PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

6 February 2025 75 minutes

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

Midterm I

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 points) 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) There is a field homomorphism $\psi : \mathbb{Q}(2^{1/4}) \to \mathbb{Q}(\sqrt{2})$.

(b) There is a homomorphism of finite fields $\psi : \mathbb{F}_3 \to \mathbb{F}_5$.

(c) If α is algebraic over a field $K \subseteq \mathbb{C}$, then $\sqrt{\alpha}$ is algebraic over K.

(d) It is possible to construct by ruler and compass the number $3^{1/3} + 5^{1/5}$.

(e) Polynomial $x^n + px^2 + px + pq \in \mathbb{Q}[x]$, where p, q are some distinct primes, is irreducible over $\mathbb{Q}$.

(f) Let $L : K$ be a field extension, $\alpha \in L$. Then $1/\alpha$ can be expressed as a polynomial in α with coefficients in K.

2 (5+10+10=25 points) Let α be a root of the polynomial $f(t) = t^3 + t + 3$.

(a) Prove that $f(t)$ is irreducible in $\mathbb{Q}[t]$.

(b) Compute the minimal polynomials for $\beta = \alpha - 1$ and $\gamma = \alpha^2 + 1$ over $\mathbb{Q}$.

(c) Express β^{-1} and γ^{-1} in the form $a + b\alpha + c\alpha^2$, where $a, b, c \in \mathbb{Q}$.

3 (5+10=15 points) (a) Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K. Define what is meant by the minimal polynomial of α over K.

(b) Compute the minimal polynomial of $\alpha := \sqrt[5]{5 + \sqrt[3]{10}}$ over $\mathbb{Q}$ and determine the degree of the field extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

4 (5+5+5+15=30 points) (a) Define the degree of the field extension $L : K$.

(b) Consider the quotient ring $\mathbb{F}_3[t]/(t^2 + t + 1)$ and compute its size.

(c) What is the degree of the field extension $\mathbb{F}_3[t]/(t^2 + t + 1) : \mathbb{F}_3$?

(d) Let $K(\alpha) : K$ be a field extension, $[K(\alpha) : K] = p$, where p is a prime number. Compute $[K(f(\alpha)) : K]$, where $f \in K[t]$ is an arbitrary polynomial of degree strictly less than p.

5 (5+5+15+15=40 points) (a) Let α be algebraic over a field K. Give the definition of algebraic conjugates of α.

(b) Suppose that α is algebraic over a field K and α has algebraic conjugates $\alpha_1, \ldots, \alpha_d$. Let $f \in K[t]$. Compute algebraic conjugates of $f(\alpha)$.

(c) Compute algebraic conjugates of $\sqrt[3]{2}i + 1$ over $\mathbb{Q}$, then over $\mathbb{Q}(\sqrt[3]{2}i)$ and, finally, over $\mathbb{Q}(2^{2/3})$.

(d) Let $K \subset \mathbb{C}$ be a field, α is algebraic over K and β is transcendental over K. Consider $K(\alpha, \beta)$ and assume that α does not belong to K. Prove that there is no θ such that $K(\alpha, \beta) = K(\theta)$ (in other words, $K(\alpha, \beta) : K$ is not a simple field extension).

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 points) 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) There is a field homomorphism $\psi : \mathbb{Q}(2^{1/4}) \to \mathbb{Q}(\sqrt{2})$.
(b) There is a homomorphism of finite fields $\psi : \mathbb{F}_3 \to \mathbb{F}_5$.
(c) If α is algebraic over a field $K \subseteq \mathbb{C}$, then $\sqrt{\alpha}$ is algebraic over K.
(d) It is possible to construct by ruler and compass the number $3^{1/3} + 5^{1/5}$.
(e) Polynomial $x^n + px^2 + px + pq \in \mathbb{Q}[x]$, where p, q are some primes, is irreducible over $\mathbb{Q}$.
(f) Let $L : K$ be a field extension, $\alpha \in L$. Then $1/\alpha$ can be expressed as a polynomial in α with coefficients in K.

Solution: (a) TRUE. Let $\alpha = 2^{1/4}$ and put $\psi(a + b\alpha) = a + b\alpha^2$. It is easy to see that this is a homomorphism.

