{6} \left( -1 + \sqrt[3]{\frac{7}{2} \left( 1 + 3i\sqrt{3} \right)} + \sqrt[3]{\frac{7}{2} \left( 1 - 3i\sqrt{3} \right)} \right). \]

You may wonder why $i$ appears in the above expression even though $\cos \left(\frac{2\pi}{7} \right)$ is real. In general, for an irreducible cubic polynomial with integer coefficients that has three real roots, the roots cannot be expressed using real radicals only; this was proved by Pierre Wantzel in 1843.)

\[ \text{Problem 2.} \]

The quadratic polynomials $x^2 + x + 2$ and $x^2 + 3$ are both irreducible over $\mathbb{F}_5$ (one can check this using Legendre symbols!). Let $\mathbb{F}_5(\alpha) = \mathbb{F}_5[x]/(x^2 + x + 2)$ and let $\mathbb{F}_5(\beta) = \mathbb{F}_5[x](x^2 + 3)$.

(a) Find an isomorphism $\iota : \mathbb{F}_5(\alpha) \to \mathbb{F}_5(\beta)$.

\[ \text{Note that since } \iota(1) = 1, \iota(k) = k \text{ for any } k \in \mathbb{F}_5. \text{ Therefore, to define } \iota, \text{ it is enough to specify a correct value for } \iota(\alpha). \text{ Hint: Since } \iota(\alpha^2 + \alpha + 2) = 0, \text{ we must have } \iota(\alpha)^2 + \iota(\alpha) + 2 = 0. \]
(b) Find the inverse of your isomorphism $\iota$ by specifying the value $\iota^{-1}(\beta)$.

**Solution.** (a) From the question, we know that we only need to specify $\iota(\alpha)$ in terms of $\beta$, and that we must have $\iota(\alpha)^2 + \iota(\alpha) + 2 = 0$. We also know that every element in $F_5(\beta)$ is of the form $j + k\beta$ for some $j, k \in F_5$. Hence we need to find $j, k \in F_5$ such that $(j + k\beta)^2 + (j + k\beta) + 2 = 0$ in $F_5(\beta)$. Note that we must have $k \neq 0$, since $x^2 + x + 2$ has no root in $F_5$. Computing, we have

$$(j + k\beta)^2 + (j + k\beta) + 2 = j^2 + 2jk\beta + k^2\beta^2 + j + k\beta + 2 = k^2\beta^2 + (2jk + k)\beta + (j^2 + j + 2).$$

We know that $\beta^2 + 3 = 0$, so $\beta^2 + 2 = 0$, thus

$$k^2(2) + (2jk + k)\beta + (j^2 + j + 2) = (2jk + k)\beta + (j^2 + j + 2k^2 + 2) = 0.$$

We need this to be zero, and we know that $\beta \notin F_5$ since $\beta^2 + 3$ is irreducible over $F_5$, so $1, \beta$ are linearly independent, i.e. this forces

$$2jk + k = 0,$$
$$j^2 + j + 2k^2 + 2 = 0.$$

Looking at the first equation, we have $k(2j + 1) = 0$ in $F_5$. Since $k \neq 0$, we have $2j + 1 = 0$, so $j = 2$. Then the second equation gives

$$4 + 2 + 2k^2 + 2 = 0 \implies 2k^2 + 3 = 0 \implies k^2 = 1 \implies k^2 = 1 \text{ or } 4,$$

from Problem set 1, problem 12. Hence we have two isomorphisms, which we call $\iota_1$ and $\iota_2$, given by

$$\iota_1(\alpha) = \beta + 2, \quad \iota_2(\alpha) = 4\beta + 2.$$

Since we did not make any choices in finding these, this also means that these are the only isomorphisms.

We could streamline the process of finding $\iota$ by noting that $x^2 + x + 2 = (x + 3)^2 + 3$ over $F_5$. This forces $\iota(\alpha) + 3 = \pm \beta$ by Problem Set 1 problem 12, which gives the same isomorphisms as above.

Note: This is in line with what we expect: we have two field extensions of $F_5$ of degree 2, which are isomorphic by Theorem 7.2(ii), and from Theorem 7.6(i), we expect $d = 2$ isomorphisms. (For those interested in the more technical parts of the notes: in particular, the Galois group of the extension is the cyclic group of order 2.)

(b) We need to find the inverses of the above maps, working over $F_5$. For $\iota$, we have

$$\alpha = \iota_1^{-1}(\beta + 2) = \iota_1^{-1}(\beta) + 2 \implies \alpha + 3 = \iota_1^{-1}(\beta).$$
So we have \( i_1^{-1}(\beta) = \alpha + 3 \). Similarly, for \( \iota_2 \), we have

\[
\alpha = \iota_2^{-1}(4\beta + 2) = 4\iota_2^{-1}(\beta) + 2 \\
\implies \alpha + 3 = 4\iota_2^{-1}(\beta) \\
\implies 4\alpha + 2 = \iota_2^{-1}(\beta).
\]

So \( \iota_2^{-1}(\beta) = 4\alpha + 2 \).

