UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level M)

GALOIS THEORY SOLUTIONS

MATH 2700

(Paper Code MATHM-2700)

January 2016, 2 hours 30 minutes

This paper contains **four** *questions*
All **FOUR** *questions should be attempted.*

Calculators are **not** *permitted in this examination.*

Do not turn over until instructed.

[H]=standard, from class, or similar to homework, [B]=bookwork, [U]=unseen

1. (a) (2+2+3+3=10 marks) [B+B+U+B] Suppose that $K \subseteq L$ are fields.

(i) Define $[L : K]$, the degree of the field extension $L : K$.

Solution: $[L : K]$ is the dimension of L as a vector space over K.

(ii) Define what it means for $L : K$ to be an algebraic extension.

Solution: $L : K$ is an algebraic extension if every element of L is algebraic over K; that is, for each $\alpha \in L$, there is some non-trivial polynomial $f \in K[t]$ for which $f(\alpha) = 0$.

(iii) Show that when $1 < [L : K] < \infty$, then there exists $\beta \in L$ for which

$$[L : K(\beta)] < [L : K].$$

Solution: The hypothesis $[L : K] > 1$ ensures that there exists an element $\beta \in L \setminus K$. But then if $[K(\beta) : K] = d$, we have $d \geq 2$. Thus, by the Tower Law, one finds that

$$[L : K] = [L : K(\beta)][K(\beta) : K] = d[L : K(\beta)],$$

whence $[L : K(\beta)] = [L : K]/d \leq [L : K]/2 < [L : K]$.

(iv) Suppose that $[L : K] < \infty$. Show that there exist elements $\alpha_1, \dots \alpha_n \in L$ for which $L = K(\alpha_1, \dots, \alpha_n)$.

Solution: If $L = K$ then we are done. We proceed by induction on $[L : K]$, with the trivial case $L = K$ as the basis. Suppose that the desired conclusion holds whenever $[L : K] < N$, and consider the situation with $[L : K] = N > 1$. From part (c), there exists $\alpha_1 \in L$ with $[L : K(\alpha_1)] < N$. But then the inductive hypothesis ensures that there exist $\alpha_2, \dots, \alpha_n \in L$ for which $L = K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n)$, confirming the inductive step.

(b) (2+5=7 marks) [B+U] (i) Define what it means for a field extension $L : K$ to be an algebraic closure.

Solution: The extension $L : K$ is an algebraic closure if it is an extension of K in which the elements of S split, for all $S \subseteq L[X]$.

(ii) Suppose that M is an algebraically closed field. Show that every irreducible polynomial in $M[t]$ has degree 1.

Solution: Suppose that $f \in M[t]$ is irreducible. Since M is algebraically closed, there is a root α of f lying in M. By uniqueness of polynomial factorisation, we see that f is divisible by $t-\alpha$ over $M[t]$, whence $f = (t-\alpha)g$ for some $g \in M[t]$. But f is irreducible, so g must be a unit, which is to say that $g \in M$. So $\deg(f) = \deg(t - \alpha) = 1$.

(c) (5+3=8 marks) [B+ B] (i) Suppose that $L : M : K$ is a tower of field extensions. Prove that whenever $L : K$ is separable, then both $L : M$ and $M : K$ are separable.

Solution: First, the separability of $M : K$ is inherited from that of $L : K$, since whenever $\alpha \in M$, then $\alpha \in L$. Next we show that $L : M$ is separable. Suppose that $\alpha \in L$, and let $m_{\alpha,M}$ denote its minimal polynomial over M, and $m_{\alpha,K}$ that over K. Let $N : M$ be a splitting field extension for $m_{\alpha,K}$ considered as a polynomial in $M[x]$. Since $m_{\alpha,K}$ is separable over K, we have $m_{\alpha,K} = (x - \alpha_1) \dots (x - \alpha_r)$, for suitable distinct $\alpha_1, \dots, \alpha_r \in N$. But $m_{\alpha,M} | m_{\alpha,K}$ in $M[x]$, so $m_{\alpha,M} = (x-\alpha_{i_1}) \dots (x-\alpha_{i_s})$, for some distinct $\alpha_{i_1}, \dots, \alpha_{i_s} \in N$. Then $m_{\alpha,M}$ is separable, and hence $L : M$ is separable.

Continued...

(ii) Suppose that $L : E : K$ and $L : F : K$ are towers of field extensions with $E : K$ and $F : K$ separable. Show that $E \cap F : K$ is a separable extension.
Solution: The field $E \cap F$ is contained in E, so $E : E \cap F : K$ is a tower of field extensions with $E : K$ separable. Then it follows from (i) that $E \cap F : K$ is separable.

