MAT205 Quiz 2 Answer Key

Question 1. True or false with justification [3 marks]

a. [1 mark] $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$.

Solution.

True. By Eisenstein's criterion at $p = 3$, $x^5 - 3$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of $\sqrt[5]{3}$ and $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = \deg(x^5 - 3) = 5$.

b. [1 mark] Every algebraic extension of $\mathbb{Q}$ has finite degree over $\mathbb{Q}$.

Solution.

False. The field $\overline{\mathbb{Q}}$ of all algebraic numbers is algebraic over $\mathbb{Q}$ but infinite-dimensional. Concretely, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ is algebraic over $\mathbb{Q}$ yet contains subfields of arbitrarily large degree, so it is not finite over $\mathbb{Q}$.

c. [1 mark] $\mathbb{Q}(\sqrt[5]{3})$ is a normal extension of $\mathbb{Q}$.

Solution.

False. The polynomial $x^5 - 3$ is irreducible over $\mathbb{Q}$ and has the root $\sqrt[5]{3} \in \mathbb{Q}(\sqrt[5]{3})$, but its other four roots $\zeta_5 \sqrt[5]{3}, \zeta_5^2 \sqrt[5]{3}, \zeta_5^3 \sqrt[5]{3}, \zeta_5^4 \sqrt[5]{3}$ (where $\zeta_5 = e^{2\pi i/5}$) are non-real and not in $\mathbb{Q}(\sqrt[5]{3}) \subset \mathbb{R}$. Thus an irreducible polynomial with a root in the field fails to split, so the extension is not normal.

Question 2. Solve [6 marks]

Let F be the splitting field of $x^5 - 3$ over $\mathbb{Q}$, $\beta = \sqrt[5]{3}$ (real), $\omega = e^{2\pi i/5}$, $F = \mathbb{Q}(\beta, \omega)$, and σ, τ as defined in the question.

a. [4 marks] Verify σ, τ, find $[F : \mathbb{Q}]$, and determine $\mathrm{Gal}(F/\mathbb{Q})$.

Solution.

Well-defined. σ sends the root β of $x^5 - 3$ to another root $\beta\omega$ of $x^5 - 3$, and fixes ω; τ fixes β and sends the root ω of the cyclotomic polynomial Φ_5 to another root ω^2. Both extend to automorphisms of $F = \mathbb{Q}(\beta, \omega)$ fixing $\mathbb{Q}$, since they permute the roots of the defining polynomials of β and ω.

Orders. $\sigma^5(\beta) = \beta\omega^5 = \beta$ and σ fixes ω, so σ has order 5. τ sends $\omega \mapsto \omega^2 \mapsto \omega^4 \mapsto \omega^3 \mapsto \omega$, a 4-cycle, so τ has order 4.

Relation. $\tau\sigma\tau^{-1}(\beta) = \tau\sigma(\beta) = \tau(\beta\omega) = \beta\omega^2 = \sigma^2(\beta)$, and both $\tau\sigma\tau^{-1}$ and σ^2 fix ω; hence $\tau\sigma\tau^{-1} = \sigma^2$.

Degree and Galois group. By Eisenstein at $p = 3$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5$; the minimal polynomial of ω is $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, so $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. Both $5, 4$ divide $[F : \mathbb{Q}]$ and $\gcd(5, 4) = 1$, so $20 \mid [F : \mathbb{Q}]$; and ω satisfies Φ_5 (degree 4) over $\mathbb{Q}(\beta)$ too, so $[F : \mathbb{Q}(\beta)] \le 4$, giving $[F : \mathbb{Q}] = [F : \mathbb{Q}(\beta)] \cdot 5 \le 20$. Hence $[F : \mathbb{Q}] = 20$.

Since $\sigma, \tau \in \mathrm{Gal}(F/\mathbb{Q})$ and $\langle \sigma, \tau \rangle$ has order $20 = |\mathrm{Gal}(F/\mathbb{Q})|$, we get $\mathrm{Gal}(F/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^5 = \tau^4 = 1,\ \tau\sigma\tau^{-1} = \sigma^2 \rangle$, the (non-abelian) Frobenius group of order 20, $F_{20} \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$.

b. [2 marks] Fixed fields of $\langle \sigma \rangle$ and $\langle \tau \rangle$.

Solution.

$$F^{\langle \sigma \rangle} = \mathbb{Q}(\omega), \qquad F^{\langle \tau \rangle} = \mathbb{Q}(\beta).$$

(Degree check: $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4 = [\mathrm{Gal}(F/\mathbb{Q}) : \langle \sigma \rangle]$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5 = [\mathrm{Gal}(F/\mathbb{Q}) : \langle \tau \rangle]$.)

Question 3. Prove [6 marks]

a. [2 marks] Prove $\langle\tau\rangle$ is not normal.

Solution.

Every element of $\langle\tau\rangle$ fixes β (by definition of τ), but

$$\sigma\tau\sigma^{-1}(\beta) = \sigma\tau(\beta\omega^{-1}) = \sigma(\beta\,\omega^{-2}) = (\beta\omega)\omega^{-2} = \beta\omega^{-1} \neq \beta,$$

so $\sigma\tau\sigma^{-1} \notin \langle\tau\rangle$. Hence $\langle\tau\rangle$ is not normal in $\mathrm{Gal}(F/\mathbb{Q})$.

b. [4 marks] Number of conjugates of $\langle\tau\rangle$, and their fixed fields.

Solution.

$\langle\tau\rangle$ is a Sylow 2-subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ (order 4, index 5). By Sylow's theorem, the number n_2 of Sylow 2-subgroups satisfies $n_2 \mid 5$ and $n_2 \equiv 1 \pmod 2$; both divisors of 5 (namely 1 and 5) are odd, so Sylow's theorem alone allows either value. But $n_2 = 1$ would mean $\langle\tau\rangle$ is the unique, hence normal, Sylow 2-subgroup, contradicting part (a). So $n_2 = 5$: there are exactly 5 subgroups conjugate to $\langle\tau\rangle$.

These conjugates are $\sigma^i\langle\tau\rangle\sigma^{-i}$ for $i = 0, 1, 2, 3, 4$, with fixed fields

$$\sigma^i\big(F^{\langle\tau\rangle}\big) = \sigma^i(\mathbb{Q}(\beta)) = \mathbb{Q}(\sigma^i(\beta)) = \mathbb{Q}(\beta\omega^i), \qquad i = 0, 1, 2, 3, 4.$$

So the 5 conjugate Sylow 2-subgroups correspond exactly to the 5 (mutually conjugate, isomorphic but distinct) subfields $\mathbb{Q}(\beta), \mathbb{Q}(\beta\omega), \mathbb{Q}(\beta\omega^2), \mathbb{Q}(\beta\omega^3), \mathbb{Q}(\beta\omega^4)$ generated by the five roots of $x^5 - 3$ — each non-normal over $\mathbb{Q}$, consistent with Question 1(c).