UNIVERSITY OF SURREY©

B. Sc. Undergraduate Programmes in Mathematical Studies

Level HE3 Examination

Module MS300 GALOIS THEORY

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 $\mathrm{f} = \sum_{r=0}^{n} a_r t^r \in \mathbb{Z}[t]$ and let p be a prime which does not divide a_n.

Let ν_p be the natural homomorphism from $\mathbb{Z}[t]$ to $\mathbb{F}_p[t]$.

(i) Prove that if $\nu_p(\mathrm{f})$ is irreducible over $\mathbb{F}_p$ then f is irreducible over $\mathbb{Z}$. [6]

(ii) Deduce that every polynomial of the form $t^3 + 2t + k$, where k is not an integer multiple of 3, is irreducible over $\mathbb{Z}$. [5]

Question 2

(a) (i) State what is meant by an **algebraic extension** of a field K. [2]

(ii) Prove that if $L : K$ is a finite field extension then it is an algebraic extension. [6]

(iii) Give an example of an algebraic extension which is not finite. [2]

(b) 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]

Question 3

(a) Define the terms **radical extension** and **constructible number**. [4]

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

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

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

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

(iv) Find the value of $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. [2]

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

(vi) Draw the lattices of subgroups of G and subfields of $\mathbb{Q}(\alpha)$. Briefly explain the Galois correspondence between these subgroups and subfields. [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 $\varepsilon = e^{2\pi i/5}$. [3]

(b) Show that $\varepsilon \notin \mathbb{Q}(\alpha)$ and explain why $\mathbb{Q}(\alpha, \varepsilon)$ is the splitting field of f over $\mathbb{Q}$. [5]

(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 $\sigma(\alpha) = \alpha\varepsilon,\ \sigma(\varepsilon) = \varepsilon$

Explain why this information is enough to determine the effect of σ on the whole of $\mathbb{Q}(\alpha, \varepsilon)$. [3]

(f) If H is the cyclic subgroup of G generated by σ, describe each element of H by its effect on α and on ε. State the order of H and identify its fixed field. [7]

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 $\mathbb{F}_p$.

(i) Show that K must have p^n elements for some positive integer n. [4]

(ii) 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]

(iii) Identify the Galois group of $\mathbb{F}_{243}$ over $\mathbb{F}_3$, and give a generator of this group. [3]

(b) (i) Define the term **solvable group**. [4]

(ii) 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 $\mathbb{Q}$. [2]

(iii) Let c and d be positive integers such that $0 < d < \frac{4}{5}c^{5/4}$ and $5 \nmid d$.

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