Math 8202 **Homework 2** **PJW**

Date due: February 9, 2009. There will be a quiz on this date. Hand in only the 5 starred questions.

K* (Fall 2002 qn. 5, part (a)) Let k be a field of characteristic $p > 0$, and $K = k(t)$ where t is an element transcendental over k. Show that $X^p - t$ is irreducible in $K[X]$.

L* (Fall 2001, qn. 6) (10%) Let $\mathbb{F}_{p^k}$ be the field with p^k elements, where p is prime.

(a) Show that $x^4 + 1 \in \mathbb{F}_p[x]$ has a root in $\mathbb{F}_{p^2}$.

(b) Deduce that $x^4 + 1$ is reducible in $\mathbb{F}_p[x]$. For which values of p does a linear factor exist in $\mathbb{F}_p[x]$?

[You may assume standard facts about finite fields.]

M Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and in $\mathbb{F}_2[x]$.

N* Prove that an algebraically closed field must be infinite.

O Find an explicit isomorphism between the splitting fields of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$, identifying the images of the roots of the first polynomial in the splitting field of the second polynomial as expressions in the roots of the second polynomial.

P* Suppose $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with $D_1, D_2 \in \mathbb{Z}$, is a biquadratic extension and that $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}$ where $a, b, c, d \in \mathbb{Z}$ are integers. Prove that the minimal polynomial $M_\theta(x)$ for θ over $\mathbb{Q}$ is irreducible of degree 4 over $\mathbb{Q}$ but is reducible modulo every prime p. In particular show that the polynomial $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime. [Use the fact that there are no biquadratic extensions over finite fields.]

Q Prove that one of $2, 3$ or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(ax^2 - 6)$$

as a root modulo p for every prime p but has no root in $\mathbb{Z}$.

R Prove that $x^{p^n} - x + 1$ is irreducible over $\mathbb{F}_p$ only when $n = 1$ or $n = p = 2$. [Note that if α is a root, then so is $\alpha + a$ for any $a \in \mathbb{F}_{p^n}$. Show that this implies $\mathbb{F}_p(\alpha)$ contains $\mathbb{F}_{p^n}$ and that $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.]

S* (a) Show that in $\mathbb{F}_2[x]$ there are 3 irreducible polynomials of degree 4, and that one of them has roots which have multiplicative order 5.

(b) Let α be a root of $x^4 + x + 1$ in some extension field of $\mathbb{F}_2$. Express $\alpha^3 + \alpha^4$ as a power of α.