The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2012-2013**

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 Let $K \subseteq L$ be an algebraic field extension. This extension need not be finite, and K need not have characteristic 0.

(i) Define the Galois group of L over K. ***(3 marks)***

(ii) Describe the connection between field homomorphisms $L \to L$, K-algebra homomorphisms $L \to L$ and elements of the Galois group. ***(3 marks)***

(iii) Define what it means for the extension to be normal and define what it means to be a Galois extension. ***(6 marks)***

(iv) Name (without proof) at least two different properties of a finite extension $K \subseteq L$ that are equivalent to $K \subseteq L$ being a Galois extension. ***(5 marks)***

(v) Give a detailed statement (without proof) of the Galois correspondence. Your answer should contain information about orders of subgroups, degrees and orders of intermediate field extensions, conjugacy and containment between subgroups, and normality of field extensions. ***(8 marks)***

2 Consider the real numbers $\alpha = \sqrt{4+\sqrt{7}}$, $\beta = \sqrt{4-\sqrt{7}}$ and let L be the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$.

(i) Determine a quartic polynomial P_α over $\mathbb{Q}$ such that $P_\alpha(\alpha) = 0$. In the following, you may assume that P_α is irreducible. ***(3 marks)***

(ii) Show that $\pm\alpha$ and $\pm\beta$ are roots of P_α. Find expressions for $\alpha \cdot \beta$, $(\alpha+\beta)^2$ and $(\alpha-\beta)^2$. ***(5 marks)***

(iii) Show that β is an element of L and write β as a $\mathbb{Q}$-linear combination of the basis $\{1, \alpha, \alpha^2, \alpha^3\}$ of L. ***(6 marks)***

(iv) Show that the extension $\mathbb{Q} \subseteq L$ is a Galois extension and determine the structure of the Galois group $Gal(L|\mathbb{Q})$. ***(5 marks)***

(v) Find all intermediate extensions M with $\mathbb{Q} \subseteq M \subseteq L$. Justify your answer. ***(6 marks)***

3 Consider the polynomial $P(X) = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$. Recall the existence of the Frobenius homomorphism $K \to K$, $a \mapsto a^2$ in any field K of characteristic 2.

(i) Show that if a is a root of P in an extension of $\mathbb{F}_2$, then so is a^2. ***(3 marks)***

(ii) List all irreducible polynomials in $\mathbb{F}_2[X]$ of order two and use this list to show that P is irreducible. ***(4 marks)***

(iii) Write a^4, a^6 and a^8 in terms of the basis $\{1, a, a^2, a^3\}$ of $\mathbb{F}_2(a)$. Deduce that the elements a, a^2, a^4 and a^8 are pairwise distinct. ***(7 marks)***

(iv) Use (iii) to show that $a^{16} = a$ and that $Gal(\mathbb{F}_2(a)|\mathbb{F}_2)$ must contain an element of order 4. ***(5 marks)***

(v) Conclude that $\mathbb{F}_2(a)$ is a splitting field for P and $Gal(\mathbb{F}_2(a)|\mathbb{F}_2) \cong \mathbb{Z}_4$, the cyclic group of order 4. ***(6 marks)***

4 Let D_4 be the group with elements $\{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ and the composition rules $\tau^2 = e$, $\sigma^4 = e$, $\tau\sigma = \sigma^3\tau$.

(i) Determine the order of all elements of D_4 (you should find five involutions, i.e. elements $g \in D_4 \setminus \{e\}$ with $g^2 = e$). ***(4 marks)***

(ii) You may assume that D_4 has precisely 10 subgroups, precisely three of which have order 4. Give a complete list of these subgroups. For each subgroup H, you should list the elements of H and give the name of a standard group that is isomorphic to H. ***(8 marks)***

(iii) Which of the subgroups of D_4 is normal? ***(7 marks)***

(iv) Let $K \subseteq L$ be a finite Galois extension with Galois group D_4. What can you deduce about the intermediate extensions M with $K \subseteq M \subseteq L$ and their various containment relations? You should prove your answer by referring to known theorems. ***(6 marks)***

5 Let $L = \mathbb{Q}(i, \sqrt{3}, \sqrt{11})$.

(i) Give a basis for L over $\mathbb{Q}$. You need not prove that your answer is correct. ***(2 marks)***

(ii) Determine the elements of $Gal(L|\mathbb{Q})$ and show that $|Gal(L|\mathbb{Q})| = [L : \mathbb{Q}]$. Deduce that $\mathbb{Q} \subseteq L$ is a Galois extension and give an explicit isomorphism $Gal(L|\mathbb{Q}) \cong \mathbb{Z}_2^3$. ***(8 marks)***

(iii) Determine the subgroups of $Gal(L|\mathbb{Q})$ that correspond, via the Galois correspondence, to the subfields

$$K_1 = \mathbb{Q}(\sqrt{3} + \sqrt{11}),\ K_2 = \mathbb{Q}(i, \sqrt{33}),\ K_3 = \mathbb{Q}(i\sqrt{33}).$$

Are all of these fields Galois extensions of $\mathbb{Q}$? ***(7 marks)***

(iv) How many intermediate fields M with $\mathbb{Q} \subseteq M \subseteq L$ exist such that $[M : \mathbb{Q}] = 4$? Justify your answer. ***(4 marks)***

(v) Show that, if $P \in \mathbb{Q}[X]$ is any irreducible polynomial of odd degree, then P has no root in L. ***(4 marks)***

End of Question Paper