MA3D5 Galois Theory – Sheet 3

Deadline: Monday 18 February 2008, 3:00pm.

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) Let K be a field and $L = K(t)$, the field of rational functions in a variable t. Let $\alpha \in L$ be algebraic over K. Prove $\alpha \in K$.

(A2) Let $\alpha \in \mathbb{C}$ be a root of $x^3+\sqrt{3}\,x+\sqrt{5}$. Which of our theorems guarantee(s) that α is algebraic over $\mathbb{Q}$? Find a nonzero $f \in \mathbb{Q}[x]$ explicitly such that $f(\alpha) = 0$.

(A3) Let p be a prime number and $\alpha = \cos(2\pi/p)$. Prove $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p-1)/2$.

(A4) 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 $\mathbb{Q}$.

(A5) Let K be the splitting field of $x^{12} - 1$ over $\mathbb{Q}$. Calculate $[K : \mathbb{Q}]$ and find an explicit $\mathbb{Q}$-basis for K. Prove that K is also the splitting field of $(x^4-1)(x^3-1)$ over $\mathbb{Q}$.

(B1) Let $\epsilon = \exp(2\pi i/7)$, $\alpha = \varepsilon + \varepsilon^2 + \varepsilon^4$, $\beta = \varepsilon^3 + \varepsilon^5 + \varepsilon^6$.

(a) Compute the elementary symmetric polynomials in α, β and prove that they are in $\mathbb{Q}$.

(b) Find $d \in \mathbb{Q}$ such that $\alpha \in \mathbb{Q}(\sqrt{d})$.

(c) Compute the elementary symmetric polynomials in $\varepsilon, \varepsilon^2, \varepsilon^4$ and prove that they are in $\mathbb{Q}(\alpha)$. (So the 7-gon can be constructed by solving quadratics and a single cubic).

(B2) Let $f = x^6 + 3$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$, $g = x^6 + 2$, $M \subset \mathbb{C}$ a splitting field of g over $\mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}) \subset \mathbb{C}$. Clearly, f and g are irreducible over $\mathbb{Q}$ by Eisenstein.

(a) Prove that K contains all 6-th roots of unity.

(b) Prove that K is a splitting field over $\mathbb{Q}$.

(c) Prove $L \subset M$.

(d) Prove $[L : \mathbb{Q}] = 4$.

(e) Prove $[M : \mathbb{Q}] = 12$.

(B3) Let p be a prime number. Prove that for any field K and any $a \in K$, the polynomial $f(x) = x^p - a$ is either irreducible, or has a root.

[Hint: If $f = gh$, factorise g, h into linear factors over a bigger field, and consider their constant terms.]

(B4) Let p be a prime number and K a field over which $x^p - 1$ splits into linear factors. Suppose that L/K is a field extension, and that $\alpha \in L$ has minimal polynomial $f \in K[x]$ of degree n coprime to p. Prove that $K(\alpha) = K(\alpha^p)$; find a counterexample if K does not contain all the pth roots of 1. [Hint: argue on the degree $[K(\alpha) : K(\alpha^p)]$ and use the result of (B3).]

(C1) Let $K \subset L$ be a (not necessarily algebraic) field extension. Let $f, g \in K[x]$. Prove that $f \mid g$ in $K[x]$ if and only if $f \mid g$ in $L[x]$.

(C2) Let $K \subset L \subset M$ be fields. Let $\alpha \in M$ be algebraic over K (hence over L).

(a) Prove that $f := \mathrm{Min}_L(\alpha)$ divides $g := \mathrm{Min}_K(\alpha)$ in $L[x]$.

(b) Prove that the coefficients of f are algebraic over K.

(c) Suppose now that $L = K(t)$, the field of rational functions in a variable t. Let $h \in K[x]$ be irreducible. Prove that h is irreducible in $L[x]$. You may use the results of (A1) and (C1).

(C3) Let $K \subset L$ be an extension having degree $[L : K] = n$ coprime to a prime number p. Let $a \in K$. Prove that a is a pth power in K if and only if it is in L.

(C4) Prove that every finite field extension is algebraic. Find an algebraic field extension which is not finite.

(C5) Prove that the 13th roots of unity can be obtained by solving a single cubic equation and some quadrics.

(D1) Let L/K be a splitting field of a polynomial $f \in K[x]$ of degree n. Prove that $[L : K]$ divides $n!$.

(D2) In this exercise, you prove that $\mathbb{C}$ is algebraically closed. Let $f \in \mathbb{R}[x]$ be monic. It suffices to prove that f has a root in $\mathbb{C}$. Let $o_2(\deg f)$ denote the greatest $k \geq 0$ such that 2^k divides the degree on f. We use induction on $r := o_2(\deg f)$.

(a) Prove it is true if $r = 0$, that is, f has odd degree.

(b) Let K be a splitting field for f over $\mathbb{R}$. Let $f = \prod_{i=1}^{n}(x - a_i)$ with $a_i \in K$. For $c \in \mathbb{R}$, define

$$g_c(x) = \prod_{1 \leq i < j \leq n} (x - a_i - a_j - c a_i a_j).$$

Compute $o_2(\deg g_c)$ and prove that $g_c \in \mathbb{R}[x]$.

(c) Finish the proof.

(D3) Let L/K be a finite field extension. Let $f \in K[x]$ be irreducible of degree p, a prime number. Suppose that f is reducible in $L[x]$. Prove that p divides $[L : K]$.