PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY – SOLUTIONS
MA 45401-H01

15th February 2024 75 minutes

This paper contains **SIX** *questions.*
All SIX answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1. [3+3+3+3+3+3=18 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 may be false with "F".

   a. There is a field isomorphism $\varphi : \mathbb{Q}(\sqrt{-5}) \to \mathbb{Q}(\sqrt{5})$.

   Solution: False (if true, then $\varphi(\sqrt{-5})^2 = \varphi(-5) = -5$, yielding a contradiction, since there exists no element ξ of $\mathbb{Q}(\sqrt{5})$ for which $\xi^2 = -5 < 0$).

   b. There is a homomorphism of finite fields $\psi : \mathbb{F}_3 \to \mathbb{F}_{37}$.

   Solution: False (if true, then since $\psi(1) = 1$, we would have $0 = \psi(1+1+1) = \psi(1) + \psi(1) + \psi(1) = 3 \in \mathbb{F}_{37}$, leading to a contradiction).

   c. If $L : K$ is a field extension, and α and β are distinct elements of L having the same minimal polynomial over K, then $K(\alpha)$ and $K(\beta)$ are isomorphic fields.

   Solution: True (this is an immediate consequence of Theorem 3.2 from the course).

   d. It is *not* possible to construct, using compass and straightedge in the usual way, a length whose 14^{th} power is twice a given length.

   Solution: True (by Eisenstein's criterion, the polynomial $t^{14} - 2$ is irreducible over $\mathbb{Q}$, and thus the element $2^{1/14}$ has minimal polynomial $t^{14} - 2$. Hence $[\mathbb{Q}(2^{1/14}) : \mathbb{Q}] = 14$, which is not a power of 2, and so $2^{1/14}$ is not constructible using compass and straightedge).

   e. The polynomial $x^{36} + x^{35} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$.

   Solution: True (it follows from Q1(b) of Homework 3 that $x^{p-1} + \ldots + x + 1$ is irreducible for any prime p, and 37 is prime).

   f. If K is a field and α is an element of an extension field L of K, then every element of $K(\alpha)$ can be expressed as a polynomial in α with coefficients in K.

   Solution: False (it is possible that α is transcendental over K, and then $1/\alpha$ is not a polynomial in α with coefficients in K).

2. [3+3+3+3=12 points]

   (a) For $j = 1$ and 2, let $L_j : K_j$ be a field extension relative to the embedding $\varphi_j : K_j \to L_j$. Suppose that $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are isomorphisms. Define what is meant by the statement that τ *extends* σ.

   Solution: The isomorphism τ *extends* σ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$.

   (b) Let $L : M : K$ be a tower of field extensions with $K \subseteq M \subseteq L$. Define what is meant by the statement that $\sigma : M \to L$ *is a K-homomorphism.*

   Solution: The mapping $\sigma : M \to L$ is a *K-homomorphism* if σ leaves K pointwise fixed, so that, for all $\alpha \in K$, one has $\sigma(\alpha) = \alpha$.

   (c) Suppose that $L : K$ is a field extension. Define what is meant by the *degree* of $L : K$.

   Solution: The *degree* of $L : K$ is the dimension of L as a vector space over K.

   (d) Suppose that $L : K$ is a field extension with $K \subseteq L$, and $\alpha \in L$ is algebraic over K. Define what is meant by the *minimal polynomial* of α over K.

   Solution: The *minimal polynomial* of α over K is the unique monic polynomial $m_\alpha(K)$ having the property that $\ker(E_\alpha) = (m_\alpha(K))$, where $E_\alpha : K[t] \to L$ denotes the evaluation map defined by putting $E_\alpha(f) = f(\alpha)$.

Continued...

3. [15 points] Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K and $\beta \in L$ is transcendental over K. Suppose also that $\alpha \notin K$. Show that $K(\alpha, \beta) : K$ is not a simple field extension.

 Solution: Suppose that $K(\alpha, \beta) = K(\gamma)$ for some $\gamma \in L$. Since $\beta \in K(\gamma)$ is transcendental over K, the field extension $K(\gamma) : K$ is not algebraic, and hence γ is transcendental over K. Since $\alpha \in K(\gamma)$, we have $\alpha = f(\gamma)/g(\gamma)$ for some $f, g \in K[t]$ with $g \neq 0$. Thus γ is a root of $h = \alpha g - f \in K(\alpha)[t]$. Since $\alpha \notin K$ and $g \neq 0$, the polynomial h cannot be the zero polynomial, and therefore γ is algebraic over $K(\alpha)$. But then, since α is algebraic over K, this implies that $[K(\gamma) : K] = [K(\gamma) : K(\alpha)][K(\alpha) : K] < \infty$, contradicting the transcendence of γ. So $K(\alpha, \beta) : K$ cannot be a simple extension.

