UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday 31 May 2002 1.30 to 4.30

PAPER 3

CONSTRUCTIVE GALOIS THEORY

Attempt ***THREE*** *questions*

There are ***five*** *questions in total*

The questions carry equal weight

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 (a) Let R be a unique factorisation domain with field of fractions $\mathbb{F}$ and let P be a prime ideal of R. Explain how one can use reduction modulo P to investigate Galois groups over $\mathbb{F}$. Give an outline proof of the validity of this approach.

(b) Show that the Galois group of the polynomial $f(X) = X^5 + X^2 + 2X + 1$ over $\mathbb{Q}$ is S_5.

(c) Show that the Galois group of the polynomial

$$f(X) = X^5 + tX^2 + (t+1)X + 1$$

over $\mathbb{F}_2(t)$ is S_5, where $\mathbb{F}_2$ is the field of order 2.

2 Write an essay on Hilbertian fields.

3 (a) Let $\mathbb{F}$ an algebraically closed field of characteristic 0 and let $\mathbb{E}$ be a finite Galois extension of $\mathbb{F}(t)$ with Galois group G over $\mathbb{F}(t)$. For any $p \in \mathbb{F} \cup \{\infty\}$ explain how to define the conjugacy class of G associated to p and the ramification index of $\mathbb{E}$ at p. Prove that your constructions are well-defined.

(b) Let $a(t)$ be a polynomial over $\mathbb{C}$, let $f(X) = X^2 - a(t)$ be an irreducible polynomial over $\mathbb{C}(t)$ and let $\mathbb{E}$ be a splitting field for f over $\mathbb{C}(t)$. Show that $\mathbb{E}$ has a branch point at $p \in \mathbb{C}$ if and only if p is a root of $a(t)$ of odd multiplicity. By transforming $t \mapsto 1/t$, determine when $\mathbb{E}$ has a branch point at ∞.

4 (a) Define what it means for a ramification type $[G, P, \mathcal{C}]$ to be rigid. Show that for each rigid ramification type there is, up to $\mathbb{C}(t)$-isomorphism, at most one finite Galois extension of $\mathbb{C}(t)$ of this type.

(b) Prove the existence of rigid triples of conjugacy classes in the symmetric groups S_n for $n \geq 3$.

(c) Let $g_1 = (12345)$, $g_2 = (12)(35)(46)$ and $g_3 = (25)(346)$. Show that the conjugacy classes of g_1, g_2 and g_3 form a rigid triple in S_6.

5 Let $\mathbb{F} = \mathbb{F}_q(t)$ be the field of rational functions over the field of order q.

(a) Let $f(X) = X^{q^d} + a_{d-1}X^{q^{d-1}} + \ldots + a_1 X^q + a_0 X$ be a polynomial over $\mathbb{F}$ with $a_0 \neq 0$. Show that $\mathrm{Gal}(f, \mathbb{F})$ is naturally a subgroup of $GL(d, q)$

(b) Show that $\mathrm{Gal}(X^{q^d} + X^q + tX, \mathbb{F}) \geq SL(d, q)$ if $d \geq 2$.

[You may assume that any subgroup of $GL(d, q)$ which is 2-transitive on 1-spaces contains $SL(d, q)$.]

(c) Let $G = \mathrm{Gal}(X^{q^d} + X^{q^2} + tX, \mathbb{F})$. Show that if $d \geq 4$ is even then G contains a normal subgroup of index 2 normalising $SL(d/2, q^2)$.