2. (a) (3+3 marks) [B+U/H] (i) State Eisenstein's criterion for irreducibility of polynomials in $\mathbb{Z}[t]$.
Solution: Suppose that $f = f_0 + f_1 t + \cdots + f_n t^n \in \mathbb{Z}[t]$ satisfies the condition that the coefficients $f_0, \ldots, f_n$ have no common factor. Suppose further that for some prime number p one has $p | f_i$ $(0 \leq i < n)$, $p \nmid f_n$ and $p^2 \nmid f_0$. Then f is irreducible over $\mathbb{Z}$.
(ii) Determine whether or not the polynomial $5t^5 - 40t - 2$ is irreducible over $\mathbb{Z}$, and explain your reasoning.
Solution: We apply Eisenstein's criterion with $p = 2$, noting that the coefficients of the polynomial in question have no common factor, and that all but the lead coefficient are divisible by 2, and further that the constant coefficient is not divisible by 4. Thus $5t^5 - 40t - 2$ is indeed irreducible.

(b) (4+2=6 marks) [B] Let $f \in \mathbb{Q}[t]$ be irreducible, suppose that L is a splitting field for f over $\mathbb{Q}$, and suppose that $L : M : \mathbb{Q}$ is a tower of field extensions. Prove that the field extension $L : M$ is normal, and deduce that it is Galois.
Solution: The field extension $L : M$ is normal and finite if and only if L is a splitting field extension for some polynomial $g \in M[x]$. But $f \in M[x]$, and L is a splitting field extension for f, so $L : M$ is normal. Any field extension in characteristic 0 is separable, and so $L : M$ is also separable. Since $L : M$ is both normal and separable, it is Galois.

(c) (3+3=6 marks) [B] Let K be a field. Suppose that $f \in K[t]$ is irreducible, and suppose that L is a splitting field for f over K. Briefly explain why, whenever $\alpha, \beta \in L$ and $f(\alpha) = 0 = f(\beta)$, then $K(\alpha) \simeq K(\beta)$. Hence deduce that there exists $\tau \in \mathrm{Gal}(L : K)$ such that $\tau(\alpha) = \beta$.
Solution: Without loss of generality, we may suppose that f is monic. The minimal polynomial α over K is $m_{\alpha,K} = f$, and likewise $m_{\beta,K} = f$. Thus, the fields $K(\alpha) \simeq K[t]/(f)$ and $K(\beta) \simeq K[t]/(f)$ are isomorphic. The identity mapping $\mathrm{id}_K : K \to K$ can therefore be extended to an isomorphism $\sigma : K(\alpha) \to K(\beta)$ with $\sigma(\alpha) = \beta$. By uniqueness of splitting fields, one can extend σ to an isomorphism $\tau : L \to L$. But then $\tau(\alpha) = \sigma(\alpha) = \beta$.

(d) (2+5=7 marks) [U+U] Throughout, let $f = t^5 - 8t - \frac{2}{5}$, let L be a splitting field for f over $\mathbb{Q}$, and let M be a field with $\mathbb{Q} \subsetneq M \subsetneq L$.
(i) 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. Here $m_{\alpha,\mathbb{Q}}$ denotes the minimal polynomial of α over $\mathbb{Q}$.
Solution: Note from part (a) and Gauss' Lemma that f is irreducible over $\mathbb{Q}$. The polynomial f is monic. Since σ is a homomorphism, we know that $\sigma(1) = 1$. Thus $\sigma(f)$ is monic. Also, if $\sigma(m_{\alpha,K})$ has a proper factorisation $g_1 g_2$, say, then $\sigma^{-1}(g_1) \cdot \sigma^{-1}(g_2)$ gives a factorisation of f over $\mathbb{Q}$ that contradicts the irreducibility of f. Thus $\sigma(m_{\alpha,K})$ is indeed irreducible.

Continued...

(ii) Suppose that $M : \mathbb{Q}$ is Galois and that f factors as a product of monic irreducibles $f_1, \ldots, f_r$ over $M[t]$. Show that $\deg(f_i) = \deg(f_1)$ for each i, and hence deduce that f remains irreducible over M.

Solution: Let $\alpha \in L$ be a root of f_1. Suppose that $\alpha_i \in L$ is a root of f_i. Then there is some $\sigma \in \mathrm{Gal}(L : K)$ so that $\sigma(\alpha) = \alpha_i$. Thus $0 = \sigma(f_1(\alpha)) = \sigma(f_1)(\alpha_i)$. Since $\sigma(f_1)$ is a monic irreducible element of $M[t]$ having α_i as a root, then $\sigma(f_1)$ is the minimal polynomial for α_i over M. In particular, we have $\deg(f_i) = \deg(f_1)$ for all i. But $\deg(f) = 5$, and so the proposed factorisation implies $r \deg(f_1) = 5$, 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.

