Math 250a: Higher Algebra
Problem Set #2 (6 October 2004): Galois theory II

1. Prove that $\mathbf{Z}$ is the only subring of $\mathbf{Q}$ that is finitely generated as a module over $\mathbf{Z}$, and conclude that $\mathbf{Z}$ is integrally closed in $\mathbf{Q}$.

2. (Proof of the result mentioned at the end of the notes on integral closure) Let A be a subring of some field F, and assume that A is integrally closed in F. Let u be an element of some field K/F which is algebraic over F and integral over A. Prove that the minimal monic polynomial of u is contained in $A[X]$. (Hint: Factor this polynomial over its splitting field.)

3. (Fermat's last theorem in $F[X]$) Suppose $A, B, C \in F[X]$ are polynomials satisfying $A + B + C = 0$, and let $W = AB' - A'B$. Show that if r is a root of A, B, or C of multiplicity m in some extension field K/F then r is a root of W of multiplicity at least $m - 1$.

   Use this to prove that if F is a field of characteristic zero then for each integer $n \geq 3$ the Fermat equation $x^n + y^n = z^n$ has no solution in relatively prime polynomials $x, y, z \in F[X]$ of positive degree. Does this remain true in characteristic $p > 0$? If not, what additional condition must be imposed on x, y, z, n?

   [The method can be generalized to $x^n + y^n + z^n = t^n$, etc., but imperfectly: already with four terms it is still not known what is the largest n for which $x^n + y^n + z^n = t^n$ has a nontrivial solution in $\mathbf{C}[X]$. Can you prove $n < 8$? Can you find an example with $n > 4$?]

4. (Problem 2 of Jacobson 4.4) Let F be a field of characteristic p. Prove that every irreducible polynomial $f \in F[X]$ can be written as $g(X^{p^e})$ for some irreducible separable polynomial $g \in F[X]$ and some nonnegative integer e. Use this to show that every root of f (in a splitting field of f) has the same multiplicity p^e.

5. (Problem 4 of Jacobson 4.5, generalized) Let $E = \mathbf{C}(t)$, the field of rational functions over $\mathbf{C}$ in a transcendental t. Fix a positive integer n and a primitive n-th root of unity $\omega \in \mathbf{C}$ [that is, a generator of the group of n-th roots of unity; for example, $\omega = e^{2\pi i/n})$]. Let σ, τ be the the following automorphisms of E:

$$(\sigma f)(t) := f(\omega t); \qquad (\tau f)(t) := f(1/t).$$

   Show that $\sigma^n = \tau^2 = (\sigma\tau)^2 = \mathrm{id}$. Determine the structure of the group G generated by σ and τ, and prove that the subfield F of E fixed by G is $\mathbf{C}(u)$ where $u = t^n + t^{-n}$.

6. (Problem 3 of Jacobson 4.4, generalized) Let k be a finite field q elements, and F a field contianing k. A polynomial $f \in F[X]$ is called a *q-polynomial* if it is of the form $\sum_{i=0}^{m} a_i X^{q^i}$ for some $a_i \in F$. Prove that a polynomial $f \in F[X]$ of positive degree is a q-polynomial if and only if its roots form a k-vector subspace of $\overline{F}$ and each root has the same multiplicity which is of the form q^e for some nonnegative integer e.

   [Note that the polynomial $X^q - X$ we used to construct k is a special case, and is a q_0-polynomial for every q_0 such that q is a power of q_0.]

7. (Problem 3 of Jacobson 4.5) Let F be a field of characteristic p, and a an element of F not in $\{b^p - b \mid b \in F\}$. Prove that the polynomial $X^p - X - a$ is irreducible over F, and determine its Galois group. Can you obtain a generalization with p replaced by a prime power q?

Problem set is due in class Wednesday the 13th.