THE UNIVERSITY OF WARWICK

THIRD YEAR EXAMINATION: JUNE 2003

GALOIS THEORY

Time Allowed: 3 hours

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

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.

1. a) Let $\alpha_1, \dots, \alpha_n$ be n quantities. Define the elementary symmetric functions σ_j in the α_i. Indicate briefly and without detailed proof the main result concerning symmetric polynomials in the α_i, and illustrate it by deriving the formula for the sum of squares $\sum \alpha_i^2$ in terms of the elementary symmetric functions σ_j. **[6]**

b) Let $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$; write down the quadratic equation satisfied by ω, and calculate ω^3. **[3]**

c) For $u, v \in \mathbb{C}$, calculate the elementary symmetric functions of the three quantities

$$u + v, \quad \omega u + \omega^2 v, \quad \omega^2 u + \omega v \qquad (*)$$

and write down the cubic polynomial $f(x)$ that has $(*)$ as its roots. **[8]**

d) Prove that $\sqrt[3]{4} - \sqrt[3]{2}$ is one root of a cubic over $\mathbb{Q}$, and determine the other two roots. **[8]**

2. a) Explain what is meant by saying that a point in the Euclidean plane is constructible by ruler and compass from a given set of points; state without proof a necessary condition for this to be the case, involving the degree of a certain field extension. **[6]**

b) Prove that an angle cannot in general be trisected using only ruler and compass. **[6]**

c) Establish the formula

$$\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta.$$

[Hint: Take real part in $(\cos + i\sin)^5$.] **[5]**

d) By choosing for example an angle θ such that $\cos 5\theta = \frac{5}{6}$, deduce that in general an angle cannot be divided into 5 equal parts using only ruler and compass. **[8]**

---

3. a) Define the Galois group $G = \mathrm{Gal}(K/k)$ of a finite field extension $k \subset K$. **[3]**

b) Assume that $K = k(\alpha)$ is a primitive extension; prove that the order of G satisfies $|G| \le [K : k]$, and state without proof the conditions under which equality holds. **[8]**

c) For an intermediate field $k \subset F \subset K$, we define F^* to be the set of automorphisms of K fixing F elementwise; for a subset $H \subset G$, we define $H^\dagger$ to be the set of elements of K fixed by every automorphism in H. Explain why F^* is a subgroup of G and $H^\dagger$ an intermediate field $k \subset H^\dagger \subset K$. Prove that

$$F^{*\dagger *} = F^*.$$

[5]

d) Find a splitting field K for the polynomial $x^3 - 3 \in \mathbb{Q}[x]$. Determine the Galois group of $K/\mathbb{Q}$, list its subgroups and describe all the fields between K and $\mathbb{Q}$. [You should assume the Main Theorem of Galois theory.] **[9]**

---

4. a) Write down all possible cycle types of permutations in the alternating group A_5. **[4]**

b) Express the following permutations as products of disjoint cycles:

$$(123)(345), \quad (12)(45)(23)(45) \quad \text{and} \quad (123)(234).$$

Deduce that A_5 can be generated by elements of order 2 only, and can also be generated by elements of order 3 only. **[5]**

c) Deduce that A_5 cannot map surjectively to any nontrivial cyclic group, and hence prove that A_5 and the symmetric group S_5 are not soluble. **[4]**

d) For each integer $n \geq 2$, prove that the polynomial

$$f_n(x) = x^5 - 3nx + 3 \in \mathbb{Q}[x]$$

has Galois group over $\mathbb{Q}$ isomorphic to S_5. Are any of the equations $f_n(x) = 0$ soluble by radicals? **[12]**

[You may use results from the course, provided that you state them clearly.]

---

5. Argued true-false:

(i) For every field k there exists a homomorphism $\mathbb{Z} \to k$ with image the prime subfield of k. **[4]**

(ii) $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$. **[4]**

(iii) If K_1 and K_2 are subfields of $\mathbb{C}$ such that $\mathrm{Gal}(K_1/\mathbb{Q})$ and $\mathrm{Gal}(K_2/\mathbb{Q})$ are isomorphic then $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$. **[4]**

(iv) A field extension of degree 2 is always normal. **[4]**

(v) A finite field is a primitive extension of its prime subfield. [You may cite structure theorems for finite fields without proof.] **[4]**

(vi) If $f \in \mathbb{Q}[x]$ is an irreducible polynomial of degree n then the n roots $\alpha_1, \ldots, \alpha_n$ of f in $\mathbb{C}$ are distinct. **[4]**

(vii) If $f \in k[x]$ is an irreducible polynomial of degree n then a splitting field K of f over k has degree $[L : K] = n!$. **[4]**

(viii) For any field k, $k[x]$ contains infinitely many irreducible monic polynomials. **[4]**

[Credit will only be given for the quality of your argument, and only up to 25 marks.]