Solution: (b) FALSE. $0 = \psi(0) = \psi(1 + 1 + 1) = \psi(1) + \psi(1) + \psi(1) = 3 \neq 0$ in $\mathbb{F}_5$.

Solution: (c) TRUE. We know that there is $f \in K[t]$ s.t. $f(\alpha) = 0$. Put $g(x) = f(x^2) \in K[x]$. Then $g(\sqrt{\alpha}) = f(\alpha) = 0$ and thus $\sqrt{\alpha}$ is an algebraic number.

Solution: (d) FALSE. The degree of $3^{1/3}$ is three; therefore, the degree of $3^{1/3} + 5^{1/5}$ is divisible by three. But we know that any constructible number must have degree 2^n for some n.

Solution: (e) TRUE. It follows from Eisenstein's criterion.

Solution: (f) FALSE. Let α be transcendental over K, then $K[\alpha] \neq K(\alpha)$.

2 (5+10+10=25 points) Let α be a root of the polynomial $f(t) = t^3 + t + 3$.

(a) Prove that $f(t)$ is irreducible in $\mathbb{Q}[t]$.
(b) Compute the minimal polynomials for $\beta = \alpha - 1$ and $\gamma = \alpha^2 + 1$ over $\mathbb{Q}$.
(c) Express β^{-1} and γ^{-1} in the form $a + b\alpha + c\alpha^2$, where $a, b, c \in \mathbb{Q}$.

Solution: (a) This polynomial of degree 3 is irreducible since it has no rational roots.

(b) The equation $\alpha^3 + \alpha + 3 = 0$ implies $\beta^3 + 3\beta^2 + 4\beta + 5 = 0$. This is a cubic polynomial again, and it is easy to check that it has no rational roots. Thus, this is the minimal polynomial for β. Now the equation $\alpha^3 + \alpha + 3 = 0$ implies $\alpha\gamma + 3 = 0$ and hence $\gamma = -3/\alpha$. Thus

$$\gamma^2 = \frac{9}{\alpha^2} = \frac{9}{\gamma - 1}\,.$$

It follows that γ is a root of the polynomial $t^3 - t^2 - 9 = 0$, which is also irreducible and hence minimal.

(c) We know that $\beta^3 + 3\beta^2 + 4\beta + 5 = 0$. It follows that $5\beta^{-1} = -(\beta^2 + 3\beta + 4) = -\alpha^2 - \alpha - 2$. From $\alpha\gamma + 3 = 0$ we see that $\gamma^{-1} = -\alpha/3$.

3 (5+10=15 points) (a) Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K. Define what is meant by the minimal polynomial of α over K.

(b) Compute the minimal polynomial of $\alpha := \sqrt[5]{5 + \sqrt[3]{10}}$ over $\mathbb{Q}$ and determine the degree of the field extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Solution: (a) The minimal polynomial of α over K is the unique monic polynomial μ_α^K such that $\mu_\alpha^K(\alpha) = 0$ and μ_α^K has the smallest degree among all polynomials over K such that $f(\alpha) = 0$.

(b) We have $\alpha^5 - 5 = \sqrt[3]{10}$ and hence $(\alpha^5 - 5)^3 = 10$. Thus the minimal polynomial of α divides $f(t) = (t^5 - 5)^3 - 10$ and we see that the leading coefficient of $f(t)$ is 1, all other coefficients are divisible by 5, and the constant coefficient $5^3 - 10$ is not divisible by 5^2. Then by Eisenstein's criterion $f(t)$ is the minimal polynomial of α.

4 (5+5+5+15=30 points) (a) Define the degree of the field extension $L : K$.

(b) Consider the quotient ring $\mathbb{F}_3[t]/(t^2+t+1)$ and compute its size.

(c) What is the degree of the field extension $\mathbb{F}_3[t]/(t^2+t+1) : \mathbb{F}_3$?

(d) Let $K(\alpha) : K$ be a field extension, $[K(\alpha) : K] = p$, where p is a prime number. Compute $[K(f(\alpha)) : K]$, where $f \in K[t]$ is an arbitrary polynomial of degree strictly less than p.

Solution: (a) This is just the dimension of L as a vector space over K.

(b) One has $t^2+t+1 = (t-1)^2$ and thus our polynomial is reducible in $\mathbb{F}_3[t]$. Anyway the ring $\mathbb{F}_3[t]/(t^2+t+1)$ is isomorphic to $S := \{a+bt \ : \ a, b \in \mathbb{F}_3\}$ and therefore has size 9.

