UNIVERSITY OF BRISTOL

School of Mathematics

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

GALOIS THEORY
MATH M2700
(Paper Code MATH-M2700J)

January 2017, 2 hours 30 minutes

SOLUTIONS

[B]=Bookwork, [H]=homework, [U]=unseen

This paper contains **four** *questions.*
Answers to all **FOUR** *questions will be used for assessment.*

On this examination, the marking scheme is indicative and is intended only as a guide to the relative weighting of the questions.

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

Do not turn over until instructed.

1. (a) (2+2+3=7 marks) Suppose that $K \subseteq L$ are fields.

(i) Define what it means for the element $\alpha \in L$ to be *algebraic* over K, and what it means for the element $\beta \in L$ to be *transcendental* over K.

Solution: [B] The element $\alpha \in L$ is algebraic over K if there exists some non-trivial polynomial $f \in K[t]$ for which $f(\alpha) = 0$. The element $\beta \in L$ is transcendental over K if there exists no non-trivial polynomial $g \in K[t]$ for which $g(\beta) = 0$.

(ii) Suppose that M is a field satisfying $K \subseteq M \subseteq L$. Define what it means for $M : K$ to be a *simple* field extension.

Solution: [B] The field extension $M : K$ is simple if there exists $\alpha \in L$ with the property that $M = K(\alpha)$.

(iii) Suppose that $\gamma \in L$ is transcendental over K. Define what is meant by the field $K(\gamma)$, and give an explicit description of its elements.

Solution: [B] The field $K(\gamma)$ is the smallest field containing both K and γ, namely the set of all elements of the shape

$$\frac{a_0 + a_1\gamma + \ldots + a_n\gamma^n}{b_0 + b_1\gamma + \ldots + b_n\gamma^n},$$

with $a_i, b_i \in K$ for each i, and with $b_0 + b_1\gamma + \ldots + b_n\gamma^n \neq 0$.

(b) (7 marks) Suppose that $\alpha \in L$ is algebraic over K but does not lie in K, and $\beta \in L$ is transcendental over K. Show that $K(\alpha, \beta) : K$ is *not* a simple extension.

Solution: [U] Suppose, if possible, that $K(\alpha, \beta) : K$ is a simple extension, say $K(\alpha, \beta) = K(\gamma)$ for some element $\gamma \in K(\alpha, \beta)$. Since, by hypothesis, one has $\alpha \notin K$, and $\alpha \in K(\gamma)$, there must be a natural number n and elements $c_i, d_i \in K$ $(0 \leq i \leq n)$, with not all the d_i zero and not all the c_i zero, and such that $c_n \neq 0$ or $d_n \neq 0$, and for which

$$\alpha = \frac{c_0 + c_1\gamma + \cdots + c_n\gamma^n}{d_0 + d_1\gamma + \cdots + d_n\gamma^n}.$$

But then γ is a root of the polynomial equation

$$(c_n - d_n\alpha)t^n + \cdots + (c_1 - d_1\alpha)t + (c_0 - d_0\alpha) = 0,$$

with coefficients from $K(\alpha)$, so that $[K(\gamma) : K(\alpha)] \leq n < \infty$. In addition, since α is algebraic over K, one has $[K(\alpha) : K] < \infty$. Then by the tower law, we find that

$$[K(\gamma) : K] = [K(\gamma) : K(\alpha)][K(\alpha) : K] < \infty.$$

But $K(\beta) \subseteq K(\gamma)$, so we are forced to conclude that $[K(\beta) : K] \leq [K(\gamma) : K] < \infty$, which implies that β is algebraic over K. This contradicts our hypothesis that β is transcendental over K, and thus we see that $K(\alpha, \beta) : K$ cannot be a simple extension.

(c) (3+3+5=11 marks)

(i) Define what it means for a field extension $L : K$ to be an *algebraic closure*.

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

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

Solution: [B] 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 we write E_α for the evaluation map $E_\alpha : K[t] \to L$. Thus $m_\alpha(K)$ is the unique monic irreducible polynomial lying in $K[t]$ having α as a root.

