Math 530 Comprehensive Exam. May, 2007.
Solve any four of the five problems.

Problem 1
You may use the fact that the discriminant of a root of $x^3 + ax + b$ is given by $-(4a^3 + 27b^2)$.
a) Suppose that $\alpha^3 = \alpha + 1$. Let $K = \mathbb{Q}(\alpha)$ and let $\mathcal{O}$ be the ring of integers. Find an integral basis for $\mathcal{O}$.

b) Factor $5\mathcal{O}$ explicitly as a product of prime ideals.

c) Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}$ over 2. Describe the field $\mathcal{O}/\mathcal{P}$ (up to isomorphism).

d) Are any primes $p \in \mathbb{Z}$ totally ramified in $\mathcal{O}$?

Problem 2
Let p be an odd prime and let ζ be a primitive pth root of unity.
a) Describe the unit group of $\mathbb{Q}(\zeta)$ as an abstract abelian group.

b) Describe the unit group of $\mathbb{Q}(\zeta + \zeta^{-1})$ as an abstract abelian group.

c) **Assume Kummer's Lemma:** *If u is a unit of $\mathbb{Q}(\zeta)$ then $u/\overline{u} = \zeta^r$ for some $r \in \mathbb{Z}$ (where $^-$ is complex conjugation).*
Prove: any unit of $\mathbb{Q}(\zeta)$ can be written in the form $\zeta^s \epsilon_1$, where $s \in \mathbb{Z}$ and ϵ_1 is a unit of $\mathbb{Q}(\zeta + \zeta^{-1})$.

Problem 3
Let $f = x^2 + x + 1 \in R[x]$, where $R = \mathbb{Z}/49\mathbb{Z}$.

(a) State Hensel's lemma.

(b) Prove that f factors as a product of two linear factors in $R[x]$.

In the next three parts you will construct a nontrivial factorization of $f \in R[x]$.

(c) Find linear polynomials $g_1, h_1 \in R[x]$ with $f \equiv g_1 h_1 \pmod 7$.

(d) Find $a_1, b_1 \in R[x]$ with $a_1 g_1 + b_1 h_1 \equiv 1 \pmod 7$.

(e) Find $u_1, v_1 \in R[x]$ such that, for $g_2 = g_1 + 7u_1$ and $h_2 = h_1 + 7v_1$, we have $f \equiv g_2 h_2 \pmod{49}$.

Problem 4
Let $K = \mathbb{Q}(\sqrt[3]{b})$ be a cubic number field and let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$, so that $\mathrm{Gal}(L/\mathbb{Q}) = S_3$. Let $p \in \mathbb{Z}$ be a prime which is unramified in K, and let Q be a prime of L over p.

(a) Show that p is unramified in L.

(b) Define the Frobenius automorphism $\phi(Q|p) \in \mathrm{Gal}(L/\mathbb{Q})$.

(c) Show that the cycle structure of the Frobenius $\phi(Q|p) \in S_3$ depends on p but not on Q.

(d) Describe the decomposition of p in $K/\mathbb{Q}$ for each of the following cases: $\phi(Q|p) = (1)$, $\phi(Q|p) = (12)$, $\phi(Q|p) = (123)$.

Problem 5

Suppose that K is a number field which is Galois over $\mathbb{Q}$ and that $\mathcal{P}$ is a prime ideal of the ring of integers $\mathcal{O}$. Define, for $m \geq 0$, the group

$$V_m := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \ : \ \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}^{m+1}} \ \text{ for all } \alpha \in \mathcal{O}\}.$$

a) Suppose that $V_0 = \{\mathrm{id}\}$. Let $p \in \mathbb{Z}$ be the prime under $\mathcal{P}$. What can you conclude about the decomposition of p in $\mathcal{O}$?

b) Prove that $\bigcap_{m=0}^{\infty} V_m = \{\mathrm{id}\}$ and that $V_m = \{\mathrm{id}\}$ for sufficiently large m.

c) Suppose that $\pi \in \mathcal{P}$. If $\sigma \in V_{m-1}$ and $\sigma(\pi) \equiv \pi \pmod{\mathcal{P}^{m+1}}$, prove that

$$\sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}^{m+1}} \quad \text{for all } \alpha \in \pi\mathcal{O}$$