UNIVERSITY OF SURREY©

M. Math. Undergraduate Programmes in Mathematical Studies

Level HE3 Examination

Module MS325 GALOIS THEORY (MMath)

Time allowed – 2 hrs

Spring Semester 2007

Answer any **three** of the five questions.

If you attempt more than three questions, only your BEST THREE answers will be taken into account.

Each question carries 30 marks.

Any results established in the course may be assumed and used without proof unless a proof is requested.

If you are asked to find or identify a group, it is sufficient to give the name by which the group is usually known, e.g. V, S_5**.**

Question 1

(a) Let $\mathrm{f} = t^3 + 24t + 16 \in \mathbb{Q}[t]$. Let $\alpha = 2^{1/3}$ and $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$.

(i) Show that one of the zeros of f is $\alpha^4 - \alpha^5$, and find the other zeros of f in terms of α and ω. [10]

You are given that f is the cubic resolvent of the quartic polynomial $\mathrm{h} = t^4 + 4t - 6 \in \mathbb{Q}[t]$. Let $\varepsilon = (\alpha - 1)^{1/2}$.

(ii) Show that h is reducible over $\mathbb{Q}(\varepsilon)$ as a product of two quadratic factors. [9]

(b) Let f be a polynomial of degree n in $\mathbb{Q}[t]$ with distinct zeros $\alpha_1, \ldots, \alpha_n$.

(i) Explain what is meant by a **symmetry** of the zeros of f. [3]

(ii) Let $\delta(\mathrm{f}) = \prod_{i<j}(\alpha_i - \alpha_j)$.

Prove that if $\delta(\mathrm{f}) \in \mathbb{Q}$ then the Galois group of f over $\mathbb{Q}$ is a subgroup of the alternating group A_n. [8]

Question 2

(a) Let α be the positive real number $\sqrt{2 + 3\sqrt{2}}$.

(i) Find μ, the minimal polynomial of α over $\mathbb{Q}$, showing that $\partial\mu = 4$. [6]

(ii) Show that $\mathbb{Q}(\alpha) : \mathbb{Q}$ is not a normal extension. [6]

(iii) Find the splitting field L of μ over $\mathbb{Q}$ and state the value of $[L : \mathbb{Q}]$. [6]

(iv) Identify the Galois group $\Gamma(L : \mathbb{Q})$. [2]

(b) (i) State what is meant by a **primitive element** for a field extension $L : K$. [2]

(ii) Let p be prime. Prove that every finite extension of the finite field $\mathbb{F}_p$ has a primitive element. You may assume that in any finite field, the multiplicative group of non-zero elements is cyclic. [6]

(iii) Give an example of a field extension which does not have a primitive element. [2]

Question 3

(a) Let $\alpha = \mathrm{e}^{2\pi\mathrm{i}/5}$, $y_1 = \alpha + \alpha^4$, $y_2 = \alpha^2 + \alpha^3$.

(i) Find a quadratic polynomial over $\mathbb{Q}$ with zeros y_1 and y_2. [6]

(ii) Hence show that $\cos \dfrac{2\pi}{5} \in \mathbb{Q}(\sqrt{5})$. [5]

(iii) Using this result, describe a ruler-and-compass method for constructing a regular pentagon. [4]

(iv) Identify the Galois group $G = \Gamma(\mathbb{Q}(\alpha) : \mathbb{Q})$ and list its elements. [3]

(v) Draw the lattices of subgroups of G and subfields of $\mathbb{Q}(\alpha)$. Briefly explain the Galois correspondence between these subgroups and subfields. [6]

(b) Prove that if a complex number z is constructible then $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of 2. You may assume the corresponding result for real numbers. [6]

Question 4

In this question, f is the polynomial $t^5 - 3$ in $\mathbb{Q}[t]$.

(a) Express the zeros of f in terms of $\alpha = 3^{1/5}$ and $\varepsilon = \mathrm{e}^{2\pi\mathrm{i}/5}$. [3]

(b) Show that $\varepsilon \notin \mathbb{Q}(\alpha)$ and explain why $\mathbb{Q}(\alpha, \varepsilon)$ is the splitting field of f over $\mathbb{Q}$. [4]

(c) Give the minimal polynomials of α over $\mathbb{Q}$ and of ε over $\mathbb{Q}(\alpha)$. Hence write down bases for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and for $\mathbb{Q}(\alpha, \varepsilon)$ over $\mathbb{Q}(\alpha)$. [8]

(d) Deduce the value of $[\mathbb{Q}(\alpha, \varepsilon) : \mathbb{Q}]$ and state, with justification, the order of the Galois group $G = \Gamma(\mathbb{Q}(\alpha, \varepsilon) : \mathbb{Q})$. [4]

(e) Let σ be a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\alpha, \varepsilon)$ such that $\sigma(\alpha) = \alpha\varepsilon,\ \sigma(\varepsilon) = \varepsilon$

If H is the cyclic subgroup of G generated by σ, show that H has order 5 and identify its fixed field. [6]

(f) Find a normal extension $M : \mathbb{Q}$ such that $\dfrac{G}{H} \cong \Gamma(M : \mathbb{Q})$ and identify the group $\Gamma(M : \mathbb{Q})$. [5]

Question 5

(a) Let p be prime, let $\mathbb{F}_p$ be the field of integers modulo p, and let K be an extension field of $\mathbb{F}_p$. Let $q = p^n$ and $\mathrm{f} = t^q - t \in \mathbb{F}_p[t]$.

Given that the zeros of f form a field $\mathbb{F}_q$, show that this field has q distinct elements and state the value of $[\mathbb{F}_q : \mathbb{F}_p]$. [6]

(b) (i) Define the term **solvable group**. [3]

(ii) Show that the symmetric group S_4 is solvable. [3]

(iii) Without giving detailed reasoning, outline the steps of the proof that S_n is not a solvable group if $n \geq 5$. [6]

(iv) Let f be an irreducible polynomial in $\mathbb{Q}[t]$ of prime degree ≥ 5.

State a condition on the zeros of f which is sufficient to show that f is *not* solvable by radicals over $\mathbb{Q}$. [1]

(v) Let c and d be positive integers such that $0 < d < \frac{4}{5}c^{5/4}$ and $5 \not| d$.

Show that $t^5 - 5ct + 5d \in \mathbb{Q}[t]$ is not solvable by radicals over $\mathbb{Q}$. [11]

INTERNAL EXAMINER: Dr D.J. Fisher
EXTERNAL EXAMINER: Prof P. Glendinning