UNIVERSITY OF BRISTOL

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

GALOIS THEORY

MATH M2700

(Paper Code MATH-M2700)

January 2015, 2 hours 30 minutes

This paper contains **five** *questions.*
A candidate's **FOUR** *best answers 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+2 marks) Suppose that $K \subseteq L$ are fields, and that $\alpha \in L$.
   (i) Define $[L : K]$, the degree of the field extension $L : K$.
   (ii) Define what it means for $L : K$ to be a finite extension.
   (iii) Suppose α is algebraic over K. Briefly explain why $K[\alpha] = K(\alpha)$.
   (iv) Is it possible that $[K(\alpha) : K] = \infty$? Briefly explain your answer.

   (b) (2+2+2+3 marks) Suppose that $K \subseteq L$ are fields such that $L : K$ is a finite extension.
   (i) Define what it means for $f \in K[X]$ to split over L.
   (ii) Define what it means for $L : K$ to be a splitting field extension.
   (iii) Define what it means for $L : K$ to be normal.
   (iv) Suppose that $L : K$ is a normal extension, and that M is a field having the property that $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.

   (c) (4+3 marks) Suppose that L is a subfield of $\mathbb{C}$ having the property that $L : \mathbb{Q}$ is an infinite, normal field extension.
   (i) Suppose that φ is an automorphism of $\mathbb{C}$. Show that whenever $\alpha \in L$, then $\varphi(\alpha) \in L$. Hence deduce that $\varphi(L) \subseteq L$.
   (ii) Prove that whenever ψ is an automorphism of $\mathbb{C}$, then $\psi(L) = L$.

2. (a) (3+3 marks)
   (i) State Eisenstein's criterion for irreducibility of polynomials in $\mathbb{Z}[t]$.
   (ii) Determine whether or not the polynomial $3t^{2015} + 24t + 2$ is irreducible over $\mathbb{Z}$, and explain your reasoning.

   (b) (3+3 marks) Let L be a field extension of K.
   (i) What does it mean for $\alpha \in L$ to be algebraic over K?
   (ii) Define, when $\alpha \in L$ is algebraic over K, the minimal polynomial of α over K.

   (c) (6 marks)
   Calculate the minimal polynomial of $\sqrt{3 + \sqrt[3]{6}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt{3 + \sqrt[3]{6}}) : \mathbb{Q}$.

   (d) (7 marks)
   Let $L : K$ be a field extension and suppose that γ is an element of L whose minimal polynomial over K has degree 9. Prove that if $h \in K[t]$ is a non-zero quadratic polynomial, then the minimal polynomial of $h(\gamma)$ over K has degree 9.

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

(i) algebraically closed
(ii) simple
(iii) Galois
(iv) separable
(v) cyclic

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

(i) Any algebraic extension of $\mathbb{Q}$ is normal.

(ii) If $L : K$ is a finite extension of fields, then every element of L is algebraic over K.

(iii) Every field extension of finite degree is a splitting field extension.

(iv) There is an isomorphism $\varphi : \mathbb{Q}(\sqrt{11}) \to \mathbb{Q}(\sqrt{-11})$ so that $\varphi(\sqrt{11}) = \sqrt{-11}$.

(v) If $L : K$ is a field extension and $\tau \in L$ is transcendental over K, then $\tau^3 + \tau + 1$ is transcendental over K.

(vi) If K_1 and K_2 are subfields of a field L, and $[L : K_1] = [L : K_2]$, then K_1 and K_2 are isomorphic fields.

(vii) 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.

(viii) A splitting field of a degree n irreducible polynomial in $\mathbb{R}[t]$ has degree $n!$ over $\mathbb{R}$.

(ix) If $L : K$ is a field extension and $L = K(\alpha)$, then for any $\beta \in L$, there exist $a, b \in K$ with $\beta = a + b\alpha$.

(x) The polynomial $x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.

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

(xii) Every field extension of $\mathbb{Q}$ of finite degree has only finitely many subfields.

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

(xiv) If K is a field and γ is an element in an extension field of K, then every element of $K(\gamma)$ is expressible as a polynomial in γ with coefficients in K.

(xv) Suppose $L : K$ is a Galois extension with $\mathrm{Gal}(L : K) \simeq S_n$. Then, for any subgroup H of S_n, there is a field M with the property that $L : M$ is a Galois extension with $\mathrm{Gal}(L : M) \simeq H$.

Continued...

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

   (b) (4+4+4 marks) Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = (X^2 - 2)(X^2 + 7)$.

   (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.

   (c) (5+4 marks) Let $K : \mathbb{Q}$ be a splitting field extension for $g(X) = X^4 - 5$.

   (i) Show that $[K : \mathbb{Q}] = 8$.

   (ii) Describe the Galois group $\mathrm{Gal}(K : \mathbb{Q})$.

5. (a) (2+3 marks) Let K be a finite field.

   (i) Define the Frobenius map on K.

   (ii) Let $m = |K|$. Show that every element of K is a root of the polynomial $t^m - t$.

   (b) (2+6+2 marks) Let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. Put $f(t) = t^p - t + 1$, and let $K = \mathbb{F}_p(\alpha)$, where α is a root of f.

   (i) Show that for all $\xi \in \mathbb{F}_p$, the element $\alpha + \xi$ is a root of f.

   (ii) Let σ be the Frobenius map on K. Show that for $1 \leq d < p$, one has that $\sigma^d(\alpha)$ is a root of f.

   (iii) Show that f is irreducible over $\mathbb{F}_p$.

   (c) (2+3+3+2 marks) Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $L = \mathbb{F}_p(t)$ be the field of fractions associated to the polynomial ring $\mathbb{F}_p[t]$.

   (i) Let M denote a splitting field for the polynomial $X^p - t \in L[X]$. Show that for some $\beta \in M$, one has $X^p - t = (X - \beta)^p$.

   (ii) Suppose that $X^p - t = fg$, where f and g are monic polynomials in $L[X]$ of positive degree. Show that one must have $f = (X - \beta)^s$ for some integer s with $1 \leq s \leq p - 1$, and deduce that $\beta^s \in L$.

   (iii) Show that $\beta \in L$, and hence obtain a contradiction to the above factorisation.

   (iv) Prove that $[M : L] = p$.

End of examination.