THE UNIVERSITY OF WARWICK

THIRD YEAR EXAMINATION: June 2006

MA3D5 GALOIS THEORY

Time Allowed: **3 hours**

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer book.

Calculators are not needed and are not permitted in this examination.

ANSWER 4 QUESTIONS.
If you have answered more than the required 4 questions in this examination, you will only be given credit for your 4 best answers.

The numbers in the margin indicate approximately how many marks are available for each part of a question.

---

1. (a) Define the elementary symmetric polynomials σ_i in variables $\alpha_1, \ldots, \alpha_n$. **[3]**

(b) Let $P \in \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Define what it means that P is symmetric. Now assume P to be symmetric. Prove that P can be expressed as a polynomial over $\mathbb{Z}$ in the elementary symmetric polynomials $\sigma_i = \sigma_i(\alpha_1, \ldots, \alpha_n)$. **[9]**

(c) Let $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, $\alpha + \beta + \gamma + \delta = 0$. Put **[4]**

$$x = (\alpha + \beta)(\gamma + \delta),$$
$$y = (\alpha + \gamma)(\beta + \delta),$$
$$z = (\alpha + \delta)(\beta + \gamma).$$

Let σ_i denote the elementary symmetric polynomials in $\alpha, \beta, \gamma, \delta$ and τ_i those in x, y, z. Prove that for every $i \geq 0$ there exists a polynomial $p_i \in \mathbb{C}[u_2, u_3, u_4]$ such that $\tau_i = p_i[\sigma_2, \sigma_3, \sigma_4]$.

(d) Deduce from (c) that every degree 4 equation can be solved by radicals. You may assume that every degree 3 equation can. **[6]**

(e) Compute p_1 explicitly. **[3]**

---

2. (a) (i) Let $K \subset L$ be a field extension. Define $[L : K]$. **[2]**

(ii) Let $K \subset L$ and $L \subset M$ be two finite field extensions. Prove that $K \subset M$ is finite, and $[M : K] = [M : L][L : K]$. **[5]**

(iii) Let $\alpha = \sqrt[5]{2} \in \mathbb{R}$. Prove $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. **[4]**

(iv) Let $\beta = \alpha + \alpha^3$. Use the statement of (ii) to prove $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. **[5]**

(b) Define $\alpha = \exp(2\pi i/3) \in \mathbb{C}$. Let $\mathbb{C}(u)$ denote the field of rational functions in a variable u. Define the $\mathbb{C}$-automorphisms s, t of $\mathbb{C}(u)$ by

$$s(u) = u^{-1}, \qquad t(u) = \alpha\, u^{-1}$$

(and s, t fix every element of $\mathbb{C}$). Put $G = \langle s, t \rangle$.

(i) Without proof define an isomorphism $\phi\colon G \to S_3$ to the symmetric group, for example by giving $\phi(s)$ and $\phi(t)$. **[3]**

(ii) Without proof list all subgroups $H \subset G$ (for example by giving generators for them) and for each of them a function $f \in \mathbb{C}(u)$ such that $\mathbb{C}(u)^H = \mathbb{C}(f)$. **[6]**

---

3. (a) Let L be a field, $G \subset \mathrm{Aut}(L)$ a subgroup and $K = L^G$. Suppose that the G-orbit $G\alpha := \{g\alpha \mid g \in G\}$ is finite for every $\alpha \in L$. Prove that L/K is algebraic, normal and separable. [Hint. Mimic our proof of the situation where G is finite.] **[7]**

(b) Let $\varepsilon = \exp(2\pi i/7) \in \mathbb{C}$. You may use the fact that ε has degree 6 over $\mathbb{Q}$. We put

$$\alpha = \varepsilon + \varepsilon^6, \quad \beta = \varepsilon^2 + \varepsilon^5, \quad \gamma = \varepsilon^3 + \varepsilon^4.$$

(i) Prove $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$ and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)] \in \{1, 2\}$ and use the Tower Law to deduce that α is of degree 3 or 6 over $\mathbb{Q}$. **[4]**

(ii) Compute the polynomial $f = (x - \alpha)(x - \beta)(x - \gamma)$ explicitly and hence prove that it is in $\mathbb{Z}[x]$. **[5]**

(iii) Prove that α is of degree 3 over $\mathbb{Q}$. **[2]**

(iv) Find explicitly an $r \in \mathbb{Z}[x]$ such that $r(\alpha) = \beta$. **[3]**

(v) Prove that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$. You may use theorems from the course but you should formulate them if you do. **[4]**

---

4. Let $K \subset L$ be a finite field extension.

(a) Define the Galois group $G = \mathrm{Gal}(L/K)$. **[2]**

(b) Let $\sigma\colon K \to M$ be a field homomorphism. Prove that the number of K-homomorphisms $L \to M$ is at most $[L : K]$. **[8]**

(c) Prove $\#G \leq [L : K]$ and state without proof when equality holds. **[4]**

(d) For a subset $H \subset G$ we define $H^\dagger = L^H = \{x \in L \mid hx = x \text{ for all } h \in H\}$. Prove that $H^\dagger$ is a subfield of L. Prove $H_1 \subset H_2 \Rightarrow H_1^\dagger \supset H_2^\dagger$. **[4]**

(e) Let $\alpha = \sqrt[4]{5} \in \mathbb{R}$, $K = \mathbb{Q}(i) \subset \mathbb{C}$ and $L = \mathbb{Q}(i, \alpha) \subset \mathbb{C}$. You may assume that $f = x^4 - 5 \in K[x]$ is irreducible, and that L/K is Galois. Find $G := \mathrm{Gal}(L/K)$, list its subgroups, and the corresponding fields between K and L. **[7]**

---

5. (a) Let K be a finite field. Prove that there exists a prime number p such that K has a subfield $\mathbb{F}_p$ of p elements, and that K has p^a elements for some $a \geq 1$. **[3]**

(b) Let K be a field of characteristic $p > 0$. Prove that the map $F\colon K \to K$, $F(a) = a^p$ is a ring homomorphism. **[5]**

(c) Let $q = p^a$ be a power of a prime number p. Prove that there exists a finite field K of q elements. You may use that splitting fields exist. **[5]**

(d) Let $\mathbb{F}_p \subset L$ be a finite extension. Prove from first principles and the above results that $L/\mathbb{F}_p$ is Galois. **[7]**

(e) Find explicitly an irreducible polynomial of degree 3 over $\mathbb{F}_5$. **[5]**

END