4. [8+8+8=24 points] Let θ denote the real number $\sqrt{3 + \sqrt[3]{6}}$, and write $L = \mathbb{Q}(\theta)$.

 (a) Calculate the minimal polynomial of θ over $\mathbb{Q}$, and hence determine the degree of the field extension $L : \mathbb{Q}$.

 Solution: Write $\theta = \sqrt{3 + \sqrt[3]{6}}$. Then $\theta^2 - 3 = \sqrt[3]{6}$, and hence $(\theta^2 - 3)^3 = 6$. On putting $f(x) = (x^2 - 3)^3 - 6 = x^6 - 9x^4 + 27x^2 - 33$, we see that $f(\theta) = 0$, and thus it follows that the minimal polynomial $m_\theta(\mathbb{Q})$ of θ over $\mathbb{Q}$ divides f. But by applying Eisenstein's criterion (and Gauss' Lemma) using the prime 3, we see that f is irreducible: the lead coefficient of f is not divisible by 3, all other coefficients are divisible by 3, and the constant coefficient -33 is divisible by 3 but not by 3^2. Hence f is the minimal polynomial of θ over $\mathbb{Q}$. The degree of the field extension $\mathbb{Q}(\sqrt{3 + \sqrt[3]{6}}) : \mathbb{Q}$ is therefore equal to $\deg f = 6$.

 (b) Let $f \in \mathbb{Q}[t]$ be a monic polynomial of degree 4. Suppose that $\alpha \in L$ satisfies the property that $f(\alpha) = 0$. Is it possible that f is irreducible over $\mathbb{Q}$? Justify your answer.

 Solution: Suppose that f is irreducible with leading coefficient $c \in \mathbb{Q} \setminus \{0\}$. Then the irreducible polynomial of α over $\mathbb{Q}$ is $c^{-1}f$ and has degree 4, whence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. But $\mathbb{Q}(\alpha)$ is a subfield of L, so by the Tower Law we have

$$6 = [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4[L : \mathbb{Q}(\alpha)],$$

 so that 4 divides 6, yielding a contradiction. Hence f cannot be irreducible over $\mathbb{Q}$.

 (c) Suppose that β and γ are elements in $\mathbb{C}$ having the property that both $\beta + \gamma$ and $\beta\gamma$ are algebraic over $\mathbb{Q}$. Prove that β and γ are both algebraic over $\mathbb{Q}$.

 Solution: Define the algebraic numbers $\lambda = \beta + \gamma$ and $\mu = \beta\gamma$, and observe that $(\beta - \gamma)^2 = \lambda^2 - 4\mu$ must then be algebraic over $\mathbb{Q}$. But then $\nu = \beta - \gamma = \pm\sqrt{\lambda^2 - 4\mu}$ is algebraic over $\mathbb{Q}$, and hence also $\beta = \frac{1}{2}(\lambda + \nu)$ and $\gamma = \frac{1}{2}(\lambda - \nu)$ must be algebraic over $\mathbb{Q}$.

5. [6+6+5=17 points] Let $L : \mathbb{Q}$ be an algebraic extension with $\mathbb{Q} \subseteq L$, and consider a homomorphism of fields $\varphi : L \to L$.

 (a) By considering $\varphi(\mathbb{Z})$, or otherwise, show that φ is a $\mathbb{Q}$-homomorphism.

 Solution: Since $\varphi(1) = 1$ (and φ is a homomorphism), one has $\varphi(n) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = n$ for each $n \in \mathbb{N}$. Thus, the homomorphism properties of φ ensure that $\varphi(0) = 0$, $\varphi(-n) = -n$ for $n \in \mathbb{N}$, and $\varphi(a/b) = \varphi(a)/\varphi(b) = a/b$ for each $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Thus φ fixes $\mathbb{Q}$ pointwise, and consequently φ is a $\mathbb{Q}$-homomorphism.

 (b) Suppose that $\alpha \in L$. Show that the minimal polynomial of α over $\mathbb{Q}$ has $\varphi^n(\alpha)$ as a root, for each non-negative integer n, where φ^n denotes the n-fold composition of φ.

