SCHOOL OF MATHEMATICS AND STATISTICS

Spring Semester 2000–01 **$2\frac{1}{2}$ hours**

Galois Theory

Answer ***Question 1*** *and three other questions. You are advised* ***not*** *to answer more than three of the questions 2 to 5: if you do, only your best three will be counted.*

1 (i) Let L be a field. What is an *automorphism* of L? If $K \subseteq L$ is a subfield of L, what does it mean for an automorphism of L to be a K-*automorphism*? ***(3 marks)***

(ii) If $K \subseteq L$ is a field extension, define its *Galois group*, and say what it means, in terms of this group, for $K \subseteq L$ to be a *Galois extension.* Give an equivalent formulation involving splitting fields. ***(3 marks)***

(iii) Let $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(a) Write down the K-automorphisms of L. Is the extension $K \subseteq L$ Galois? ***(3 marks)***

(b) It is given that $\mathrm{Gal}(L/\mathbb{Q})$ has order four. Write down the effect of each of the four elements of the group on $\sqrt{2}$ and $\sqrt{5}$. ***(4 marks)***

(c) Which of these four elements lie in $\mathrm{Gal}(L/K)$? ***(1 mark)***

(iv) Determine the degrees of the splitting fields over $\mathbb{Q}$ of the following polynomials:

(a) $x^4 - 3$; ***(3 marks)***

(b) $x^4 + x^2 + 1$. ***(4 marks)***

(v) Write down

(a) $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})|$; ***(1 mark)***

(b) $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|$. ***(1 mark)***

(vi) Suppose that $K \subseteq M \subseteq L$ are field extensions and that the extension $K \subseteq L$ is Galois. One of $K \subseteq M$ and $M \subseteq L$ is automatically also Galois. Which is it? Give a brief explanation for your answer. ***(2 marks)***

2 Let $n \geq 1$ be an integer and let $\lambda_n \in \mathbb{C}[x]$ denote the nth cyclotomic polynomial. That is,

$$\lambda_n = \prod (x - \zeta),$$

where ζ runs over the distinct, primitive nth roots of unity.

(i) Show that

$$x^n - 1 = \prod_{d|n} \lambda_d.$$

(4 marks)

(ii) Explicitly compute a polynomial in $\mathbb{Q}[x]$ of degree 6 with $e^{4\pi i/9}$ as a root. Show directly that your polynomial is irreducible over $\mathbb{Q}$, stating clearly any results that you use. ***(8 marks)***

(iii) Show that each cube root of a primitive 9th root of unity is a primitive 27th root of unity, and that all primitive 27th roots of unity occur in this way. Deduce that $\lambda_{27}(x) = \lambda_9(x^3)$. Hence write down $\lambda_{27}(x)$. ***(11 marks)***

(iv) Verify the formula of (i) in the case $n = 27$. ***(2 marks)***

3 Let $f = x^4 - 2x^2 - 6 \in \mathbb{Q}[x]$ and let M denote the splitting field of f over $\mathbb{Q}$. Let $\alpha = \sqrt{1 + \sqrt{7}}$.

(i) Show that the roots of f are $\pm\alpha$, $\pm\dfrac{i\sqrt{6}}{\alpha}$, and deduce that $M = \mathbb{Q}(\alpha, i\sqrt{6})$. ***(4 marks)***

(ii) It is given that $[M : \mathbb{Q}] = 8$. Specify the elements of $\mathrm{Gal}(M/\mathbb{Q})$ by giving their effect on each of α and $i\sqrt{6}$, justifying your answer. ***(8 marks)***

(iii) Show that there exist automorphisms $\phi, \psi \in \mathrm{Gal}(M/\mathbb{Q})$ such that ϕ has order 4, ψ has order 2, and $\mathrm{Gal}(M/\mathbb{Q}) = \langle \phi, \psi \rangle$. ***(5 marks)***

(iv) Write $\psi\phi\psi^{-1}$ in the form $\phi^i\psi^j$. To which well-known group is $\mathrm{Gal}(M/\mathbb{Q})$ isomorphic? ***(3 marks)***

(v) Write $L = \mathbb{Q}(\alpha + \dfrac{i\sqrt{6}}{\alpha})$. Using the Galois correspondence, find $[L : \mathbb{Q}]$. ***(5 marks)***

4 Let $n > 2$ be an integer and let ζ denote a primitive nth root of unity.

(i) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$, the group of units in $\mathbb{Z}_n$. ***(6 marks)***

(ii) Write down $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. ***(1 mark)***

(iii) Let $\beta = \zeta + \dfrac{1}{\zeta}$. Show that ζ satisfies a quadratic equation with coefficients in $\mathbb{Q}(\beta)$. Show also that $\mathbb{Q}(\beta) \subset \mathbb{R}$, and deduce that $\zeta \notin \mathbb{Q}(\beta)$. ***(6 marks)***

(iv) What is $|\mathrm{Gal}(\mathbb{Q}(\beta)/\mathbb{Q})|$? Justify your answer. ***(2 marks)***

(v) In the particular case $n = 9$, deduce that $\mathrm{Gal}(\mathbb{Q}(\beta)/\mathbb{Q}) \cong C_3$.

Solve $x^3 - 3x + 1 = 0$ and write the three roots in the form $\zeta^r + \zeta^{-r}$ for certain integers r.

Show that, for all integers $r \geq 1$ there is a polynomial $P_r(x) \in \mathbb{Q}[x]$ such that $\zeta^r + \zeta^{-r} = P_r(\beta)$, and deduce that the splitting field of $x^3 - 3x + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\beta)$. ***(10 marks)***

5 (i) Let p be a prime number. Let G be a transitive subgroup of S_p (i.e. for any $a, b \in \{1, \ldots, p\}$ there exists $\theta \in G$ with $\theta(a) = b$) which contains a transposition. Prove that $G = S_p$. ***(11 marks)***

(ii) Show that the Galois group of $3x^7 - 7x^6 - 7x^3 + 21x^2 - 7$ over $\mathbb{Q}$ is isomorphic to S_7. ***(14 marks)***

End of Question Paper