Queen Mary
University of London

Main Examination period 2017

MTH745P/U: Further Topics in Algebra (Fields and Galois Theory)

Duration: 3 hours

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

You should attempt ALL questions. Marks available are shown next to the questions.

Calculators are not permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Complete all rough work in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it shall be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiners: J. N. Bray and A. R. Fink

Question 1. [30 marks] Let L and K be two fields with $L \geqslant K$.

(a) Show that L is a vector space over K. **[4]**

(b) Define the **degree** $[L : K]$ of L over K. **[2]**

(c) What does it mean for $\alpha \in L$ to be **algebraic** over K, and what does it mean for α to be **transcendental** over K? **[3]**

(d) What does it mean for a field extension $L : K$ to be (i) **finite**; and (ii) **algebraic**? Show that every finite field extension is algebraic. **[5]**

(e) Suppose α is algebraic over K. Define the **minimal polynomial** of α over K. **[3]**

(f) Suppose α is algebraic over K, and has minimal polynomial $m(X)(\in K[X])$ over K.

(i) Prove that $m(X)$ is irreducible over K.

(ii) State a relationship between the degree of $m(X)$ and the degree of the field extension $K(\alpha) : K$.

(iii) Show that if $f(X) \in K[X]$ satisfies $f(\alpha) = 0$ then $m(X) \mid f(X)$ (in $K[X]$). **[8]**

(g) State the **(Short) Tower Law** for (finite) field extensions. **[2]**

(h) Write down (without proof) bases for $\mathbb{F}_2(t, \omega)$ over

(i) $\mathbb{F}_2(t^3)$;

(ii) $\mathbb{F}_2(t)$;

(iii) $\mathbb{F}_2(t^3, \omega)$.

Here, t is transcendental over $\mathbb{F}_2$ and ω is an element (not in $\mathbb{F}_2$) satisfying $\omega^2 + \omega + 1 = 0$. Note that $\mathbb{F}_2(t, \omega) = \mathbb{F}_2(t^3)[t, \omega]$. **[3]**

Question 2. [20 marks] Let K be a field in which $2 \neq 0$, and let $D \in K$ be a non-square in K. Let $S := \{\lambda^2 : \lambda \in K\}$ denote the set of squares in K.

(a) Give, with proof, a condition that $\lambda \in K \setminus S$ be a square in $K(\sqrt{D})$. **[4]**

(b) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ has degree 4 over $\mathbb{Q}$. [You may assume that 2, 5 and 10 are non-squares in $\mathbb{Q}$.] **[4]**

(c) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$, and find the minimal polynomial for $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$. **[6]**

(d) Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are not isomorphic (as fields). **[4]**

(e) Write down an isomorphism from $\mathbb{F}_2(t)$ to its proper subfield $\mathbb{F}_2(t^2)$ (where t is transcendental over $\mathbb{F}_2$). **[2]**

Question 3. [20 marks] Let K be a field.

(a) Define the **formal derivative** $\mathrm{D}f$ for any $f = f(X) \in K[X]$. **[3]**

(b) Prove the following properties of the operator D:

(i) $\mathrm{D}(f+g) = \mathrm{D}f + \mathrm{D}g$,

(ii) $\mathrm{D}(fg) = f(\mathrm{D}g) + (\mathrm{D}f)g$, and

(iii) $\mathrm{D}(\lambda f) = \lambda(\mathrm{D}f)$,

for all $f, g \in K[X]$ and $\lambda \in K$. **[4]**

(c) Let L be a splitting field over K for f. Prove that f has a multiple root in L if and only both f and $\mathrm{D}f$ are divisible by some non-constant polynomial in $L[X]$. **[8]**

(d) Show that if K has characteristic 0, then $\mathrm{D}f = 0$ if and only if f is constant. **[3]**

(e) State a necessary and sufficient condition for $\mathrm{D}f = 0$ in the case where K has characteristic p, with $p > 0$. **[2]**

Question 4. [10 marks] Let K be a finite field.

(a) Characterise, up to isomorphism, the fields which can arise as the prime subfield of K. **[2]**

(b) Briefly explain why K must have prime power order. **[2]**

(c) Prove that the multiplicative group of K is cyclic. [You may assume that each nonzero element x of K satisfies $x^{q-1} - 1 = 0$, where K has size q.] **[6]**

Question 5. [20 marks]

(a) State the Fundamental Theorem of Galois Theory. **[6]**

The polynomial $f(X) := X^3 + 3X - 2$ is irreducible over $\mathbb{Q}$. Its unique real root is

$$\alpha = \sqrt[3]{1+\sqrt{2}} + \sqrt[3]{1-\sqrt{2}},$$

and its other two complex roots are

$$\beta = -\tfrac{1}{2}\alpha + \tfrac{1}{4}\sqrt{-6}(\alpha^2+\alpha+2) \quad \text{and} \quad \gamma = -\tfrac{1}{2}\alpha - \tfrac{1}{4}\sqrt{-6}(\alpha^2+\alpha+2).$$

In what follows, you should express field elements and subfields in terms of α, β, γ and $\sqrt{-6}$.

(b) Compute the Galois group $G = \mathrm{Gal}(L : \mathbb{Q})$, of L over $\mathbb{Q}$, where L is a splitting field for f over $\mathbb{Q}$. (We can take L to be the subfield of $\mathbb{C}$ with this property.) **[6]**

(c) Choose **two** subgroups of $G = \mathrm{Gal}(L : \mathbb{Q})$ other than G and the trivial subgroup. For **each** of your chosen subgroups H of G, give the fixed field of H, and state whether $\mathrm{Fix}(H) : \mathbb{Q}$ is a normal extension. **[8]**

End of Paper.