(c) The set S is a vector space over $\mathbb{F}_3$ of dimension two but S is not a field. For example, $(t-1)^2 \equiv 0\,(t^2+t+1)$ and we have zero divisors. Hence this is not field extension.

After some thought, I came to the conclusion that points (b) and (c) are overcomplicated, so I give full marks to any reasonable argument.

(d) Since $K(f(\alpha)) \subseteq K(\alpha)$, we have the field tower $K - K(f(\alpha)) - K(\alpha)$ and hence by the tower law we have $p = [K(\alpha) : K] = [K(\alpha) : K(f(\alpha))][K(f(\alpha)) : K]$ and therefore $[K(f(\alpha)) : K] \in \{1, p\}$. But $g(x) = f(x) - f(\alpha)$ belongs to $K(f(\alpha))$ and $g(\alpha) = 0$. Thus $[K(\alpha) : K(f(\alpha))] \le \deg f < p$. It follows that $[K(f(\alpha)) : K] = p$.

5 (5+5+15+15=40 points) (a) Let α be algebraic over a field K. Give the definition of algebraic conjugates of α.

(b) Suppose that α is algebraic over a field K and α has algebraic conjugates $\alpha_1, \dots, \alpha_d$. Let $f \in K[t]$. Compute algebraic conjugates of $f(\alpha)$.

(c) Compute algebraic conjugates of $\sqrt[3]{2}i + 1$ over $\mathbb{Q}$, then over $\mathbb{Q}(\sqrt[3]{2}i)$ and, finally, over $\mathbb{Q}(2^{2/3})$.

(d) Let $K \subset \mathbb{C}$ be a field, α is algebraic over K and β is transcendental over K. Consider $K(\alpha, \beta)$ and assume that α does not belong to K. Prove that there is no θ such that $K(\alpha, \beta) = K(\theta)$ (in other words, $K(\alpha, \beta) : K$ is not a simple field extension).

Solution: (a) Suppose that $\mu_\alpha^K(x) = \prod_{j=1}^d (x - \alpha_j)$, where α_j belong to a certain extension of K. Then $\alpha_1, \dots, \alpha_d$ are algebraic conjugates of α.

(b) These are $f(\alpha_1), \dots, f(\alpha_d)$, see lectures.

(c) Let $\alpha = \sqrt[3]{2}i + 1$. We have $(\alpha - 1)^6 = -4$ and therefore α is a root of the polynomial $f(t) = (t-1)^6 + 4$. Other roots of f are $\pm\sqrt[3]{2}i + 1$ and $\pm\sqrt[3]{2}\varepsilon_\pm + 1$, where $\varepsilon_\pm = \pm\frac{\sqrt{3}}{2} + \frac{i}{2}$. Using Vieta's formulae, one can check that $f(t)$ is the minimal polynomial. Thus all these roots are algebraic conjugates of α. Over $\mathbb{Q}(\sqrt[3]{2}i)$ the minimal polynomial is $t - \alpha$ and hence α is the only algebraic conjugate of α. Now

$$(t - \sqrt[3]{2}i - 1)(t + \sqrt[3]{2}i - 1) = (t-1)^2 + 2^{2/3} \in \mathbb{Q}(2^{2/3}),$$

and this is, obviously, the minimal polynomial of α over $\mathbb{Q}(2^{2/3})$. Hence $\pm\sqrt[3]{2}i + 1$ are algebraic conjugates of α over $\mathbb{Q}(2^{2/3})$.

(d) Suppose that $K(\alpha, \beta) = K(\theta)$. Clearly, θ is transcendental over K. Further, we have $\alpha = f(\theta)/g(\theta)$, where $f, g \in K[t]$, $g(\theta) \neq 0$ and hence $h(t) := \alpha g(t) - f(t)$ belongs to $K(\alpha)[t]$ and is obviously nonzero (recall that $\alpha \notin K$ and $g(\theta) \neq 0$). One has $h(\theta) = 0$ and therefore θ is algebraic over $K(\alpha)$. But this gives us a contradiction with the tower law: $\infty = [K(\theta) : K] = [K(\theta) : K(\alpha)][K(\alpha) : K] < \infty$.

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.