MA3D5 Galois Theory – Sheet 5

Deadline: Thursday, 13 March 2008, 3pm.

Solutions to Section B are for handing in. Please put your solutions into the MA3D5 Galois Theory box in front of the Undergraduate Office. Mention your department if it is not mathematics.

(A1) Put $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{C}$. Find the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ and all intermediate fields.

(B1) Let $K = \mathbb{R}(t)$, the field of rational functions in one variable. Let $P \subset \mathbb{R}[t]$ be the ideal generated by t.

(a) Prove that P is a prime ideal.

(b) Prove that $f = x^4 - t \in \mathbb{R}[t][x]$ is Eisenstein at P.

(c) Let L be a splitting field for f over K. Prove that L contains a square root i of -1. Prove $[L : K] = 8$.

(d) Let $\alpha \in L$ be a root of f. Prove that every $g \in G := \mathrm{Gal}(L/K)$ preserves $A = \{\alpha, \alpha i, \alpha i^2, \alpha i^3\}$. Prove that every $g \in G$ preserves the graph with vertex set A and (unoriented) edges $\{\alpha\, i^k, \alpha\, i^{k+1}\}$ where $k \in \{0, 1, 2, 3\}$. Deduce that $G \cong D_8$.

[Hint: you may assume that D_8 is the automorphism group of the above graph, and has 8 elements.]

(e) Give two generators of G and their values at i, α. List all subgroups of G (by group generators), and the corresponding intermediate fields (by field generators). Show either in inclusion diagrams as on page 73 of the printed notes. Give a full proof for just one of the most difficult subgroups (choose yourself) and no proofs for the others.

(B2) In this exercise you should list all results from the lecture notes which you use. Let K be a field and $M = K(z)$ the field of rational functions in a variable z. Let $G \subset \mathrm{Gal}(M/K)$ be the subgroup generated by

$$s\colon z \mapsto 1 - z \qquad \text{and} \qquad t\colon z \mapsto z^{-1}$$

and $L = M^G$.

(a) Prove that the orders of (respectively) s, t, st are (respectively) $2, 2, 3$. [It follows that there is an isomorphism $G \to S_3$, $s \mapsto (12)$, $t \mapsto (23)$, don't prove this.]

(b) Write

$$y = \frac{z^3 - 3z + 1}{z(z-1)}.$$

Prove $M^{\langle st \rangle} = K(y)$.

(c) Prove $y + s(y) = 3$.

(d) Deduce from (c) that $L = K(w)$ where $w = y\,s(y)$. [This can be done without many calculations.]

(e) List all subgroups of G (by group generators) and the corresponding intermediate fields (by field generators). Proofs are not necessary.

(f) If N is a field and $a \in N$ is such that $f := (x^3 - 3x + 1) - a\,x(x-1)$ is irreducible, prove that the splitting field of f over N has degree 3 over N.

(C1) Let $L \subset \mathbb{C}$ be the splitting field of $x^4 - 2$. Prove that $L = \mathbb{Q}(i + \sqrt[4]{2})$. [Hint: Find at least five elements of the $\mathrm{Gal}(L/\mathbb{Q})$-orbit of $i + \sqrt[4]{2}$.]

(C2) In this question, we assume nothing to be known about finite fields. Let p be a prime number and put $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (which is known to be a field). Let $\mathbb{F}_p \subset K$ be a finite extension of degree d. Let $F\colon K \to K$ be the Frobenius map, defined by $F(t) = t^p$, and which we know to be a ring homomorphism.

(a) Prove that F is bijective.

(b) Prove that $K^{\langle F\rangle} = \mathbb{F}_p$.

(c) Deduce from (b) and some results from the lectures that $K/\mathbb{F}_p$ is Galois, and that the Galois group is generated by F. Also prove that $F \in G$ has order d.

(d) Without using the fact that K^* is cyclic, prove that all elements $t \in K$ satisfy $t^{p^d} - t = 0$.

(e) Prove that $K/\mathbb{F}_p$ is normal and separable.

(C3) Let L/K be a Galois extension with group G. For $H_1, H_2 \in \mathcal{G}$, prove that $\langle H_1, H_2\rangle^\dagger = H_1^\dagger \cap H_2^\dagger$ and $(H_1 \cap H_2)^\dagger = H_1^\dagger H_2^\dagger$ where F_1F_2 is the field generated by $F_1 \cup F_2$.

(D1) For each of the following polynomials f, determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ where K is a splitting field of f over $\mathbb{Q}$, and all intermediate fields.

(a) $x^4 - 8x^2 + 8$.

(b) $x^4 - 8x^2 + 4$.

(c) $x^4 - 22\,x^2 + 25$.

(d) $x^6 + x^3 + 1$.

(D2) Let p be an odd prime number and put $\varepsilon = \exp(2\pi i/p)$. Prove that

$$\Big(\sum_{k \in \mathbb{F}_p} \varepsilon^{k^2}\Big)^2 = (-1)^{(p-1)/2} p.$$

Much harder is: find out which of the two square roots it is.

(D3) On page 87 of the printed notes there is a sketch of a proof that the cyclotomic polynomials are irreducible over $\mathbb{Q}$. Fill in the details.

(D4) Let L/K be a splitting field of a separable $f \in K[x]$. Prove that L/K is separable.