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.

©Trevor D. Wooley, Purdue University 2024. This material is copyright of Trevor D. Wooley at Purdue University unless explicitly stated otherwise. It is provided exclusively for educational purposes at Purdue University, and is to be downloaded or copied for your private study only.

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY – SOLUTIONS

MA 45401-H01

28th March 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. Let $f \in \mathbb{Z}[t]$ be a polynomial, every root of which has multiplicity 2024. Then f is not separable over $\mathbb{Q}$.

   Solution: False – consider, for example, the polynomial $(t-1)^{2024}$, each irreducible factor of which is linear and hence separable over $\mathbb{Q}$.

   b. If $L : K$ is an algebraic extension of fields with $K \subseteq L$, then the algebraic closure $\overline{L}$ of L is isomorphic to the algebraic closure $\overline{K}$ of K.

   Solution: True – we have that $\overline{K}$ and $\overline{L}$ are both algebraic closures of K, and so Proposition 4.9 shows that $\overline{L}$ is isomorphic to $\overline{K}$.

   c. Every algebraic extension of $\mathbb{Q}$ is separable.

   Solution: True – this is a result from class (and holds more generally for every field K of characteristic 0).

   d. Suppose that K and L are fields with $K \subseteq L$, and L is algebraically closed. Then the field extension $L : K$ is normal.

   Solution: False – consider, for example $\mathbb{Q} \subseteq \mathbb{C}$. The extension $\mathbb{C} : \mathbb{Q}$ is not normal, because this extension is not algebraic.

   e. Suppose that $L : M$ and $M : K$ are field extensions with $L : K$ normal. Then $L : M$ is a normal field extension.

   Solution: True – this is a result from class (Proposition 6.3).

   f. Let $f \in \mathbb{Z}[x]$ be a polynomial having prime degree p, and let θ be any root of f in a splitting field extension for f over $\mathbb{Q}$. Then $[\mathbb{Q}(\theta) : \mathbb{Q}] = p$.

   Solution: False – consider $f(x) = x^p$, so that $\theta = 0$ and $[\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1$.

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

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

   Solution: Suppose that $M : K$ is a field extension relative to the embedding $\varphi : K \to M$, and $S \subseteq K[t] \setminus K$ has the property that every $f \in S$ splits over M. Let L be a field with $\varphi(K) \subseteq L \subseteq M$. Then $L : K$ *is a splitting field extension for* S if L is the smallest subfield of M containing $\varphi(K)$ over which every polynomial $f \in S$ splits. [Full credit if you assumed that $K \subseteq M$, and worked with a single polynomial instead of a set.]

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

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

   (c) Let $L : K$ be a field extension. Define what it means for an element $\alpha \in L$ to be separable over K.

   Solution: An element $\alpha \in L$ is *separable* over K when α is algebraic over K and its minimal polynomial $m_\alpha(K)$ is separable (meaning that it has no multiple roots in $\overline{K}$).

Continued...

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

Solution: An algebraic extension $L : K$ is *separable* if every $\alpha \in L$ is separable over K.

3. [8+8+8=24 points] This question concerns the polynomial $f(t) = t^4 - (t+1)^2 \in \mathbb{Q}[t]$.

(a) Find a splitting field extension $L : \mathbb{Q}$ for f, justifying your answer.

Solution: Working over $\overline{\mathbb{Q}}$, one finds that $f(t) = t^4 - (t+1)^2 = (t^2 - t - 1)(t^2 + t + 1)$, and hence $f(t) = (t - \frac{1}{2}(1+\sqrt{5}))(t - \frac{1}{2}(1-\sqrt{5}))(t + \frac{1}{2}(1+\sqrt{-3})(t + \frac{1}{2}(1-\sqrt{-3}))$. Thus, on taking $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$, we find that $L : \mathbb{Q}$ is a splitting field extension for f.

(b) Determine the degree of your splitting field extension $L : \mathbb{Q}$, justifying your answer.