Continued...

Solution: Since φ is a $\mathbb{Q}$-homomorphism of $\mathbb{Q}$, we see that $\varphi(m_\alpha(\mathbb{Q})) = m_\alpha(\mathbb{Q})$. Moreover, writing $f = m_\alpha(\mathbb{Q})$, we have $0 = \varphi(0) = \varphi(f(\alpha)) = f(\varphi(\alpha))$, so that $\varphi(\alpha)$ is a root of f whenever α is a root of f. By iterating this argument, it follows that $\varphi^n(\alpha)$ is a root of f for all non-negative integers n.

(c) Suppose that $\alpha \in L$. Show that there is a positive integer d with the property that $\varphi^d(\alpha) = \alpha$. Moreover, putting $\beta = \alpha + \varphi(\alpha) + \ldots + \varphi^{d-1}(\alpha)$, with d taken to be the smallest such non-negative integer, show that φ is a $\mathbb{Q}(\beta)$-homomorphism of L.

Solution: We have that for each non-negative integer n, the element $\varphi^n(\alpha)$ of L is a root of $m_\alpha(\mathbb{Q})$. But the degree of the latter polynomial is a positive integer, say m. Thus, when $n \geq m$, it follows from the pigeon-hole principle that there exist integers i and j with $0 \leq i < j \leq n$ for which $\varphi^i(\alpha) = \varphi^j(\alpha)$. But φ is a homomorphism of fields, and hence injective, so that $\varphi^{j-i}(\alpha) = \alpha$. Putting $d = j - i$, we consequently find that d is a positive integer with $\varphi^d(\alpha) = \alpha$.

Now let d be the smallest positive integer with the property that $\varphi^d(\alpha) = \alpha$, and observe that then $\varphi(\beta) = \varphi(\alpha) + \varphi^2(\alpha) + \ldots + \varphi^d(\alpha) = \varphi(\alpha) + \varphi^2(\alpha) + \ldots + \varphi^{d-1}(\alpha) + \alpha = \beta$. So β, and hence also $\mathbb{Q}(\beta)$, is fixed by φ, whence φ is a $\mathbb{Q}(\beta)$-homomorphism of L.

6. [7+7=14 points] With t an indeterminate, let $f \in \mathbb{Z}[t]$ be a polynomial of degree $n \geq 1$, and put $K = \mathbb{Q}(f)$.

(a) Find a polynomial $F \in K[X]$ satisying the property that $F(t) = 0$, and hence deduce that the field extension $\mathbb{Q}(t) : K$ is algebraic of degree at most n.

Solution: Put $F(X) = f(X) - f(t) \in K[X]$. Then we have $F(t) = f(t) - f(t) = 0$, so that $m_t(K)$ divides $F(X)$. But $K = \mathbb{Q}(f) \subseteq \mathbb{Q}(t)$, so $[\mathbb{Q}(t) : K] = \deg(m_t(K)) \leq \deg(F) = \deg(f) = n$, and we conclude that $\mathbb{Q}(t) : K$ is an algebraic extension of degree at most n.

(b) Let $g \in \mathbb{Z}[t]$ be a polynomial distinct from f. By considering $m_g(K)$, or otherwise, show that there exists a non-zero polynomial $H(X,Y) \in \mathbb{Z}[X,Y]$ with the property that $H(f(t), g(t)) = 0$.

Solution: We have $g \in \mathbb{Q}(t)$, where $\mathbb{Q}(t) : K$ is an algebraic extension. Let $h = m_g(K)$ be the minimal polynomial of g over K. Then for some positive integer m, we have $h(X) = h_0 + h_1 X + \ldots + h_m X^m$, where each $h_i \in K$ is a quotient of polynomials in f with coefficients from $\mathbb{Q}$. Note that $h(g) = 0$. Multiply $h(X)$ through by the product of all denominators of the h_i to obtain $h^*(X) \in (\mathbb{Q}[f])(X)$ for which $h^*(g) = 0$. The latter relation is equivalent to a polynomial equation $H^*(f, g) = 0$ with $H^* \in \mathbb{Q}[X,Y]$. Finally, multiply through by the product of the denominators of the rational coefficients from $\mathbb{Q}$ in H^* to give a non-zero polynomial $H \in \mathbb{Z}[X,Y]$ for which $H(f, g) = 0$.

End of examination.