3. (a) (10 marks)[B] Define what it means for a field extension $L : K$ to be

(i) normal: *Solution:* An extension $L : K$ is normal if $L : K$ is algebraic and, for any irreducible polynomial $f \in K[X]$, either f has no root in L, or f splits in L.

(ii) a splitting field extension: *Solution:* The extension $L : K$ is a splitting field extension if it is a minimal extension of K in which the elements of S split, for some $S \subseteq K[X]$.

(iii) separable: *Solution:* An extension $L : K$ is separable if every element of L is algebraic over K, and each element has a minimal polynomial f over K, say of degree n, which has n distinct roots in a splitting field for f over K.

(iv) finite: *Solution:* An extension $L : K$ is finite if, viewed as a K-vector space, the field L has finite dimension.

(v) Galois: *Solution:* An extension $L : K$ is Galois if it is finite, normal and separable.

(b) (15 marks) Indicate whether each of the following statements is always true or can be false. For those that are false, please provide a short (one or two sentence) justification. Each fully correct answer is worth 1 mark.

(i) Every algebraic extension of $\mathbb{Q}$ is separable.

Solution: [B] True.

(ii) If $L : K$ is an extension of fields, then the algebraic closure $\overline{L}$ of L is equal to the algebraic closure $\overline{K}$ of K.

Solution: [B] False. Consider $L = \mathbb{R}$ and $K = \mathbb{Q}$. Whenever $\xi \in \mathbb{R}$ is transcendental (not algebraic) over $\mathbb{Q}$, for example $\xi = \pi$, then the element $\xi \in \mathbb{R} \subset \overline{\mathbb{R}} = \mathbb{C}$ does not lie in $\overline{\mathbb{Q}}$, the set of algebraic numbers.

(iii) Every field extension of finite degree is normal.

Solution: [B] False. A field extension $\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}$ is finite, but the minimal polynomial for $\sqrt[3]{5}$ does not split over $\mathbb{Q}(\sqrt[3]{5})$.

(iv) There is an isomorphism $\varphi : \mathbb{Q}(\sqrt[4]{11}) \to \mathbb{Q}(i\sqrt[4]{11})$, where we write $i = \sqrt{-1}$.

Solution: [U] True.

(v) Suppose that K is a field of characteristic p. If $L : K$ is a field extension and $\tau \in L$ is transcendental over K, then τ^p is transcendental over L.

Solution: [B] False. Since $\tau \in L$, one has $\tau^p \in L$, and hence $[L(\tau^p) : L] = [L : L] = 1$. Thus τ^p is trivially algebraic over L.

Continued...

(vi) Let $L : \mathbb{Q}$ be a field extension, and suppose that K_1 and K_2 are subfields of L with the property that $[K_1 : \mathbb{Q}]$ and $[K_2 : \mathbb{Q}]$ are coprime. Then $K_1 \cap K_2 = \mathbb{Q}$.

Solution: [U] True.

(vii) Suppose that $f \in K[t] \setminus \{0\}$, and that $\beta \in \overline{K}$ has the property that $f(\beta) = 0$. Then f is an element of the ideal generated by the minimal polynomial of β over K.

Solution: [B] True.

(viii) When p is an odd prime, any splitting field of a degree p irreducible polynomial in $\mathbb{F}_p[t]$ has degree $p!$ over $\mathbb{F}_p$.

Solution: [U] False. Consider the polynomial $f = x^p - x + 1$, which is irreducible over $\mathbb{F}_p$, since $a^p = a$ for all $a \in \mathbb{F}_p$. Let $L : \mathbb{F}_p$ be a splitting field extension for f, and denote by θ any root of f in L. Then the roots of f are $\theta, \theta + 1, \ldots, \theta + p - 1$, and so $[L : \mathbb{F}_p] = [\mathbb{F}_p(\theta) : \theta] = p$. When $p > 2$, one has $p! > p$, and so we contradict the assertion made in the question.

(ix) Let $f \in \mathbb{Q}[x]$ be cubic and irreducible, and suppose that f has a root α in a splitting field L for f over $\mathbb{Q}$. Then there exists $\beta \in L$ with $\mathbb{Q}(\alpha, \alpha^2, \alpha^3) = \mathbb{Q}(\beta)$.

