Math 250a: Higher Algebra
Problem Set #2 (21 September 2001): Galois Theory II

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

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 \( W = AB^e - A'B \). 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.

[What happens in characteristic \( p > 0 \)? Can you generalize to \( x^n + y^n + z^n = t^n \), etc.?]

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) Let \( E = \mathbb{C}(t) \), the field of rational functions over \( \mathbb{C} \) in a transcendental \( t \). Fix a cube root of unity \( \omega \in \mathbb{C} \) [that is, \( \omega \neq 1 \) such that \( \omega^3 = 1 \); for example, \( \omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3}) \)]. Let \( \sigma, \tau \) be the following automorphisms of \( E \):

\[
(\sigma f)(t) := f(\omega t); \quad (\tau f)(t) := f(1/t).
\]

Show that \( \sigma^3 = \tau^2 = (\sigma \tau)^2 = \text{id} \). Determine the structure of the group \( G \) generated by \( \sigma \) and \( \tau \), and prove that the subfield \( F \) of \( E \) fixed by \( G \) is \( \mathbb{C}(u) \) where \( u = t^3 + t^{-3} \).

6. (Problem 3 of Jacobson 4.4) Let \( F \) be a field of characteristic \( p \). A polynomial \( f \in F[X] \) is called a \( p \)-polynomial if it is of the form \( \sum_{i=0}^m a_i X^{p^i} \) for some \( a_i \in F \). Prove that a polynomial \( f \in F[X] \) of positive degree is a \( p \)-polynomial if and only if its roots in a splitting field of \( f \) are closed under addition and each root has the same multiplicity which is of the form \( p^e \) for some nonnegative integer \( e \).

If you already know about finite fields, you can generalize this as follows: let \( q \) be a power of the prime \( p \), and \( F \) a field of characteristic \( p \) containing the \( q \)-element field \( \mathbb{F}_q \); 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 \( a_i \in F \). Then a \( p \)-polynomial is a \( q \)-polynomial if and only if its roots are an \( \mathbb{F}_q \)-vector subspace of the splitting field, and their common multiplicity \( p^e \) is a power of \( q \).]

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.

Problem set is due in class Friday the 28th.