UNIVERSITY OF SURREY©

M. Math. Undergraduate Programmes in Mathematical Studies

Level HE3 Examination

Module MS325 GALOIS THEORY (M.Math. version)

Time allowed – 2 hours

Spring Semester 2008

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.

Question 1

(a) The polynomial $\mathrm{f} \in \mathbb{Q}[t]$ is defined by $\mathrm{f} = t^3 + 6t - 2$.

(i) Find the zeros of f in terms of $\alpha = 2^{1/3}$ and $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$. [8]

(ii) Identify the Galois group $\Gamma_{\mathrm{Q}}(\mathrm{f})$. Define each element of this group by its effect on α and on ω. [7]

(iii) Given that $\mathbb{Q}(\alpha, \omega)$ is the splitting field of f over $\mathbb{Q}$, sketch the lattice diagrams for this example. Identify each subgroup of $\Gamma_{\mathbb{Q}}(\mathrm{f})$ and subfield of $\mathbb{Q}(\alpha, \omega)$. [6]

(b) Let $\mathrm{f} = \sum_{r=0}^{n} a_r t^r$ where $a_0, \ldots, a_n \in \mathbb{Z}$. Suppose a prime integer p divides $a_0, \ldots, a_{n-1}$, but p does not divide a_n and p^2 does not divide a_0.

Let ν_p be the natural homomorphism from $\mathbb{Z}[t]$ to $\mathbb{F}_p[t]$. For $a \in \mathbb{Z}$, let $\overline{a}$ denote $\nu_p(a)$.

(i) Show that $\nu_p(\mathrm{f}) = \overline{a}_n t^n$. [2]

Now suppose $\mathrm{f} = \mathrm{gh}$, where $\mathrm{g} = \sum_{r=0}^{k} b_r t^r$, $\mathrm{h} = \sum_{r=0}^{m} c_r t^r$ are in $\mathbb{Z}[t]$ and $\partial\mathrm{g} < \partial\mathrm{f}$, $\partial\mathrm{h} < \partial\mathrm{f}$.

(ii) Show that either $\overline{b}_0 = 0$ or $\overline{c}_0 = 0$, but not both. [3]

(iii) Assuming that $\overline{b}_0 = 0$, deduce that $\mathrm{g} = 0$. What result does this prove? [4]

Question 2

(a) (i) If $\mathrm{f} = t^4 + ct^2 + dt + e \in \mathbb{Q}[t]$, it is known that

$$\mathrm{f} = \left(t^2 + kt + \frac{k^2 + c}{2} - \frac{d}{2k}\right)\left(t^2 - kt + \frac{k^2 + c}{2} + \frac{d}{2k}\right)$$

where $-k^2$ is a zero of ρ, the cubic resolvent of f.

Letting α_1, α_2 be the zeros of the first factor and α_3, α_4 be the zeros of the second factor, show that if $u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$ then $\rho(u) = 0$. [4]

(ii) You are given that the cubic resolvent of $t^4 + dt + e$ is $\rho = t^3 - 4et + d^2$.

If now $\mathrm{f} = t^4 - 12t - 5$, show that -4 is a zero of the cubic resolvent of f. Use the quadratic factors given in part (i) to find the zeros of f. [8]

(iii) Identify the Galois group of f over $\mathbb{Q}$. [2]

(b) Let $L : K$ be a normal field extension, i.e. every polynomial in $K[t]$ which has at least one zero in L has all its zeros in L.

