MA3D5 Galois Theory – Sheet 4

Deadline: Monday, 9 March 2009, 3:00.

Please put your solutions into the MA3D5 Galois Theory box in front of the Undergraduate Office. Mention your department if it is not mathematics.

(4.1) 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 6th 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 $[M : \mathbb{Q}] = 12$.

(4.2) Let $f \in K[X]$ be irreducible. Prove the following.

- (a) Suppose that the characteristic of K is 0. Then f is separable.
- (b) Suppose that the characteristic of K is a prime number p. Then f is inseparable if and only if there exists a polynomial g such that $f = g(X^p)$.

(4.3)
- (a) Let $f = X^3 - 3X - 1$. Prove that f is irreducible in $\mathbb{Q}[x]$.
- (b) Prove directly that if $\alpha \in \mathbb{C}$ is a root of f then so is $2 - \alpha^2$.
- (c) Let $\alpha \in \mathbb{C}$ be a root of f and put $K = \mathbb{Q}(\alpha)$. Prove that K is Galois over $\mathbb{Q}$. [Hint: use the theorem saying that splitting field plus separable implies Galois].

(4.4) Let ε be a complex primitive 7th root of unity. Put $L = \mathbb{Q}(\varepsilon)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$.

- (a) Say why we already know that $L/\mathbb{Q}$ is Galois of degree 6.
- (b) Prove that there exists a unique element $s \in G$ such that $s(\varepsilon) = \varepsilon^3$.
- (c) Prove that s has order 6.
- (d) Prove that $G = \langle s \rangle$.
- (e) Give a generator for the group $\mathbb{Q}(\alpha)^* \subset G$ where $\alpha = \varepsilon + \varepsilon^{-1}$. Deduce that the degree of α over $\mathbb{Q}$ is 3.
- (f) Compute the minimum polynomial over $\mathbb{Q}$ of α.
- (g) Give all subgroups of G and the corresponding fields, both by generators. (You should prove your results but you don't have to say how you found them). Hint: if H is a subgroup of G, use the algorithm of example 81 to find elements of $H^\dagger$.
- (h) Prove that $X^2 + 7$ factors completely over L.