The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2013–2014**

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.*

Please leave this exam paper on your desk
Do not remove it from the hall

Registration number from U-Card (9 digits)
to be completed by student

Blank

1 (i) Consider the cubic equation

$$t^3 + pt + q = 0, \qquad (*)$$

where p and q are real numbers.

(a) Show that if $(*)$ has repeated roots then $4p^3 + 27q^2 = 0$.

(b) Show that if $(*)$ has one real and two (non-real) complex roots, then $4p^3 + 27q^2 > 0$. **(9 marks)**

(ii) Define the following concepts:

- the characteristic of a field,
- a homomorphism of fields,
- the degree of a homomorphism of fields,
- an automorphism of a field,
- an ideal in a ring.

(9 marks)

(iii) Suppose that $\varphi\colon K \to L$ is a homomorphism of fields.

(a) Show that φ is injective.

(b) Show that K and L have the same characteristic. **(7 marks)**

2 A polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ is *primitive* if the greatest common divisor of $a_0, \ldots, a_d$ is 1.

(a) Prove that if $f(x)$ and $g(x)$ are primitive polynomials in $\mathbb{Z}[x]$, then so is $f(x)g(x)$. **(5 marks)**

(b) Let $q(x)$ be a monic polynomial in $\mathbb{Z}[x]$, and suppose that there is a factorisation $q(x) = f(x)g(x)$ with both of $f(x)$ and $g(x)$ monic polynomials in $\mathbb{Q}[x]$.

Show that in fact $f(x)$ and $g(x)$ lie in $\mathbb{Z}[x]$. **(7 marks)**

(c) List the quadratic polynomials over $\mathbb{F}_2$ and establish whether they are reducible or irreducible. **(4 marks)**

(d) Show that the polynomial $x^5 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$.

Deduce, using (b) and (c) or otherwise, that the polynomial $x^5 + x^2 + 1$ is also irreducible in $\mathbb{Q}[x]$. **(9 marks)**

3 (a) Let L and M be fields, and let $\theta_1, \ldots, \theta_n \colon L \to M$ be n distinct homomorphisms. Let $b_1, \ldots, b_n \in M$ and suppose that for all $a \in L$ we have

$$\sum_{i=1}^{n} b_i \theta_i(a) = 0.$$

Show that $b_1 = b_2 = \cdots = b_n = 0$. **(10 marks)**

(b) Now let K be another field and let $\varphi \colon K \to L$ and $\psi \colon K \to M$ be field homomorphisms with $\deg(\varphi) < \infty$.

Write $E(\varphi, \psi)$ for the set of homomorphisms $\theta \colon L \to M$ with $\theta\varphi = \psi$.

Using (a) or otherwise, show that $|E(\varphi, \psi)| \leqslant \deg(\varphi)$. **(10 marks)**

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

4 Put $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})$.

(a) Write down a basis for L over $\mathbb{Q}$. (You are not asked to prove that your answer is correct.) **(3 marks)**

In the rest of the question you may assume without proof that $L/\mathbb{Q}$ is Galois.

(b) List without proof the elements of the group $G(L/\mathbb{Q})$. To which well-known group is $G(L/\mathbb{Q})$ isomorphic? **(6 marks)**

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

$K_1 = \mathbb{Q}(\sqrt{14})$, $K_2 = \mathbb{Q}(\sqrt{6}, \sqrt{21})$, $K_3 = \mathbb{Q}(\sqrt{2} + \sqrt{7})$, $K_4 = \mathbb{Q}(\sqrt{42})$.

(7 marks)

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

(e) How many fields M are there with $\mathbb{Q} < M < L$ and $[M : \mathbb{Q}] = 4$? **(5 marks)**

5 Consider the polynomial $f(x) = x^4 + 8x^2 - 2 \in \mathbb{Q}[x]$.

Define $\alpha = \sqrt{3\sqrt{2} - 4}$, and $M = \mathbb{Q}(\alpha, \sqrt{-2})$.

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$, stating clearly, without proof, any general criterion which you use. **(5 marks)**

(b) Show that $f(x)$ has roots $\pm\alpha, \pm\sqrt{-2}/\alpha$. Deduce that M is a splitting field for $f(x)$. **(7 marks)**

(c) Show that $\mathbb{Q}(\alpha) = M \cap \mathbb{R} \neq M$, and deduce that $[M : \mathbb{Q}] = 8$. **(5 marks)**

(d) Show that there exist automorphisms $\varphi, \psi \in G(M/\mathbb{Q})$ such that φ has order 4, ψ has order 2, and $G(M/\mathbb{Q}) = \langle \varphi, \psi \rangle$. **(8 marks)**

End of Question Paper