(iii) Suppose that L is an algebraically closed field, and that $M : L$ is an algebraic extension with $L \subseteq M$. Show that $M = L$.

Solution: [U] Suppose that $\alpha \in M$. Then, by hypothesis, we have that α is algebraic over L. Let $m_\alpha(L)$ denote the minimal polynomial of α over L. Since L is algebraically closed, we find that $m_\alpha(L)$ splits over L. Since $m_\alpha(L)$ is a minimal polynomial, and hence irreducible, it follows that $m_\alpha(L)$ must be linear, and hence $m_\alpha(L) = t - \alpha \in L[t]$. We conclude that $\alpha \in L$, and hence all elements of M also lie in L. We therefore have $M \subseteq L \subseteq M$, whence $M = L$.

2. (a) (5 marks) Suppose that $L : \mathbb{Q}$ is a field extension with $\mathbb{Q} \subseteq L$, and that $\alpha \in L$ is a root of the polynomial $f(t) = 2t^9 - 25t^3 + 5$. Prove that there exists no element $\beta \in \mathbb{Q}(\alpha)$ having minimal polynomial $m_\beta(\mathbb{Q})$ over $\mathbb{Q}$ of degree 5.

Solution: [U $\approx$H] By applying Eisenstein's criterion with the prime 5, one finds that the polynomial f is irreducible over $\mathbb{Q}$, and hence $m_\alpha(\mathbb{Q}) = f$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 9$. Since $\beta \in \mathbb{Q}$, it follows that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, and hence the tower law delivers the relation

$$9 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}].$$

Thus $\deg m_\beta(\mathbb{Q}) = [\mathbb{Q}(\beta) : \mathbb{Q}]$ divides 9, so is one of 1, 3 and 9. It is therefore not possible that β has minimal polynomial over $\mathbb{Q}$ of degree 5, as required.

(b) (2+5=7 marks) Suppose that $E : K$ and $F : K$ are finite extensions having the property that K, E and F are all contained in a field L.

(i) Define what is meant by the *compositum* EF of the fields E and F.

Solution: [B] The compositum EF of the fields E and F is the smallest subfield of L containing both E and F.

(ii) Suppose that $E : K$ and $F : K$ are normal. Prove that $EF : K$ is normal.

Solution: [B] Suppose that $E : K$ and $F : K$ are normal extensions. Thus $E : K$ is a splitting field extension for some $g \in K[t] \setminus K$, and $F : K$ is a splitting field extension for some $h \in K[t] \setminus K$. Let

$$A = \{\alpha \in L : g(\alpha) = 0\} \quad \text{and} \quad B = \{\beta \in L : h(\beta) = 0\}.$$

Thus $E = K(A)$ and $F = K(B)$, and we have $EF = K(A \cup B)$. So $EF : K$ is a splitting field extension for $gh \in K[t]$. Hence $EF : K$ is normal.

(c) (2+6=8 marks) Suppose that $L : M$ is an algebraic field extension with $M \subseteq L$, and let $\overline{M}$ denote an algebraic closure of M.

(i) What does it mean for a polynomial $f \in M[t]$ to be *separable* over M?

Solution: [B] A polynomial $f \in M[t]$ is separable over M if each of its irreducible factors g has $\deg g$ distinct roots over $\overline{M}$.

(ii) Prove that when $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism, then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M. [Here we have written $m_\alpha(M)$ for the minimal polynomial of α over M.]

