UNIVERSITY OF BRISTOL

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

GALOIS THEORY

MATH M2700

(Paper Code MATH-M2700)

January 2016, 2 hours 30 minutes

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

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+3=10 marks) Suppose that $K \subseteq L$ are fields.

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

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

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

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

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

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

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

(c) (5+3=8 marks) (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.

(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.

2. (a) (3+3=6 marks)

(i) State Eisenstein's criterion for irreducibility of polynomials in $\mathbb{Z}[t]$.

(ii) Determine whether or not the polynomial $5t^5 - 40t - 2$ is irreducible over $\mathbb{Z}$, and explain your reasoning.

(b) (4+2=6 marks)

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.

(c) (3+3=6 marks)

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 $\tau(\alpha) = \beta$.

(d) (2+5=7 marks)

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 $\mathbb{Q}$.

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

Continued...

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

(i) normal
(ii) a splitting field extension
(iii) separable
(iv) finite
(v) Galois

(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.

(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.

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

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

(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.

(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 $K_1 \cap K_2 = \mathbb{Q}$.

(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.

(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 $\mathbb{F}_p$.

(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 $\mathbb{Q}(\alpha, \alpha^2, \alpha^3) = \mathbb{Q}(\beta)$.

(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 $[\mathbb{Q}(\theta) : \mathbb{Q}] = p$.

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

(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 $\mathrm{card}(K) = n$.

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

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

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

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

Continued...

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

   (b) (3+4+2=9 marks) 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 $x^{p^n} - x$.

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

   (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 $d|n$.

   (c) (4+4+4=12 marks) 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.

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

   (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.

End of examination.