**Problem 3.** The sextic \( x^6 + x + 1 \) is irreducible over \( \mathbb{F}_2 \). Let \( \mathbb{F}_2(\gamma) = \mathbb{F}_2[x]/(x^6 + x + 1) \) so that \( \mathbb{F}_2(\gamma) \) is a field of order \( 2^6 \).

(a) Express \( \gamma^{21} \) and \( \gamma^9 \) in the form \( a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + a_4\gamma^4 + a_5\gamma^5 \).

(b) Prove that the field \( \mathbb{F}_2(\gamma^{21}) \) is \( \mathbb{F}_2(\gamma) \)'s subfield of order \( 2^2 \) and that the field \( \mathbb{F}_2(\gamma^9) \) is its subfield of order \( 2^3 \). Hint: Don’t work too hard! For example, for the second of these, it’s enough to show that \( (\gamma^9)^{21} = \gamma^9 \) and that \( \gamma^9 \notin \mathbb{F}_2 \) (explain why this is enough, using theorems above!).

**Solution.** (a) Using the fact that \( \gamma^6 + \gamma + 1 = 0 \), we have \( \gamma^6 = -\gamma - 1 = \gamma + 1 \) over \( \mathbb{F}_2 \). Hence

\[
\gamma^{21} = (\gamma^6)^3\gamma^3 = (\gamma + 1)^3\gamma^3 = (\gamma^3 + \gamma^2 + \gamma^1 + 1)^3\gamma^3 = \gamma^6 + \gamma^5 + \gamma^4 + \gamma^3 = \gamma + 1 + \gamma^5 + \gamma^4 + \gamma^3.
\]

So \( \gamma^{21} = 1 + \gamma + \gamma^3 + \gamma^4 + \gamma^5 \). Similarly,

\[
\gamma^9 = (\gamma + 1)^3 = (\gamma^3 + \gamma^2 + \gamma^1 + 1) = \gamma^6 + \gamma^5 + \gamma^4 + \gamma^3 = \gamma^3 + \gamma^4.
\]

(b) Consider the field \( \mathbb{F}_2(\gamma^{21}) \). We have \( (\gamma^{21})^{22} = 1 \) by Theorem 7.4(i), since \( \mathbb{F}_2(\gamma) \) has order 64. Hence \( (\gamma^{21})^{22} = \gamma^{21} \). Since \( \gamma^{21} \) generates the field \( \mathbb{F}_2(\gamma^{21}) \) over \( \mathbb{F}_2 \), this means that the map \( \text{Frob}^2: a \mapsto a^{22} \) fixes the field \( \mathbb{F}_2(\gamma^{21}) \). By Theorem 7.6(v), this means that \( \mathbb{F}_2(\gamma^{21}) \) has order \( 2^2 \), where \( e|2 \), so it has order \( 2^1 \) or \( 2^2 \). Hence either \( \mathbb{F}_2(\gamma^{21}) \) is the base field \( \mathbb{F}_2 \), or \( \mathbb{F}_2(\gamma^{21}) \) is the subfield of \( \mathbb{F}_2(\gamma) \) of order \( 2^2 \). From part (a), we know that \( \gamma^{21} \notin \mathbb{F}_2 \), so \( \mathbb{F}_2(\gamma^{21}) \) cannot be \( \mathbb{F}_2 \). Hence \( \mathbb{F}_2(\gamma^{21}) \) is the subfield of \( \mathbb{F}_2(\gamma) \) of order \( 2^2 \).

Similarly for the field \( \mathbb{F}_2(\gamma^9) \): we have \( (\gamma^9)^{23} = 1 \), so \( (\gamma^9)^{23} = \gamma \) and therefore the map \( \text{Frob}^3: a \mapsto a^{23} \) fixes \( \mathbb{F}_2(\gamma^9) \). As above, by Theorem 7.6(v), this means that either \( \mathbb{F}_2(\gamma^9) \) is the base field \( \mathbb{F}_2 \), or it is the subfield of \( \mathbb{F}_2(\gamma) \) of order \( 2^3 \). From part (a), we know that \( \gamma^9 \notin \mathbb{F}_2 \), so \( \mathbb{F}_2(\gamma^9) \) cannot be \( \mathbb{F}_2 \). Hence \( \mathbb{F}_2(\gamma^9) \) is the subfield of \( \mathbb{F}_2(\gamma) \) of order \( 2^3 \).