Solutions to the Exam

December, 2025

1. (a) $(x^2+x+1)(x^2-x+1)$
   (b) $(x^2+x+1)(x^2-x+1)$
   (c) $(x-\omega)(x+\omega)(x-\omega^2)(x+\omega^2)$ where $\omega = e^{2\pi i/3} = \frac{1}{2}\big(-1+\sqrt{-3}\big)$
   (d) $(x-2)(x+2)(x-3)(x+3)$

2. The extension $F = \mathbb{Q}[\alpha] \supset \mathbb{Q}$ is the splitting field of $f(x)$: it is a Galois extension containing all four roots of $m(x)$, namely

$$\begin{aligned}
\alpha_1 &= i+\sqrt{2} &&= \alpha \in F,\\
\alpha_2 &= i-\sqrt{2} &&= \tfrac{1}{3}(\alpha^3-2\alpha) \in F,\\
\alpha_3 &= -i+\sqrt{2} &&= -\tfrac{1}{3}(\alpha^3-2\alpha) \in F,\\
\alpha_4 &= -i-\sqrt{2} &&= -\alpha \in F.
\end{aligned}$$

   (a) $[F:\mathbb{Q}] = 4$, the degree of $f(x)$.
   (b) $\{1, \alpha, \alpha^2, \alpha^3\}$. In place of the powers of α, you can substitute the corresponding powers of α_i for any of the four roots α_i. Or you can take $\{1, i, \sqrt{2}, \sqrt{-2}\}$ as a basis. But clearly you cannot use $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ since these are linearly dependent.
   (c) Divide $\alpha^4 - 2\alpha^2 + 9 = 0$ by α to obtain $\alpha^{-1} = \frac{1}{9}\big(2\alpha^2 - \alpha^4\big)$.
   (d) See above.
   (e) F has exactly five subfields: $\mathbb{Q}$, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{-2}]$, F. These correspond to the five subgroups of G, which are G, $\langle\tau\rangle$, $\langle\sigma\rangle$, $\langle\sigma\tau\rangle$, $\langle\iota\rangle$ respectively; see (f).
   (f) F has four automorphisms; $G = \operatorname{Aut} F = \{\iota, \sigma, \tau, \sigma\tau\}$ where

$$\begin{aligned}
\iota(a+bi+c\sqrt{2}+d\sqrt{-2}) &= a+bi+c\sqrt{2}+d\sqrt{-2},\\
\sigma(a+bi+c\sqrt{2}+d\sqrt{-2}) &= a+bi-c\sqrt{2}-d\sqrt{-2},\\
\tau(a+bi+c\sqrt{2}+d\sqrt{-2}) &= a-bi+c\sqrt{2}-d\sqrt{-2},\\
\sigma\tau(a+bi+c\sqrt{2}+d\sqrt{-2}) &= a-bi-c\sqrt{2}+d\sqrt{-2}.
\end{aligned}$$

   for $a, b, c, d \in \mathbb{Q}$. Note that τ is complex conjugation. The four automorphisms permute the four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ by $\iota = ()$, $\sigma = (1\,2)(3\,4)$, $\tau = (1\,3)(2\,4)$, $\sigma\tau = (1\,4)(2\,3)$.
   (g) A glance at the subfields of F, listed in (c), shows that the only subfield of F containing β is F itself.

3. (a) ϕ is *not* an automorphism since it maps ω (a root of unity) to $-\omega$, which is not a cube root of unity.

   (b) ϕ is *not* an automorphism. Recall that $\mathbb{R}$ has no nontrivial automorphisms. Note that ϕ maps $\sqrt{2}$ (a square in F) to $-\sqrt{2}$, which is not a square in F.

   (c) Yes, ϕ is an automorphism of F. If we write $F = \{a + bi \,:\, a, b \in \mathbb{F}_3\}$, then $\phi(a + bi) = a - bi$.

   (d) Yes, ϕ is an automorphism of F since $F \supset \mathbb{Q}$ is a Galois extension generated by any of the four primitive fifth roots of unity, $\zeta, \zeta^2, \zeta^3, \zeta^4$, and ϕ is the unique automorphism mapping one of the roots to a conjugate root, namely $\zeta \mapsto \zeta^2$.

4. Consider the primitive fifth root of unity $\zeta = e^{2\pi i/5}$, and let $\alpha = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{5}$, so that $\alpha^2 = \zeta^2 + \zeta^{-2} + 2$. Now $\alpha^2 + \alpha = (1 + \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2}) + 1 = 1$, so $\alpha^2 + \alpha - 1 = 0$ and $\alpha = \frac{1}{2}\big(-1 \pm \sqrt{-5}\big)$. Since $\alpha > 0$, we must use the '+' sign, and $\cos\frac{2\pi}{5} = \frac{\alpha}{2} = -\frac{1}{4} + \frac{1}{4}\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$.

5. Use the extended Euclidean algorithm to first find $31^{-1} = 88$, so $x = \frac{17}{31} = 17{\cdot}88 = 1496 = 82$.

6. (a) F (b) T (c) F (d) F (e) T (f) T (g) F (h) F (i) F (j) T

   Comments (not required, but provided here for your benefit):

   (a) The only automorphism of the field of real numbers is the identity map $\iota(a) = a$.

   (b) This is the 'fixed field' of σ, which is featured so prominently in Galois theory.

   (c) The extension $\mathbb{C} \supset \mathbb{R}$ of degree two has infinitely many one-dimensional subspaces, but only one of them, $\mathbb{R}$, is a subfield. For example, the subspace $\{bi : b \in \mathbb{R}\} \subset \mathbb{C}$ is not a subfield.

   (d) The infinite field $\mathbb{F}_2(x)$ has characteristic 2.

   (e) Let p be any prime divisor of n; then $n = 0$ in $\mathbb{F}_p$.

   (f) As discussed in class, the multiplicative group of nonzero elements in any finite field is a cyclic group. (In fact, we did find a generator for this group of order 24.)

   (g) We have seen examples of number fields of degree 4 having a Galois group which is a Klein four-group. There are also extensions of degree 4 that are not even Galois; for example $\alpha = 2^{1/4}$ has minimal polynomial $m(x) = x^4 - 2 = (x^2 + \alpha^2)(x + \alpha)(x - \alpha)$ and the extension $E \supset \mathbb{Q}$ has only two automorphisms.

   (h) We have considered the splitting field $E \supset \mathbb{Q}$ of the polynomial $x^3 - 2$, which admits two automorphisms σ, τ such that $\sigma\tau \neq \tau\sigma$.

   (i) The polynomial $x^5 + x + 1$ has five complex roots, since $\mathbb{C}$ is algebraically closed. The work of Galois (later part of Abel's Theorem) showed that these roots are not expressible using mere radicals (since the Galois group of this polynomial is the nonsolvable group S_5).

   (j) Clearly $5\alpha{+}1 \in \mathbb{Q}[\alpha]$. Conversely, $\alpha = \frac{1}{5}(\beta{-}1) \in \mathbb{Q}[\beta]$ where $\beta = 5\alpha{+}1$.