Solution: We have $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, since the minimal polynomial for $\sqrt{5}$ over $\mathbb{Q}$ is $t^2 - 5$. The minimal polynomial for $\sqrt{-3}$ over $\mathbb{Q}(\sqrt{5})$ divides $t^2 + 3$. Since $\sqrt{-3} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$, one sees that t^2+3 has no root in $\mathbb{Q}(\sqrt{5})$, and hence is irreducible over $\mathbb{Q}(\sqrt{5})$. Thus $[L : \mathbb{Q}(\sqrt{5})] = 2$, and so $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$, by the tower law.

(c) Determine the subgroup of S_4 to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.

Solution: The group $G = \mathrm{Gal}(L : \mathbb{Q})$ can be identified by extension of $\mathbb{Q}$-homorphisms, first the inclusion map $\mathbb{Q} \to L$ to a $\mathbb{Q}$-homomorphism $\mathbb{Q}(\sqrt{5}) \to L$, and then to a $\mathbb{Q}$-homomorphism $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3}) \to L$. The first extension is defined by an action permuting the roots $\sqrt{5}$ and $-\sqrt{5}$ of the irreducible polynomial $t^2 - 5$ defining the extension $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$. The second is defined by an action permuting the roots $\sqrt{-3}$ and $-\sqrt{-3}$ of the irreducible polynomial $t^2 + 3$ defining the extension $L : \mathbb{Q}(\sqrt{5})$. Thus we see that G is generated by permutations σ, τ and $\sigma\tau = \tau\sigma$ on the roots $\pm\sqrt{5}$ and $\pm\sqrt{-3}$ of the polynomial f, where these maps fix $\mathbb{Q}$ pointwise, and $\sigma = (\sqrt{5}, -\sqrt{5})$ and $\tau = (\sqrt{-3}, -\sqrt{-3})$. Thus $\sigma\tau = \tau\sigma = (\sqrt{5}, -\sqrt{5})(\sqrt{-3}, -\sqrt{-3})$, and $G \cong \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leq S_4$.

4. [14 points] Suppose that $L : K$ is a splitting field extension for the polynomial $f \in K[t] \setminus K$. Prove that $[L : K]$ divides $(\deg f)!$.

Solution: We proceed by induction on $n = \deg(f)$, noting that the case $n = 1$ is immediate. Now, when $n > 1$, we split the argument according to whether f is reducible or not over K. If f is irreducible, let $\alpha \in L$ be any root of f. Then f factors as $(t - \alpha)g$ for some other polynomial $g \in K(\alpha)[t]$ of degree $n - 1$. Moreover, we have that L is a splitting field for g over $K(\alpha)$. By induction, we therefore see that $[L : K(\alpha)]$ divides $(n-1)!$. Since $[K(\alpha) : K] = n$, the Tower Law shows that $[L : K]$ divides $n \cdot (n-1)! = n!$.

On the other hand, if $f = gh$ is reducible, let M be the subfield of L generated by K and the roots of g. Then M is a splitting field for g over K and L is a splitting field for h over M. By induction, we have that $[M : K]$ divides $r!$ and $[L : M]$ divides $(n-r)!$, where $r = \deg(g)$. Hence $[L : K] = [L : M][M : K]$ divides $r!(n-r)!$, which in turn divides $n!$ (with quotient equal to the binomial coefficient $\binom{n}{r}$).

We have confirmed the inductive step in both cases, and the desired conclusion follows.

5. [7+7=14 points] (a) Suppose that M is an algebraically closed field. Show that all polynomials in $M[t]$ are separable.

Continued...

Solution: Suppose that $f \in M[t]$ is irreducible and $\deg(f) > 1$. Then f is non-zero and non-constant and has a root $\alpha \in M$. Define $g \in M[t]$ by means of the relation $f = (t - \alpha)g$. Then g has degree $\deg(f) - 1 \geq 1$, and thus f is not irreducible over $M[t]$, leading to a contradiction. Thus, every irreducible polynomial in $M[t]$ has degree 1. Such a polynomial cannot have multiple roots, and so must be separable. Every polynomial in $K[X]$ is therefore a product of separable polynomials, and must consequently itself be separable.

(b) Suppose that p is a prime number and t is an indeterminate, and let $L = \overline{\mathbb{F}}_p(t)$, where $\overline{\mathbb{F}}_p$ denotes the algebraic closure of $\mathbb{F}_p$. Are all polynomials in $L[X]$ separable? Justify your answer.