Solution: [U] True.

(x) 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: [U] False. Consider $f(x) = x^p$. Then $\theta = 0$ and $[\mathbb{Q}(\theta) : \mathbb{Q}] = 1 \neq p$.

(xi) Suppose that $L : M$ and $M : K$ are field extensions, and the field extension $L : K$ is normal. Then $M : K$ is normal.

Solution: [B] False. Let $\alpha = \sqrt[3]{2}$ and let ω be a primitive cubic root of unity. Put $L = \mathbb{Q}(\alpha, \omega)$, $M = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}$. Then $L : \mathbb{Q}$ is normal, since L is a splitting field for the polynomial $t^3 - 2$ over $\mathbb{Q}$. But $M : K$ is not normal, since $t^3 - 2$ is the minimal polynomial for α over $\mathbb{Q}$, yet does not split over M.

(xii) When p is a prime number, then for every multiple n of p there exists a field extension $K : \mathbb{F}_p$ such that $\mathrm{card}(K) = n$.

Solution: [U] False. Every such extension of finite degree has the property that $\mathbb{F}_p$ is finite, hence has order equal to a power of p. Then it is impossible that $\mathrm{card}(K) = 6p$, for example.

(xiii) If $L : \mathbb{Q}$ is a cyclic field extension, then the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ is cyclic.

Solution: [B] True.

(xiv) Suppose that $M : L$ and $L : K$ are finite Galois extensions. Then $M : K$ is a Galois extension.

Solution: [B] False. For example, consider $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$. These are both finite extensions, and separable since $\mathrm{char}(\mathbb{Q}) = 0$. They are also normal, since they are splitting fields for the respective polynomials $t^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})(t)$ and $t^2 - 2 \in \mathbb{Q}(t)$. But $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ is not normal, since $m_{\sqrt[4]{2},\mathbb{Q}}(t) = t^4 - 2$, which does not split over $\mathbb{Q}(\sqrt[4]{2})$ (note: $i\sqrt[4]{2}$ is a root not contained in $\mathbb{Q}(\sqrt[4]{2})$).

(xv) Suppose $M : L$ and $L : K$ are finite Galois extensions. Then

$$\mathrm{Gal}(M : L) \lhd \mathrm{Gal}(M : K).$$

Solution: [B] True.

Continued...

4. (a) (4 marks) [B] State the Fundamental Theorem of Galois Theory.

Solution: Suppose that $L : K$ is finite. Let $G = \mathrm{Gal}(L : K)$, and let $K_0 = \phi(G)$, the set of elements of L fixed by the action of G. Also, when M is a field intermediate between L and K_0, let $\gamma(M) = \mathrm{Gal}(L : M)$. Then (i) The map ϕ from the set of subgroups of G onto the set of fields intermediate between L and K_0 is injective, and γ is the inverse map; (ii) A subgroup H of G is normal if and only if $\phi(H) : K_0$ is a normal extension; (iii) Suppose that $H \lhd G$. Then whenever $\sigma \in G$, one has $\sigma|_{\phi(H)} \in \mathrm{Gal}(\phi(H) : K_0)$. Furthermore, the map $\sigma \to \sigma|_{\phi(H)}$ is a homomorphism of G onto $\mathrm{Gal}(\phi(H) : K_0)$ with kernel H, so that $\mathrm{Gal}(\phi(H) : K_0) \simeq G/H$.

(b) (3+4+2=9 marks) [B+B+H] Let p be a prime number , let K be the finite field having p elements, and let L be a field extension of K with $|L| = p^n$.

(i) Show that $a^{p^n} = a$ for all elements $a \in L$, and deduce that $L : K$ is a splitting field extension for $x^{p^n} - x$.

Solution: The group $L^\times$ has order $p^n - 1$, and hence it follows from Lagrange's theorem that whenever $a \neq 0$, then $a^{p^n-1} = 1$. Thus $a^{p^n} = a$ whenever $a \neq 0$, a relation that is trivial for $a = 0$. We deduce that the polynomial $x^{p^n} - x$ has as roots precisely the p^n elements of L, so that L is a splitting field for $x^{p^n} - x$.

(ii) Define the Frobenius map ϕ on L, and deduce that $\mathrm{Gal}(L : K) = \langle\phi\rangle$.

