Math 418, Midterm 2

Due **Friday, April 4 (by 5 pm)**

1) [3+3+4 pts.] Let K be an extension of F of degree n.

(a) For any $\alpha \in K$ prove that α acting by left multiplication on K is an F-linear transformation on K.

(b) Prove that K is isomorphic to a subfield of the ring $M_n(F)$ of $n \times n$ matrices over F, so $M_n(F)$ contains an isomorphic copy of every extension of F of degree $\leqslant n$.

(c) Let $K = \mathbb{Q}(\sqrt{D})$ for some squarefree integer D. Let $\alpha = a + b\sqrt{D}$ be an element of K. Use the basis $1, \sqrt{D}$ for K as a vector space over $\mathbb{Q}$ and show that the matrix of the linear transformation "multiplication by α" on K has the matrix $\left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right)$. Prove directly that the map $a + b\sqrt{D} \mapsto \left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right)$ is an isomorphism of the field K with a subfield of the ring $M_2(\mathbb{Q})$.

2) Determine the splitting field and its degree over $\mathbb{Q}$ for $f(X) = X^4 + X^2 + 1$ and respectively for $g(X) = X^6 - 4$.

3) [5+5 pts.] (a) Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[X]$ that has a root in K splits completely in $K[X]$.

(b) Let K_1 and K_2 be finite extensions of F contained in the field K, and assume that both are splitting fields over F. Prove that both their composite K_1K_2 and their intersection $K_1 \cap K_2$ are splitting fields over F.

4) [5+5 pts.] (a) For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $X^p - X + a$ is irreducible and is separable (i.e. it does not have multiple roots) over $\mathbb{F}_p$.

(b) Prove that

$$X^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (X - \alpha).$$

Conclude that

$$\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$$

so the product of the nonzero elements in the finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$.

5) [5+5 pts.] (a) Let $f \in \mathbb{F}_p[X]$ be a monic irreducible polynomial with $\deg f = n$. Show that $f(X)$ divides $X^{p^n} - X$ in $\mathbb{F}_p[X]$.

(b) Show that the degree of each monic irreducible divisor f of $X^{p^n} - X$ is a divisor of n.

6) If F is a finite field, show that any element of F is the sum of two squares (Hint: for each $a \in F$ consider the cardinalities of the sets $\{u^2 : u \in F\}$ and $\{a - u^2 : u \in F\}$).

7) 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 $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1D_2}$ where $a, b, c, d \in \mathbb{Z}$. 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.

8) [3+7 pts.] (a) Prove that for n odd, $n > 1$,

$$\Phi_{2n}(X) = \Phi_n(-X).$$

(b) Use the Möbius Inversion formula indicated in Section 14.3 to prove

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$