MA3D5 Galois Theory – Sheet 5

Deadline: Thursday 7 May 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.

(5.1) Let $K \subset L$ be finite fields. Prove that L is separable over K. [Hint: this is immediate from a few theorems, but which?].

(5.2) Let p be a prime number and $a, b \geq 1$. Prove that $\mathbb{F}_{p^a}$ can be embedded into $\mathbb{F}_{p^b}$ (that is, is isomorphic to a subfield of $\mathbb{F}_{p^b}$) if and only if $a \mid b$. [Hint: For $\Leftarrow$ use proposition 108 on $\mathrm{Gal}(L/K)$ for finite fields $K \subset L$. Before you find the intermediate field $\mathbb{F}_{p^a}$ you find the corresponding subgroup].

(5.3) Find a generator of the multiplicative group $\mathbb{F}_{31}^{\times}$.

(5.4) For each $d \in \{3, 5, 7, 9\}$, find at least one irreducible $f \in \mathbb{F}_2[X]$ such that if α is a root of f in an extension of $\mathbb{F}_2$, then $\#\langle\alpha\rangle = d$, where $\langle\alpha\rangle$ is the multiplicative group generated by α.

(5.5) Let p be a prime number and $a \geq 1$. Prove that there exists an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree a. [Hint: The degree of an algebraic extension of the form $K(\alpha)/K$ equals the degree of the minimum polynomial of α over K].

(5.6) (Not for handing in). Let $\mathbb{F}_q$ be a finite field of q elements and let $a \geq 1$. Write $g = X^{q^a} - X$.

- (a) Prove that there exists an irreducible polynomial in $\mathbb{F}_q[X]$ of degree a.
- (b) Prove that g has no multiple roots in any field extension.
- (c) Let $a \geq 1$. Prove that g is the product of all irreducible monic polynomials in $\mathbb{F}_q[X]$ whose degree divides a.
- (d) Let $h_d(q)$ be the number of monic irreducible $f \in \mathbb{F}_q[X]$ of degree d. Prove
$$\sum_{d \mid a} d\, h_d(q) = q^a. \qquad (1)$$
- (e) Prove that there exists a polynomial $H_a \in \mathbb{Q}[Y]$ such that $h_a(r) = H_a(r)$ for all prime powers r.
- (f) Let $f \in \mathbb{F}_q[X]$ be of degree d. Prove that f is irreducible if and only if f is coprime to $X^{q^a} - X$ whenever $a < d$. (This gives a fast algorithm to check irreducibility.)