The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2010–2011**

Galois theory **2 hours 30 minutes**

*Answer **four** questions. You are advised **not** to answer more than four questions: if you do, only your best four will be counted.*

1 (a) Define what is meant by an *automorphism* of a field. ***(3 marks)***

(b) Let K be an extension field of $\mathbb{Q}$, and let ϕ be an automorphism of K. Prove that $\phi(q) = q$ for all $q \in \mathbb{Q}$. ***(5 marks)***

(c) Define the *Galois group* $G(L/K)$ for a field extension $K \leq L$. ***(2 marks)***

(d) Show that $G(\mathbb{Q}(i)/\mathbb{Q})$ is a cyclic group of order two. (Your proof should be complete and self-contained, except that you may assume part (b).) ***(9 marks)***

(e) Give an example of an extension $K \leq L$ where $[L : K] = 4$ but $|G(L/K)| = 2$. Justify your answer. ***(6 marks)***

2 Put $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(a) Give a basis for L over $\mathbb{Q}$. (You need not prove that your answer is correct.) ***(3 marks)***

(b) List the elements of the group $G(L/\mathbb{Q})$, and show that $|G(L/\mathbb{Q})| = [L : \mathbb{Q}]$. To which well-known group is $G(L/\mathbb{Q})$ isomorphic? ***(5 marks)***

(c) For each of the following fields K_i, determine the subgroup $H_i \leq G(L/\mathbb{Q})$ that corresponds to K_i under the Galois correspondence.

$$K_1 = \mathbb{Q}(\sqrt{10}) \qquad K_2 = \mathbb{Q}(\sqrt{6}, \sqrt{15}) \qquad K_3 = \mathbb{Q}(\sqrt{2} + \sqrt{5}) \qquad K_4 = \mathbb{Q}(\sqrt{30})$$

(6 marks)

(d) Use the Galois correspondence to show that $K_1 \leq K_3$, then prove the same thing by a direct calculation. ***(4 marks)***

(e) How many fields M are there with $\mathbb{Q} < M < L$ and $[M : \mathbb{Q}] = 4$? ***(4 marks)***

(f) Show that if $f(x) \in \mathbb{Q}[x]$ is an irreducible monic polynomial of degree 3, then $f(x)$ has no roots in L. ***(3 marks)***

3 (a) Define the cyclotomic polynomial $\phi_n(x)$. ***(2 marks)***

(b) State the rule relating the polynomials $\phi_n(x)$ to the polynomials $x^m - 1$. ***(2 marks)***

(c) Find $\phi_2(x)$, $\phi_4(x)$ and $\phi_8(x)$, then state and prove a general formula for $\phi_{2^k}(x)$. ***(6 marks)***

(d) Put

$$\zeta = \frac{\sqrt{2+\sqrt{2}} + \sqrt{2-\sqrt{2}}\, i}{2}.$$

Show that $\phi_{16}(\zeta) = 0$, and thus that $\mathbb{Q}(\zeta) = \mathbb{Q}(\mu_{16})$. ***(6 marks)***

(e) Prove that $\mathbb{Q}(i) \leq \mathbb{Q}(\zeta)$ and that $G(\mathbb{Q}(\zeta)/\mathbb{Q}(i))$ is a cyclic group of order 4. You may assume general facts about cyclotomic fields and their Galois groups, provided that you state them clearly. ***(9 marks)***

4 Put $f(x) = x^3 - 12x - 34$.

(a) State Eisenstein's criterion, and use it to prove that $f(x)$ is irreducible over $\mathbb{Q}$. ***(4 marks)***

(b) Calculate $f(x)$ and $f'(x)$ for $x = -2$, $x = 2$ and $x = 5$. By considering the shape of the graph, show that $f(x)$ has precisely one real root, say α. ***(5 marks)***

(c) Show that $\alpha = 2^{5/3} + 2^{1/3}$. ***(4 marks)***

(d) Let the other two roots be β and γ, and put $K = \mathbb{Q}(\alpha, \beta, \gamma)$. Show that $G(K/\mathbb{Q})$ contains an element of order two, and deduce that $G(K/\mathbb{Q})$ is the full group of permutations of the set $\{\alpha, \beta, \gamma\}$. ***(6 marks)***

(e) Calculate the numbers

$$\begin{aligned} s_1 &= \alpha + \beta + \gamma \\ s_2 &= \alpha\beta + \beta\gamma + \gamma\alpha \\ s_3 &= \alpha\beta\gamma. \end{aligned}$$

(3 marks)

(f) Calculate $\alpha^2 + \beta^2 + \gamma^2$ (by relating it to s_1, s_2 and s_3). ***(3 marks)***

5 (a) Give a detailed statement, without proof, of the Galois correspondence. You should include information about orders of subgroups, degrees and Galois groups of intermediate field extensions, conjugacy and containment between subgroups, and normality of field extensions. ***(11 marks)***

(b) Suppose we have a normal extension L/K such that $G(L/K)$ is cyclic of order 30. Prove that for each positive integer d that divides 30, there is a unique field M_d with $K \subseteq M_d \subseteq L$ and $[M_d : K] = d$. Prove also that M_d is normal over K. ***(9 marks)***

(c) Suppose we have a normal extension L/K with $|G(L/K)| = 105$ and subgroups $A, B \leq G(L/K)$ with $|A| = 21$ and $|B| = 35$. Prove that $L^A \cap L^B = K$. ***(5 marks)***

End of Question Paper