PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

27 March 2025 75 minutes

This paper contains **FIVE** *questions worth a total of 140 points.*

Midterm II

Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1 (5+5+5+5+5+5=30) Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with “T”, and those which are false with “F”.

(a) Every algebraic extension of $\mathbb{Q}$ is separable.
(b) Every algebraic extension of $\mathbb{Q}$ is normal.
(c) A splitting field is unique up to isomorphism.
(d) For any polynomial $f \in K[t]$, its Galois group $\mathrm{Gal}_K(f)$ acts transitively on the roots of f.
(e) Let $K - M - L$ be a field extension. If $K - L$ is normal, then $M - L$ is normal.
(f) Let $K - M - L$ be a field extension. If $K - L$ is separable, then $M - L$ is separable.

2 (5+5+5+5=20) (a) Let $K - L$ be a field extension. Define what it means for $f \in K[t]$ splits over L.

(b) Define what it means for a field extension $L : K$ to be a splitting field extension.

(c) Define what it means for a field extension $L : K$ to be normal.

(d) Define what it means for a field to be algebraically closed.

3 (5+10+10=25) (a) Give a definition of Galois group (historical or modern).

(b) Let $f(t) = (t+1)^4 - (t+2)^2 \in \mathbb{Q}[t]$. Find a splitting field extension $L : \mathbb{Q}$ for f and compute $[L : \mathbb{Q}]$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(L)$.

4 (5+10+10=25) (a) Let $f \in K[t]$, $L = K(\alpha_1, \ldots, \alpha_n)$ be the splitting field of f (here, as always, $\alpha_1, \ldots, \alpha_n$ are roots of f). Compute $\mathrm{Gal}_L(f)$.

(b) Let $t^8 - 16 \in \mathbb{Q}[t]$. Find a splitting field extension $L : \mathbb{Q}$ for f and compute $[L : \mathbb{Q}]$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(L)$.

5 (5+10+10+15=40) (a) Let p be a prime number and $\overline{\mathbb{F}}_p$ be a the algebraic closure of $\mathbb{F}_p$. Put $K := \overline{\mathbb{F}}_p(t)$. Give an example of $f \in K[X]$ such that f is inseparable, or prove that such an example does not exist.

(b) Find $\mathrm{Gal}_{\mathbb{Q}}(t^3 - 3)$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(t^{17} - 1)$.

(d) Find $\mathrm{Gal}_{\mathbb{F}_2(t)}(\mathbb{F}_4(t))$.

Solutions

General remark. If there is a typo in any task, then the maximum score will be awarded for that task.

1 (5+5+5+5+5+5=30) Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which are false with "F".

(a) Every algebraic extension of $\mathbb{Q}$ is separable.
(b) Every algebraic extension of $\mathbb{Q}$ is normal.
(c) A splitting field is unique up to isomorphism.
(d) For any polynomial $f \in K[t]$, its Galois group $\mathrm{Gal}_K(f)$ acts transitively on the roots of f.
(e) Let $K - M - L$ be a field extension. If $K - L$ is normal, then $M - L$ is normal.
(f) Let $K - M - L$ be a field extension. If $K - L$ is separable, then $M - L$ is separable.

Solution. (a) TRUE. See lectures, more generally the same takes place for any field of characteristic zero.

(b) FALSE. Take $\mathbb{Q}(2^{1/3})$.

(c) TRUE. It was a result in lectures.

(d) FALSE. This is true only if f is irreducible. If f is reducible, then $\mathrm{Gal}_K(f)$ acts transitively on the roots of each irreducible factor of f.

(e) TRUE. It was a result in lectures.

(f) TRUE. It was a result in lectures.

2 (5+5+5+5=20) (a) Let $K - L$ be a field extension. Define what it means for $f \in K[t]$ splits over L.

(b) Define what it means for a field extension $L : K$ to be a splitting field extension.

(c) Define what it means for a field extension $L : K$ to be normal.

(d) Define what it means for a field to be algebraically closed.

Solution. (a) It means that for $\varphi : K \to L$ one has $\varphi(f) = c\prod_{j=1}^{d}(t - \alpha_j)$, where $c \in \varphi(K)$ and $\alpha_j \in L$.

(b) We assume that f splits over M (see part (a)) and $L \subseteq M$. Then $L : K$ is a splitting field extension if L is the smallest subfield of M, containing $\varphi(K)$ over which f splits.

(c) The extension $K - L$ is normal if it is algebraic, and every irreducible polynomial $f \in K[t]$ either splits over L or has no root in L.

(d) A field K is algebraically closed if any non–constant polynomial $f \in K[t]$ has a root in K.

3 (5+10+10=25) (a) Give a definition of Galois group (historical or modern).

(b) Let $f(t) = (t+1)^4 - (t+2)^2 \in \mathbb{Q}[t]$. Find a splitting field extension $L : \mathbb{Q}$ for f and compute $[L : \mathbb{Q}]$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(L)$.

Solution. (a) We give a modern definition. Let $L : K$ be a field extension. Then $\mathrm{Gal}_K(L) = \mathrm{Aut}_K(L)$, that is a collection of automorphisms $\varphi : L \to L$ such that $\varphi(k) = k$ for any $k \in K$.