Solution: [H] Suppose that $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism. Since $L : M$ is algebraic, we know that $m_\alpha(M)$ exists. Over $\overline{M}$, we have

$$m_\alpha(M) = \prod_{i=1}^{d} (t - \alpha_i)^{r_i}$$

where $\alpha_1, \ldots, \alpha_d$ are distinct and $r_1, \ldots, r_d \in \mathbb{N}$. Then

$$\sigma(m_\alpha(M)) = \prod_{i=1}^{d} (t - \sigma(\alpha_i))^{r_i},$$

and since σ is necessarily injective, we know that $\sigma(\alpha_1), \ldots, \sigma(\alpha_d)$ are distinct. Thus $m_\alpha(M)$ has multiple roots if and only if $\sigma(m_\alpha(M))$ has multiple roots. We know that $\sigma(m_\alpha(M))$ is irreducible over $\sigma(M)$ since $m_\alpha(M)$ is irreducible over M. Hence $m_\alpha(M)$ is separable over M if and only if $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$.

(d) (1+4=5 marks) Let $L : K$ be a field extension with $K \subseteq L$, and suppose that K has characteristic $p > 0$.

(i) Define the Frobenius monomorphism φ on L.
Solution: [B] The Frobenius map $\varphi : L \to L$ is defined by $\varphi(\alpha) = \alpha^p$, for each $\alpha \in L$, since p is the characteristic of L.

(ii) Suppose that $f \in L[t]$ is an inseparable polynomial fixed under the action of the Frobenius map, so that $\varphi(f) = f$. Is it possible that $f \in L[t^p]$? Justify your answer.
Solution: [U] Suppose that $f \in L[t^p]$, so that for some $a_0, \ldots, a_n \in L$, one has

$$f(t) = a_0 + a_1 t^p + \ldots + a_n t^{np}.$$

Since f is fixed by Frobenius, we have

$$\begin{aligned} a_0 + a_1 t^p + \ldots + a_n t^{np} = f = \varphi(f) &= \varphi(a_0) + \varphi(a_1) t^p + \ldots + \varphi(a_n) t^{np} \\ &= a_0^p + a_1^p t^p + \ldots + a_n^p t^{np} \\ &= (a_0 + a_1 t + \ldots + a_n t^n)^p. \end{aligned}$$

Then $f = g^p$, say, where $g \in L[t]$ is also fixed by Frobenius. But g is inseparable only when $g \in L[t^p]$. Thus g has the same property as f, but has smaller degree. By repeating this descent, we find that for some natural number r, one has $f = h^{p^r}$, where $h \in L[t]$ is linear, and therefore separable. Thus we obtain a contradiction. Then f cannot be inseparable.

Continued...

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

(i) normal
Solution: [B] 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: [B] 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) an extension by radicals
Solution: [B] The extension $L : K$ is an extension by radicals if there are intermediate fields

$$L = L_r : L_{r-1} : \ldots : L_0 = K$$

having the property that $L_i = L_{i-1}(\beta_i)$, with $\beta_i^n \in L_{i-1}$ for some $n \in \mathbb{N}$, for $1 \leq i \leq r$.

(iv) cyclic
Solution: [B] An extension $L : K$ is cyclic if it is Galois, with cyclic Galois group.

(v) Galois
Solution: [B] 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) When $L : K$ is an algebraic field extension with $K \subseteq L$, and L is algebraically closed, then the field extension $L : K$ is normal.
Solution: [U≈B] True.

(ii) 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: [B] True.

(iii) All simple extensions of $\mathbb{Q}$ are isomorphic.
Solution: [U≈H] False. The extensions $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ are both simple, yet

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \neq 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

(iv) There is a homomorphism of finite fields $\varphi : \mathbb{F}_7 \to \mathbb{F}_{2017}$.
Solution: [U] False. Note that 2017 is not divisible by 7. We may suppose that 2017 is a prime power, for otherwise there is no finite field $\mathbb{F}_{2017}$ (and in fact 2017 is prime). We derive a contradiction to the statement. Writing $n \cdot 1$ for the n-fold sum $1 + \ldots + 1$,

$$0 = \varphi(0) = \varphi(7 \cdot 1) = 7 \cdot \varphi(1) = 7 \cdot 1 = 7 \in \mathbb{F}_{2017},$$

and yet $7 \neq 0$ in $\mathbb{F}_{2017}$, since 2017 is not a power of 7. Contradiction.

