MA3D5 Galois Theory – Sheet 3

Deadline: Thursday, 26 February 2008, 3:00.

Question (3.6) is not 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.

(3.1) Suppose that $K \subset L$ is a field extension. Let $\alpha \in L$ be algebraic over K of degree m and $\beta \in L$ be algebraic over K of degree n.

(a) Prove that $\alpha + \beta$ is algebraic over K of degree $\leq mn$.

(b) If m, n are coprime, prove $[K(\alpha, \beta) : K] = mn$.

(c) Let $\alpha := 2^{1/2} \in \mathbb{R}$, $\beta := 5^{1/3} \in \mathbb{R}$, $\gamma := \alpha + \beta$. Prove $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$.

(d) Prove that γ is of degree 6 over $\mathbb{Q}$.

(e) Compute the minimal polynomial of γ over $\mathbb{Q}$.

(3.2) Let K be a field. Let α be an element in a larger field whose minimum polynomial over K has odd degree. Prove that $K(\alpha) = K(\alpha^2)$.

(3.3) In this exercise you will fill some gaps in example 85.

(1) Prove that $K^{\langle st \rangle} = \mathbb{C}(X^3)$.

(2) Prove that $K^G = \mathbb{C}(v)$ where $v = X^3 + X^{-3}$.

(3) Compute the minimum polynomial of $u = X + X^{-1}$ over $\mathbb{C}(v)$.

(3.4) Let M/K be an extension of degree $d < \infty$. Suppose that $G = \mathrm{Gal}(M/K)$ has t elements. Prove that $t \leq d$. Prove that $t = d$ if and only if M/K is Galois. Hint: Consider $L = G^\dagger$ and use theorem 82 and the tower law.

(3.5) Let K be a field of characteristic $\neq 3$ and write $L = K(X)$. Let $\alpha \in K$ be a primitive cube root of unity. Define $s, t \in \mathrm{Gal}(K(X)/K)$ by

$$s(X) = \alpha X, \qquad t(X) = \frac{-X + 1}{2X + 1}$$

and write $G = \langle s, t \rangle$.

(a) Prove: G preserves $\{0, 1, \alpha, \alpha^2\}$ where we use the $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$ constructed in exercise (3.6).

(b) From now on, you may assume that G has 12 elements. Find $p, q \in K[X]$ of degree at most 12 such that $r := p/q$ is in L^G but not in K. Hint: why does the G-orbit of X^3 have at most 4 elements?

(c) Deduce that $L^G = K(r)$.

(3.6) (Not for handing in). Let K be a field and $n \geq 1$. Let $\mathrm{GL}(n, K)$ be the group of invertible $n \times n$ matrices or equivalently, the group of invertible K-linear maps from K^n to itself.

(a) Prove that there exists a $\mathrm{GL}(2, K)$-action on the field $K(X)$ by K-automorphisms, defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (X) = \frac{aX + b}{cX + d}.$$

(b) Prove that an element of $\mathrm{GL}(2, K)$ acts trivially on $K(X)$ if and only if it is scalar. Notation: we let H denote the group of scalar elements and put

$$\mathrm{PGL}(2, K) := \mathrm{GL}(2, K)/H.$$

We have shown that $\mathrm{PGL}(2, K)$ is a subgroup of $\mathrm{Gal}(K(X), K)$.

(c) Prove that $\mathrm{PGL}(2, K) = \mathrm{Gal}(K(X)/K)$. Notation: as usual, $\mathrm{PGL}(2, K)$ acts on the set of 1-dimensional linear subspaces of K^2. Instead of the subspaces

$$K\binom{a}{1}, \text{ respectively, } K\binom{1}{0}$$

where $a \in K$ we simply write a, respectively, ∞. Thus we obtain a $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$. Roughly, it is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (t) = \frac{at + b}{ct + d}$$

for all $t \in K \cup \{\infty\}$.