(b) We have $f(t) = (t^2+t-1)(t^2+3t+3)$. Thus f has roots $(1\pm\sqrt{5}/2$ and $(-3\pm i\sqrt{3})/2$. It follows that $L = \mathbb{Q}(\sqrt{5}, i\sqrt{3})$. Further $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ and the minimal polynomial for $i\sqrt{3}$ is $t^2 + 3$. It follows that $[L : \mathbb{Q}] = 2 \cdot 2 = 4$ thanks to the tower law.

(c) Any $\varphi \in \mathrm{Gal}_{\mathbb{Q}}(L)$ permutes the roots of $t^2 - 5$ and any such φ can be extended to L by taking $\varphi(i\sqrt{3}) = \pm i\sqrt{3}$. Thus $\mathrm{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and in terms of permutations one has $\mathrm{Gal}_{\mathbb{Q}}(f) = \{Id, (12), (34), (12)(34)\} \cong V_4$.

4 (5+10+10=25) (a) Let $f \in K[t]$, $L = K(\alpha_1, \dots, \alpha_n)$ be the splitting field of f (here, as always, $\alpha_1, \dots, \alpha_n$ are roots of f). Compute $\mathrm{Gal}_L(f)$.

(b) Let $t^8 - 16 \in \mathbb{Q}[t]$. Find a splitting field extension $L : \mathbb{Q}$ for f and compute $[L : \mathbb{Q}]$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(L)$.

Solution. (a) One can consider the polynomials $f_j(t_1, \dots, t_n) = t_j - \alpha_j \in L[t_1, \dots, t_n]$. Then $f_j(\alpha_1, \dots, \alpha_n) = 0$ but for any $\sigma \in S_n$, $\sigma \neq Id$ there is j such that $\sigma(j) = i \neq j$. Hence $\sigma f_j(\alpha_1, \dots, \alpha_n) = \alpha_i - \alpha_j \neq 0$. Thus $\mathrm{Gal}_L(f) = \{Id\}$.

Similarly, one can use the modern definition of Galois group. Then we see that any automorphism φ such that $\varphi(l) = l$ for any $l \in L$ is, obviously, Id.

(b) We have $t^8 - 16 = \prod_{\varepsilon \in \sqrt[8]{1}} (t - \varepsilon\sqrt{2})$. Thus $L = \mathbb{Q}(\sqrt{2}, \varepsilon_8)$, where as always $\varepsilon_8 = e^{\pi i/4} = (1+i)/\sqrt{2}$. Hence $L = \mathbb{Q}(\sqrt{2}, i)$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Thus $[L : \mathbb{Q}(\sqrt{2})] = 2$ and by the tower law $[L : \mathbb{Q}] = 4$.

(c) The same argument as in Question 3 gives us $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \{Id, (12), (34), (12)(34)\} \cong V_4$.

5 (5+10+10+15=40) (a) Let p be a prime number and $\overline{\mathbb{F}}_p$ be a the algebraic closure of $\mathbb{F}_p$. Put $K := \overline{\mathbb{F}}_p(t)$. Give an example of $f \in K[X]$ such that f is inseparable, or prove that such an example does not exist.

(b) Find $\mathrm{Gal}_{\mathbb{Q}}(t^3 - 3)$.

(c) Find $\mathrm{Gal}_{\mathbb{Q}}(t^{17} - 1)$.

(d) Find $\mathrm{Gal}_{\mathbb{F}_2(t)}(\mathbb{F}_4(t))$.

Solution. (a) Put $f(X) = X^p - t$. Then $f \in K[X]$ is irreducible (see lectures or apply the Eisenstein criterion and Gauss' lemma) but $f(X) = (X - \alpha)^p$, where $\alpha \in \overline{K}$, $\alpha^p = t$. Therefore, f is not separable.

(b) The roots of $t^3 - 3$ are $\alpha_j := 3^{1/3}\varepsilon_3^j$, $j = 0, 1, 2$ and hence $\alpha_2, \alpha_3 \notin \mathbb{Q}(\alpha_1)$. Thus $\mathrm{Gal}_{\mathbb{Q}}(t^3 - 3) \cong S_3$ (see lectures).

(c) This is a cyclotomic polynomial and we know that $\mathrm{Gal}_{\mathbb{Q}}(x^{17} - 1) \cong \mathbb{Z}_n$, where $n = \varphi(17) = 16$.

(d) One has $\mathbb{F}_4 = \mathbb{F}_2(g)$, where g is a primitive root, i.e., $\mathbb{F}_4^* = \{1, g, g^2\}$. In particular, $g^3 = 1$ and $1 + g + g^2 = 0$. Thus g is a root of irreducible and separable polynomial $X^2 + X + 1 = 0$. Therefore $\mathbb{F}_4(t) = \mathbb{F}_2(g)(t)$ and $|\mathrm{Gal}_{\mathbb{F}_2(t)}(\mathbb{F}_4(t))| = [\mathbb{F}_4(t) : \mathbb{F}_2(t)]$. It follows that $\mathrm{Gal}_{\mathbb{F}_2(t)}(\mathbb{F}_4(t)) \cong \mathbb{Z}_2 = \{Id, \Phi\}$, where $\Phi(a) = a^2$ is the Frobenius automorphism.