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

(vi) An algebraic extension of $\mathbb{Q}$ has only finitely many subfields.
Solution: [U] False. The extension $\overline{\mathbb{Q}} : \mathbb{Q}$, where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$, is an algebraic extension. Yet there are infinitely distinct subfields of $\overline{\mathbb{Q}}$ given by the fields $\mathbb{Q}(\sqrt{d})$, with d prime.

(vii) Any algebraic extension of $\mathbb{Q}$ is normal.
Solution: [H] False. Consider the example $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $t^3 - 2$, and this has splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity. The polynomial $t^3 - 2$ does not split completely over $\mathbb{Q}(\sqrt[3]{2})$, and hence $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ is not normal.

(viii) When $L : K$ is a field extension with $K \subseteq L$, and α and β are distinct elements of L having the same minimal polynomial over K, then $K(\alpha)$ is isomorphic to $K(\beta)$.
Solution: [B] True.

(ix) The real number $\sqrt[3]{2 + \sqrt{2}}$ can be constructed by ruler and compass.
Solution: [U] False. Write $\alpha = \sqrt[3]{2 + \sqrt{2}}$. Then $(\alpha^3 - 2)^2 = 2$, whence $\alpha^6 - 4\alpha^2 + 2 = 0$. The polynomial $t^6 - 4t^2 + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion using the prime 2. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Since the latter is not a power of 2, one finds that α cannot be constructed by ruler and compass.

(x) Suppose that $L : K$ is finite and separable. Then $L : K$ is simple.
Solution: [B] True.

(xi) There is no polynomial f over a finite field of characteristic p which is irreducible and of degree p.
Solution: [U≈H] False. Consider $f(t) = t^2 - t + 1$ over $\mathbb{F}_2$. Since $a^2 = a$ for all $a \in \mathbb{F}_2$, one sees that $f(a) \neq 0$ for all $a \in \mathbb{F}_2$. So f cannot have a linear factor over $\mathbb{F}_2$, and hence must be irreducible.

(xii) There exist polynomials $f \in \mathbb{Q}[t]$ of degree 5 solvable by radicals.
Solution: [B] True.

(xiii) Suppose that $M : L$ and $L : K$ are finite separable extensions. Then $M : K$ is separable.
Solution: [B] True.

(xiv) Suppose that $M : L$ and $L : K$ are field extensions with $M : K$ normal. Then $M : L$ is a normal field extension.
Solution: [B] True.

(xv) Let $K = \overline{\mathbb{F}_p(t)}$ denote the algebraic closure of $\mathbb{F}_p(t)$. Then there exist inseparable polynomials in $K[X]$.
Solution: [U≈B] False. Over any algebraically closed field, the only irreducible polynomials are linear. Thus, it is not possible that an irreducible polynomial in $K[X]$ has multiple roots. Thus no polynomial in $K[X]$ can be inseparable.

Continued...

4. (a) (4 marks) State the Fundamental Theorem of Galois Theory.
Solution: [B] Suppose that $L : K$ is finite. Let $G = \mathrm{Gal}(L : K)$, and let $K_0 = \varphi(G)$, 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 $\varphi(H) : K_0$ is a normal extension;
(iii) Suppose that $H \lhd G$. Then whenever $\sigma \in G$, one has $\sigma|_{\varphi(H)} \in \mathrm{Gal}(\varphi(H) : K_0)$. Furthermore, the map $\sigma \to \sigma|_{\varphi(H)}$ is a homomorphism of G onto $\mathrm{Gal}(\varphi(H) : K_0)$ with kernel H, so that $\mathrm{Gal}(\varphi(H) : K_0) \simeq G/H$.