Solution: No, not all polynomials in $L[X]$ separable. Consider, for example, the polynomial $f = X^p - t \in L[X]$, and let $\alpha \in \overline{L}$ be a root of f. Thus, we have $\alpha^p = t$. We show first that f is irreducible over L. Since t is irreducible in $\overline{\mathbb{F}}_p[t]$, it follows from Eisenstein's criterion via Gauss's Lemma that f is irreducible over $\overline{\mathbb{F}}_p(t) = L$. Finally, to see that f is not separable over L, we use the fact that $\mathrm{char}(K) = p$ and p divides the binomial coefficients $\binom{p}{k}$ for $1 \leq k < p$. Hence $(X - \alpha)^p = X^p - t$. Thus α is the only root of f, even though f is irreducible over L with $\deg f = p > 1$, and so f is not separable.

6. [8+8=16 points] Throughout, let f denote the polynomial $t^5 - 9t - 3 \in \mathbb{Q}[t]$, let L be a splitting field for f over $\mathbb{Q}$, and let M be a field with $\mathbb{Q} \subsetneq M \subsetneq L$ (that is, a field strictly intermediate between $\mathbb{Q}$ and L).

(a) Show that, for any $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$, and for any $\alpha \in M$, the polynomial $\sigma(m_\alpha(\mathbb{Q}))$ is monic and irreducible over $\mathbb{Q}$. Here $m_\alpha(\mathbb{Q})$ denotes the minimal polynomial of α over $\mathbb{Q}$.

Solution: Suppose that $\alpha \in M$. Then $m_\alpha(\mathbb{Q})$ is monic and irreducible over $\mathbb{Q}$. Since σ is a homomorphism, we know that $\sigma(1) = 1$. Thus $\sigma(m_\alpha(\mathbb{Q}))$ is monic. Also, if $\sigma(m_\alpha(\mathbb{Q}))$ has a proper factorisation $g_1 g_2$, say, then $\sigma^{-1}(g_1) \cdot \sigma^{-1}(g_2)$ gives a factorisation of $m_\alpha(\mathbb{Q})$ over $\mathbb{Q}$, contradicting the irreducibility of $m_\alpha(\mathbb{Q})$. Thus $\sigma(m_\alpha(\mathbb{Q}))$ is indeed irreducible.

(b) Suppose that $M : \mathbb{Q}$ is normal and that f factors as a product of monic irreducibles $f_1, \ldots, f_r$ (of positive degree) over $M[t]$. Show that $\deg(f_i) = \deg(f_1)$ for each i.

Solution: Let $\alpha \in L$ be a root of f_1 and $\beta \in L$ be a root of f_i. Since f_1 and f_i are monic and irreducible over $M[t]$, we have $f_1 = m_\alpha(M)$ and $f_i = m_\beta(M)$. Also, since f is irreducible over $\mathbb{Q}$, there is some $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ with $\sigma(\alpha) = \beta$. We have $0 = \sigma(f_1(\alpha)) = \sigma(f_1)(\beta)$. Since $M : K$ is normal, it follows from Theorem 6.4 that $\sigma(M) \subseteq M$, so that $\sigma(f_1) \in M[t]$. Then $\sigma(f_1)$ is a monic polynomial divisible by $m_\beta(M) = f_i$. So $\deg(f_1) \geq \deg(f_i)$. Applying this argument with σ^{-1} in place of σ, we see that $\deg(f_i) \geq \deg(f_1)$. Consequently, we have $\deg(f_i) = \deg(f_1)$ for all i.

(c) Show that if $M : \mathbb{Q}$ is normal, then f remains irreducible over M.

Solution: Observe that $\deg(f) = 5$, and so the proposed factorisation implies that $r \deg(f_1) = 5$, whence $\deg(f_i) = 1$ for all i, or $\deg(f_1) = 5$ and $r = 1$. In the former case, the field M is equal to the splitting field L of f over $\mathbb{Q}$, contradicting that M is a proper intermediate field. In the latter case, we see that f remains irreducible over M.

End of examination.