Solution: The Frobenius map $\sigma : L \to L$ is defined by $\sigma(\alpha) = \alpha^p$, where p is the characteristic of K. The extension $L : K$ is a splitting field extension, and hence normal, and is also separable from (i) (alternatively, the latter follows since L is algebraic over its prime subfield). Thus $L : K$ is Galois and $|\mathrm{Gal}(L : K)| = [L : K] = n$. One has $\phi \in \mathrm{Gal}(L : K)$. Let $d = \mathrm{ord}(\phi)$, and note that since $\phi \in \mathrm{Gal}(L : K)$ and $|\mathrm{Gal}(L : K)| = n$, then $d \leq n$. Thus, for all $\alpha \in L$, we have $\alpha = \phi^d(\alpha) = \alpha^{p^d}$, so that every one of the p^n elements of L is a root of the polynomial $x^{p^d} - x$. But this polynomial can have at most p^d roots, and so $d = n$. Then $|\langle\phi\rangle| = n = |\mathrm{Gal}(L : K)|$, whence $\langle\phi\rangle = \mathrm{Gal}(L : K)$.

(iii) Noting that $\langle\phi\rangle \simeq \mathbb{Z}/n\mathbb{Z}$, show that there can exist a subfield of L having p^d elements only when $d|n$.

Solution: Since $\mathrm{Gal}(L : K) = \langle\phi\rangle \simeq \mathbb{Z}/n\mathbb{Z}$, it follows that $\mathrm{Gal}(L : K)$ can have a subgroup of index d only when $d|n$. But by the Fundamental Theorem of Galois Theory, there can be a subfield M of L with $[M : K] = d$ only when $\mathrm{Gal}(L : K)$ has a subgroup of index d. Thus, a subfield M of L having p^d elements can exist only when $d|n$.

(c) (4+4+4 marks) [≈ H+U] Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = X^3 - 3$.

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

Solution: One has $L = \mathbb{Q}(\alpha, \omega)$, where $\alpha = \sqrt[3]{3}$ and $\omega = (-1 + \sqrt{-3})/2$ is a primitive cubic root of unity. The polynomial f is irreducible by Eisenstein's criterion, using the prime 3, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Further, one has $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, since ω is a root of $\Phi_3 = X^2 + X + 1$, which is irreducible over $\mathbb{Q}$. So $[L : \mathbb{Q}(\alpha)] = 1$ or 2. But $\omega \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, so that $X^2 + X + 1$ must be irreducible over $\mathbb{Q}(\alpha)$. Hence $[L : \mathbb{Q}(\alpha)] = 2$, and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Continued...

(ii) Describe the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).

Solution: The Galois group $\mathrm{Gal}(L : \mathbb{Q})$ is generated by σ and τ, where σ and τ leave $\mathbb{Q}$ fixed pointwise, and $\sigma(\alpha) = \omega\alpha$ and $\sigma(\omega) = \omega$, and $\tau(\alpha) = \alpha$ and $\tau(\omega) = \omega^2$. Thus $\sigma\tau(\alpha) = \tau\sigma^2(\alpha) = \omega\alpha$ and $\sigma\tau(\omega) = \tau\sigma^2(\omega) = \omega^2$. Then

$$\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau : \sigma^3 = 1,\, \tau^2 = 1,\, \sigma\tau = \tau\sigma^2 \rangle \simeq D_3.$$

.

(iii) Apply the Fundamental Theorem of Galois Theory to find all fields M for which $\mathbb{Q} \subsetneq M \subsetneq L$, explaining carefully how you applied the Fundamental Theorem in this process.

Solution: We know that $\mathrm{Gal}(L : \mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. The fields M that we are to find are the fixed fields of the subgroups $H_1 = \langle\sigma\rangle$, $H_2 = \langle\tau\rangle$, $H_3 = \langle\sigma\tau\rangle$ and $H_4 = \langle\sigma^2\tau\rangle$. With M_i the fixed field of H_i, we have $M_1 = \mathbb{Q}(\omega)$, $M_2 = \mathbb{Q}(\alpha)$, $M_3 = \mathbb{Q}(\omega^2\alpha)$ and $M_4 = \mathbb{Q}(\omega\alpha)$. Notice here that the Fundamental Theorem of Galois Theory shows that $[M_i : \mathbb{Q}] = |\mathrm{Gal}(L : \mathbb{Q})|/|H_i|$. Consequently, having identified an element in the fixed field M_i of H_i, one can check to see if this generates the whole fixed field. For example, one sees that $\omega^2\alpha$ is fixed by $\sigma\tau$, and

$$[M_3 : \mathbb{Q}] = 6/|\langle\sigma\tau\rangle| = 6/2 = 3 = [\mathbb{Q}(\omega^2\alpha) : \mathbb{Q}],$$

whence $M_3 = \mathbb{Q}(\omega^2\alpha)$.

End of examination.