(b) (4+4+4 marks) Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = X^4 - 4$.
(i) Determine the degree of the extension $L : \mathbb{Q}$, justifying your answer.
Solution: [U≈B≈H] One has $L = \mathbb{Q}(\sqrt{2}, \sqrt{-2})$. We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$. The minimal polynomial for $\sqrt{-2}$ over $\mathbb{Q}(\sqrt{2})$ divides $X^2 + 2$. Since $\sqrt{-2} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, one sees that $X^2 + 2$ has no root in $\mathbb{Q}(\sqrt{2})$, and hence is irreducible over $\mathbb{Q}(\sqrt{2})$. Thus $[L : \mathbb{Q}(\sqrt{2})] = 2$, and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

(ii) Describe the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).
Solution: The group $\mathrm{Gal}(L : \mathbb{Q})$ is generated by σ and τ, where these maps fix $\mathbb{Q}$ pointwise, and $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{-2}) = \sqrt{-2}$, and $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{-2}) = -\sqrt{-2}$. Thus $\sigma\tau(\sqrt{2}) = \tau\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma\tau(\sqrt{-2}) = \tau\sigma(\sqrt{-2}) = -\sqrt{-2}$. Then σ, τ, $\sigma\tau$ each have order 2, and $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau : \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(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 $\mathrm{Gal}(L : \mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. The fields M that we are to find are the fixed fields of the subgroups $H_1 = \langle \sigma \rangle$, $H_2 = \langle \tau \rangle$, and $H_3 = \langle \sigma\tau \rangle$. With M_i the fixed field of H_i, we have $M_1 = \mathbb{Q}(\sqrt{-2})$, $M_2 = \mathbb{Q}(\sqrt{2})$, $M_3 = \mathbb{Q}(\sqrt{-1})$. 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 $\sqrt{-1} = \sqrt{-2}/\sqrt{2}$ is fixed by $\sigma\tau$, and

$$[M_3 : \mathbb{Q}] = 4/|\langle \sigma\tau \rangle| = 4/2 = 2 = [\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}],$$

whence $M_3 = \mathbb{Q}(\sqrt{-1})$.

(c) (3+3+3=9 marks) Let $L : K$ be a finite Galois extension with Galois group G, and suppose that $\alpha \in L$.
(i) Let $f_\alpha(t) = \prod_{\sigma \in G}(t - \sigma(\alpha))$. Show that $f_\alpha \in K[t]$.
Solution: [U≈H] Since $L : K$ is Galois, the fixed field of G is K. Then $\alpha \in K$ if and

only if $\tau(\alpha) = \alpha$ for every $\tau \in G$. Since the action of τ on G is simply to permute the elements of G, we find that whenever $\tau \in G$, one has

$$\tau(f_\alpha(t)) = \prod_{\sigma \in G} (t - \tau(\sigma(\alpha))) = \prod_{\rho \in G} (t - \rho(\alpha)) = f_\alpha(t).$$

Then $f_\alpha(t)$ has each of its coefficients in the fixed field of G, so $f_\alpha \in K[t]$.

(ii) Show that the minimal polynomial $m_\alpha(K)$ of α over K divides $f_\alpha(t)$.

Solution: [U≈H] Since $\mathrm{id} \in G$, one has that $t - \alpha$ is a factor of $f_\alpha(t)$, and hence $f_\alpha(\alpha) = 0$. Consequently, one must have $m_\alpha(K) | f_\alpha$.

(iii) Suppose that $\sigma(\alpha) \neq \tau(\alpha)$ whenever $\sigma, \tau \in G$ satisfy $\sigma \neq \tau$. Show that one has $m_\alpha(K) = f_\alpha$.

Solution: [U≈H] Over $L[t]$ one has that $t - \alpha$ divides $m_\alpha(K)$. Then since m_α is fixed by the action of G (its coefficients lie in K), we find that $t - \sigma(\alpha)$ divides $\sigma(m_\alpha(K)) = m_\alpha(K)$ for each $\sigma \in G$. By hypothesis, moreover, the elements $\sigma(\alpha)$ are distinct for $\sigma \in G$, and thus $\prod_{\sigma \in G}(t - \sigma(\alpha)) = f_\alpha(t)$ divides $m_\alpha(K)$. Thus we find that $m_\alpha(K)$ and f_α divide each other, and this implies that f_α is the minimal polynomial of α.

End of examination.