(i) Prove that L is a splitting field for some polynomial in $K[t]$. You may assume the Primitive Element Theorem. [5]

(ii) Name the extra properties that $L : K$ must have in order for it to be a **Galois extension**. [2]

(iii) If $[L : K]$ is a Galois extension and M is an intermediate field between K and L, prove that $\Gamma(L : M)$ is a normal subgroup of $\Gamma(L : K)$. You may assume that $M : K$ is a normal extension if and only if $\sigma(M) = M$ for all $\sigma \in \Gamma(L : K)$. [9]

Question 3

(a) (i) Let K be a field of characteristic 0 and suppose $\mathrm{f} \in K[t]$ is irreducible over K. Prove that f is separable. You may assume that a repeated zero of f is also a zero of the formal derivative Df. [8]

(ii) Give an example of a field L and a polynomial $\mathrm{f} \in L[t]$ such that f is irreducible over L but not separable. [3]

(b) (i) Let $\mathrm{f} = 1 + t + t^2 + \cdots + t^{p-1}$ where p is prime. By considering $\mathrm{f}(t+1)$, show that f is irreducible over $\mathbb{Q}$. You may assume that the binomial coefficient $\binom{p}{r}$ is divisible by p for $r = 1, \ldots, p-1$. [7]

(ii) Show that $(1 - t^p)(1 + t^p + t^{2p} + \cdots + t^{(p-1)p}) = 1 - t^{p^2}$ and express $1 - t^{p^2}$ as a product of irreducible polynomials over $\mathbb{Q}$. [6]

(iii) Hence show that when p is a prime greater than 2, a regular p^2-sided polygon cannot be constructed using ruler and compass only. [6]

Question 4

In this question f is the irreducible polynomial $t^4 - 4t^2 + 6$ in $\mathbb{Q}[t]$. You are given that the zeros of f are $-\alpha, \alpha, -\beta$ and β, where $\alpha = \sqrt{2 + \mathrm{i}\sqrt{2}}$ and $\beta = \sqrt{2 - \mathrm{i}\sqrt{2}}$.

(a) Find $\alpha\beta$ in its simplest form. Deduce that $L = \mathbb{Q}(\alpha, \sqrt{6})$ is the splitting field of f over $\mathbb{Q}$. [5]

(b) By considering the minimal polynomials of α over $\mathbb{Q}$ and of $\sqrt{6}$ over $\mathbb{Q}(\alpha)$, find the degree of the extension $L : \mathbb{Q}$. [4]

(c) Let σ be the $\mathbb{Q}$-automorphism of L given by $\sigma(\alpha) = \beta, \sigma(\sqrt{6}) = -\sqrt{6}$. Show that $\sigma(\beta) = -\alpha$. Find the automorphisms σ^2, σ^3 and σ^4, defining each one by its effect on α and $\sqrt{6}$ [7]

(d) Deduce that the Galois group $\Gamma(L : \mathbb{Q})$ has a cyclic subgroup C of order 4. State an abstract group to which $\Gamma(L : \mathbb{Q})$ is isomorphic. [5]

(e) Let $\gamma = \dfrac{\alpha}{\beta} - \dfrac{\beta}{\alpha}$. Find the minimal polynomial of γ over $\mathbb{Q}$. [3]

(f) Show that the fixed field of C is $\mathbb{Q}(\gamma)$. [6]

Question 5

(a) Let p be prime, $n \in \mathbb{N}$ and $q = p^n$. Let $\mathbb{F}_q$ be the finite field with q elements. Define the map $\theta : \mathbb{F}_q \to \mathbb{F}_q$ by $\theta(x) = x^p$.

(i) Show that θ is a field automorphism. [6]

(ii) Show that θ generates a cyclic group of order n. Explain why this group is $\Gamma(\mathbb{F}_q : \mathbb{F}_p)$. [7]

(b) Define the terms

(i) the **derived subgroup** of a group G, [3]

(ii) a **perfect group**. [2]

(c) Let $\mathrm{f} = t^5 - 80t + 20 \in \mathbb{Q}[t]$ and let $G = \Gamma_{\mathbb{Q}}(\mathrm{f})$.

Show that G contains an element of order 5 and a transposition. Stating any group-theoretic properties that you use, deduce that f is not solvable by radicals over $\mathbb{Q}$.

[12]

INTERNAL EXAMINER: Dr D.J. Fisher
EXTERNAL EXAMINER: Dr D. Chillingworth