MA 3D50

THE UNIVERSITY OF WARWICK

THIRD YEAR EXAMINATION: June 2007

MA3D50 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.

Each question consists of 2 or 3 unrelated parts (a), (b), ...

1. (a) Let K be a field. Prove that every ideal in the polynomial ring $K[x]$ is generated by just one element. **[6]**

(b) (i) Prove that $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible. **[4]**

(ii) Let $\varepsilon := \exp(2\pi i/5)$, $L = \mathbb{Q}(\varepsilon) \subset \mathbb{C}$. Prove that there exists a unique field automorphism σ of L such that $\sigma(\varepsilon) = \varepsilon^2$. Briefly state results from the lectures that you're using. **[4]**

(iii) Prove that $L/\mathbb{Q}$ is Galois and that $\langle 1\rangle$, $\langle\sigma\rangle$, $\langle\sigma^2\rangle$ are precisely the subgroups of $G := \mathrm{Gal}(L/\mathbb{Q})$. Briefly state results from the lectures that you're using. **[5]**

(iv) Putting $\alpha := 2\varepsilon + \sqrt{5}$, prove $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\alpha)$. Briefly state results from the lectures that you're using. **[6]**

---

2. (a) In the following, briefly state results from the lectures that you're using.

(i) Put $f = x^6 + a\,x^5 + a\,x + 1 \in \mathbb{C}[x]$. Find an explicit $g \in \mathbb{C}[y]$ such that $x^{-3}f(x) = g(x + x^{-1})$. Prove that f can be solved by radicals. **[3]**

(ii) Prove or disprove the following. Put $h = x^5 + a\,x^4 + a\,x + 1 \in \mathbb{C}[x]$. Then h can be solved by radicals. **[4]**

(b) Let A be an integral domain and K its field of fractions.

(i) What does it mean, by definition, for an ideal in a ring to be a prime ideal? List without proof the prime ideals in the polynomial ring $\mathbb{C}[t]$. **[3]**

(ii) Let $P \subset A$ be a prime ideal, and let P^2 be the ideal of A generated by **[7]**

$$\{pq \mid p, q \in P\}.$$

Let $f = \sum_{k=0}^{n} a_k\,x^k \in A[x]$ be a polynomial such that

(1) $a_n \notin P$;
(2) $a_k \in P$ if $0 \le k < n$;
(3) $a_0 \notin P^2$.

Prove that f cannot be written gh with $g, h \in A[x]$ of degree $< n$.

(iii) State Gauss' lemma and deduce that if $f \in \mathbb{C}[t][x]$ is irreducible then it is irreducible in $\mathbb{C}(t)[x]$. **[3]**

(iv) Prove that $f := t^7 + x^5 + t\,x^3 + t \in \mathbb{C}(t)[x]$ is irreducible. **[5]**

---

3. (a) (i) Let $f = x^3 - 3\,x + 1$. Prove that f is irreducible in $\mathbb{Q}[x]$. **[3]**

(ii) Prove directly that if $\gamma \in \mathbb{C}$ is a root of f then so is $\gamma^2 - 2$. **[2]**

(iii) Let $\alpha \in \mathbb{C}$ be a root of f and put $K = \mathbb{Q}(\alpha)$. Prove that $K/\mathbb{Q}$ is a Galois extension. Briefly state results from the lectures that you're using. **[6]**

(iv) Choose yourself a nontrivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$ and write down its matrix with respect to the $\mathbb{Q}$-basis $(1, \alpha, \alpha^2)$ of K. **[4]**

(b) Let L/K be a field extension. Let A, B be subfields of L and suppose $K \subset A \cap B$. Let C be the subfield of L, generated by $A \cup B$.

(i) Prove or disprove the following. If A/K and B/K are finite, then so is C/K. **[6]**

(ii) A field extension Q/P is said to be *purely transcendental* (pt) if every element of $Q \setminus P$ is transcendental over P. **[4]**
Prove or disprove the following. If A/K and B/K are purely transcendental, then so is C/K.
[Hint. You may use that the field of rational functions $K(t)/K$ is pt.]

