The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2011–2012**

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) Explain what is meant by the following. ***(7 marks)***

(1) A *homomorphism* of fields.

(2) The *degree* of a homomorphism.

(3) An *automorphism* of a field.

(4) The *Galois group* of a field extension.

(b) Show that any homomorphism of fields is injective. ***(5 marks)***

(c) Let N/K be a field extension of finite degree. Explain what it means for N to be *normal* over K. You should give one criterion in terms of roots of polynomials, and another criterion in terms of numbers of homomorphisms. ***(5 marks)***

(d) Which of the following fields are normal over $\mathbb{Q}$? Justify your answers briefly. ***(8 marks)***

$$L_1 = \mathbb{Q}(\sqrt{11}, \sqrt{13})$$
$$L_2 = \mathbb{Q}(e^{2\pi i/11})$$
$$L_3 = \mathbb{Q}(2^{1/11})$$
$$L_4 = \mathbb{Q}\left(\sqrt{3+\sqrt{7}}\right)$$

2 (a) Let p be a prime number, and let $f(x)$ be an irreducible monic polynomial of degree p over $\mathbb{Q}$. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Suppose that $f(x)$ has precisely $p-2$ real roots. Prove that the Galois group $G(K/\mathbb{Q})$ contains a transposition. ***(2 marks)***

(b) Let R be the set of complex roots of $f(x)$, and define a relation on R by declaring that $\alpha \sim \beta$ if either $\alpha = \beta$ or the transposition $(\alpha\ \beta)$ lies in $G(K/\mathbb{Q})$. Show that this is an equivalence relation, and that all equivalence classes have the same size. ***(10 marks)***

(c) Deduce that $G(K/\mathbb{Q})$ is isomorphic to the whole symmetric group Σ_p. ***(3 marks)***

(d) Now let $L \subseteq \mathbb{C}$ be a normal extension of $\mathbb{Q}$ such that $G(L/\mathbb{Q}) \simeq C_5$. Let α be any element of L that does not lie in $\mathbb{Q}$, and let $g(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Show that $g(x)$ must have degree 5, and that it must split over L. ***(5 marks)***

(e) Now show (using ideas from (a), or otherwise) that $g(x)$ must have five real roots. ***(5 marks)***

3 Consider the polynomial $f(x) = x^4 - 24x^2 + 4$. Some of the values of f are as follows:

x	0	1	2	3	4	5
$f(x)$	4	-19	-76	-131	-124	29

(a) Use the above table to show that f has four real roots and no integer roots. ***(4 marks)***

(b) Suppose we have a factorisation $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Show that $c = -a$ and either $a = 0$ or $b = d$. By continuing this analysis further, show that a, b, c and d cannot all be integers. ***(7 marks)***

(c) Deduce that $f(x)$ is irreducible over $\mathbb{Q}$, stating carefully any general results that you use. ***(5 marks)***

(d) Now let α be the largest real root of $f(x)$. Put $\beta = \frac{1}{2}\alpha^2 - 6$ and $\gamma = \frac{1}{4}\alpha(\alpha^2 - 22)$. Simplify β^2 and γ^2, and show that they are integers. ***(6 marks)***

(e) Use (d) to find primes p and q such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. ***(3 marks)***

4 Put $\zeta = e^{2\pi i/21}$ and $L = \mathbb{Q}(\zeta)$.

(a) State a general theorem about Galois groups of cyclotomic fields. Use it to show that there are automorphisms $\rho, \tau \in G(L/\mathbb{Q})$ such that $\rho^6 = \tau^2 = 1$ and

$$G(L/\mathbb{Q}) = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \tau, \rho\tau, \rho^2\tau, \rho^3\tau, \rho^4\tau, \rho^5\tau\}.$$

(8 marks)

(b) Give a formula for the cyclotomic polynomial $\varphi_{21}(x)$ in terms of polynomials of the form $x^k - 1$. (You need not carry out the relevant divisions.) ***(4 marks)***

(c) You may assume that

$$\sqrt{-3} = \zeta^7 - \zeta^{-7}$$
$$\sqrt{-7} = -(\zeta^3 - \zeta^{-3})(\zeta^6 - \zeta^{-6})(\zeta^9 - \zeta^{-9}).$$

Use this to find $\rho(\sqrt{-3})$, $\tau(\sqrt{-3})$, $\rho(\sqrt{-7})$ and $\tau(\sqrt{-7})$. ***(6 marks)***

(d) Use the Galois correspondence to show that there is a unique field K with $\mathbb{Q} < K < L$ and $[K : \mathbb{Q}] = 4$. Give generators for that subfield. ***(7 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. ***(10 marks)***

(b) List all the elements of the alternating group A_4 and their orders. ***(3 marks)***

(c) List all the subgroups of A_4, and state which of them are normal. In particular, you should show that there is a unique subgroup of order 4. You may assume without proof that there are no subgroups of order 6. ***(8 marks)***

(d) Let L be a normal extension of $\mathbb{Q}$ such that the Galois group $G(L/\mathbb{Q})$ is isomorphic to A_4. What can we deduce about the subfields of L? You should give as many details as possible, but you need not justify them. ***(4 marks)***

End of Question Paper