SCHOOL OF MATHEMATICS AND STATISTICS

Spring Semester 2002–03 2 hours 30 minutes

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 $K \subseteq L$ be a field extension. What does it mean for $\phi : L \longrightarrow L$ to be a K-*automorphism* of L? ***(3 marks)***

(ii) If $K \subseteq L$ is a field extension, define its *Galois group*. What does it mean to say that $K \subset L$ is a *Galois* extension? ***(3 marks)***

(iii) Let $f(x)$ denote the polynomial $x^4 + 3$, and let $g(x)$ denote the polynomial $x^4 + 4$, both regarded as polynomials over $\mathbb{Q}$.

(a) Determine the splitting fields of these two polynomials. ***(4 marks)***

(b) Hence write down the degree of each of the splitting fields over $\mathbb{Q}$. ***(3 marks)***

(c) Exactly one of f and g is irreducible. Say which it is, giving a reason. ***(2 marks)***

(iv) Write down

(a) $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})|$. ***(1 mark)***

(b) $|\mathrm{Gal}(\mathbb{Q}(4^{1/3})/\mathbb{Q})|$. ***(1 mark)***

(c) $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$, where ζ is a primitive nth root of unity, for some integer $n \geq 1$. ***(1 mark)***

(v) Suppose that $K \subseteq M \subseteq L$ are field extensions and that the extension $K \subseteq L$ is Galois. When is L/M Galois? Give a reason for your answer. When is M/K Galois? Give an example of fields $K \subseteq M \subseteq L$ with L/K Galois, but with M/K not Galois. ***(4 marks)***

(vi) Let K be a field and let $f \in K[x]$ be a non-constant polynomial. What does it mean to say that the equation $f(x) = 0$ is *soluble by radicals over* K? ***(3 marks)***

2 Let $f(x)$ denote the quartic $x^4 + 2x^2 + 4x + 2$ (regarded as a polynomial over $\mathbb{Q}$).

(i) Explain why $f(x)$ is irreducible. Write down its resolvent cubic, and factorise this cubic completely. ***(4 marks)***

(ii) Briefly explain the algorithm to solve a quartic equation, and illustrate the method by finding the solutions to the equation $f(x) = 0$. ***(8 marks)***

(iii) What is the splitting field of f? If K denotes this splitting field, what is $[K : \mathbb{Q}]$? Why is $K/\mathbb{Q}$ Galois, and how many elements does $\mathrm{Gal}(K/\mathbb{Q})$ have? ***(3 marks)***

(iv) Let α_1, α_2, α_3 and α_4 denote the four roots of f. Write down the $\mathbb{Q}$-automorphisms of K, and determine the permutation of the roots corresponding to each element of the Galois group. What is the structure of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$? ***(6 marks)***

(v) Define the *discriminant* of a quartic equation in terms of the roots of the quartic. Using the expressions for the roots that you found above, compute the discriminant of the quartic f. Explain how this helps you to check your answer to the last part of (iv). ***(4 marks)***

3 (i) Let n be a positive integer. Show that

$$x^n - 1 = \prod_{d|n} \lambda_d(x),$$

where $\lambda_d(x)$ is the dth cyclotomic polynomial, which you should define.

Deduce that $n = \sum_{d|n} \phi(d)$. ***(6 marks)***

(ii) Explicitly compute a polynomial of degree six in $\mathbb{Q}[x]$ that has $e^{\pi i/9}$ as a root. ***(5 marks)***

(iii) By making a substitution and using Eisenstein's criterion, show that your polynomial is irreducible in $\mathbb{Q}[x]$. ***(4 marks)***

(iv) Let $n \geq 1$ be an integer and let ζ be a primitive nth root of unity. Show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$. ***(7 marks)***

(v) Is $\mathrm{Gal}(\mathbb{Q}(e^{\pi i/9})/\mathbb{Q})$ cyclic? Justify your assertion. ***(3 marks)***

4 Let $\zeta = e^{\frac{2\pi i}{7}}$. Write $\beta = \zeta + \zeta^{-1} = \zeta + \zeta^6$ and $\gamma = \zeta + \zeta^2 + \zeta^4$.

(i) Recall that $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Hence find a cubic equation satisfied by β. ***(5 marks)***

(ii) Using de Moivre's Theorem, show that $\beta = 2\cos\left(\frac{2\pi}{7}\right)$. ***(2 marks)***

(iii) Expand γ^2 as a series in ζ, and show that $\gamma^2 + \gamma + 2 = 0$. ***(6 marks)***

(iv) Deduce that $\mathbb{Q}(\sqrt{-7}) \subseteq \mathbb{Q}(\zeta)$. ***(2 marks)***

(v) Use the result of Question 3(iv) to deduce that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic with six elements. ***(3 marks)***

(vi) By (v), we can write $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ for some automorphism θ. Write down the subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Draw the subgroup lattice for this group. (You may assume that any subgroup of a cyclic group is again cyclic.) ***(4 marks)***

(vii) Using the earlier parts of the question, draw the corresponding subfield lattice. ***(3 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 $G = S_p$. ***(12 marks)***

(ii) Show that the Galois group of $x^5 - 20x + 20$ over $\mathbb{Q}$ is isomorphic to S_5. ***(11 marks)***

(iii) Explain briefly why S_5 is not a soluble group. ***(2 marks)***

End of Question Paper