 Question 4 continued overleaf

---

4. (a) (i) Suppose that the polynomial $f = x^2 + px + q \in \mathbb{C}[x]$ factorizes as $f = (x+\alpha)(x+\beta)$. Compute $g = (x+\alpha+\beta^2)(x+\beta+\alpha^2)$ explicitly, giving its coefficients in terms of p, q. **[3]**

(ii) Prove or disprove the following. Let $f \in \mathbb{C}[x_1, \ldots, x_4]$ be a symmetric polynomial in four variables. Define $g_i \in \mathbb{C}[a,b,c]$ $(1 \le i \le 4)$ by **[3]**

$$\begin{aligned} g_1 &= a^2(b+c), \\ g_2 &= b^2(c+a), \\ g_3 &= c^2(a+b), \\ g_4 &= a^4+b^4+c^4. \end{aligned}$$

Then $h := f(g_1, g_2, g_3, g_4) \in \mathbb{C}[a,b,c]$ is symmetric.

(b) (i) Define the *characteristic* of a ring A. **[2]**

(ii) Let A be a ring of characteristic p, a prime number. Define $F : A \to A$ by $F(a) = a^p$. Prove that F is a ring homomorphism. **[4]**

(iii) Let A, F be as in (ii). Let $n \ge 0$ and $B = \{a \in A \mid F^n(a) = a\}$. Prove that B is a subring of A. **[2]**

(iv) Let p be a prime number, $n \ge 1$, $q = p^n$, $\mathbb{F}_p := \mathbb{Z}/p$ and let K be a splitting field of $h := x^q - x$ over $\mathbb{F}_p$. Prove that every element of K is a root of h. **[6]**

(v) Let L be a field of 8 elements. How many elements $a \in L$ satisfy $a^5 + a + 1 = 0$? **[5]**

---

5. (a) Let $n \geq 1$. Let $L = \mathbb{C}(t_1, \ldots, t_n)$ be the field of rational functions in n variables (that is, the field of fractions of the polynomial ring $\mathbb{C}[t_1, \ldots, t_n]$). Let the symmetric group act on L by

$$r(t_i) = t_{r(i)} \quad \text{and} \quad r(a) = a$$

for all $r \in S_n$, $i \in \{1, \ldots, n\}$, $a \in \mathbb{C}$.

(i) Give the definition of σ_k, the kth elementary symmetric polynomial of $t_1, \ldots, t_n$. **[2]**

(ii) We put $M = \mathbb{C}(\sigma_1, \ldots, \sigma_n) \subset L$ and **[8]**

$$K = L^{S_n} := \{f \in L \mid r(f) = f \text{ for all } r \in S_n\}.$$

State the main theorem of symmetric polynomials, and prove $K = M$.

(iii) Prove that L/K is Galois and $\mathrm{Gal}(L/K) \cong S_n$. Briefly state results from the lectures that you're using. **[3]**

(b) Recall that a field extension $K \subset L$ is separable if and only if no irreducible polynomial $f \in K[x]$ has a multiple root in L. **[7]**

Let p be a prime number, $\mathbb{F}_p$ a field of p elements, $L := \mathbb{F}_p(t)$ (rational functions), $K := \mathbb{F}_p(t^p) \subset L$. Is $K \subset L$ separable? Is it normal? Is it finite? Is it Galois?

(c) Let $K \subset L$ be fields. Let $\mathcal{F}$ denote the set of intermediate fields and $\mathcal{G}$ the set of subgroups of $G := \mathrm{Gal}(L/K)$.

(i) Define the map $\mathcal{F} \to \mathcal{G}$, $F \mapsto F^*$ that features in Galois theory. **[1]**

(ii) Let $F \in \mathcal{F}$ and $g \in G$. Prove that $gF^*g^{-1} = (gF)^*$. **[4]**
