MODERN ALGEBRA (MATH 210) PROBLEM SET 8

1. Describe the set of integers of the form $a^2 - ab + b^2$ ($a, b \in \mathbb{Z}$). (You may use the results of last week's problem set.)

2. Suppose $r + si$ ($r, s \in \mathbb{Q}$) is the zero of a monic polynomial in $\mathbb{Z}[x]$. Show that $r, s \in \mathbb{Z}$.

3. Suppose p is an odd prime.

(a) Show that exactly half of $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\}$ are square modulo p.
(b) Prove that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^*$.
(c) Show that $a^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if a is a perfect square modulo p.
(d) Show that if neither a nor b are perfect squares modulo p, then ab is a perfect square modulo p.

4. Show that $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$. (You may use the fact that π and e are transcendental over $\mathbb{Q}$.)

5. Suppose that K is a field of characteristic 0, and $f(x) \in K[x]$ is irreducible. Show that f does not have repeated roots. Show that this is false in characteristic p. (*Hint:* consider $K = \mathbb{F}_p(t)$, $f(x) = x^p - t$.)

6. Suppose $f(x) \in \mathbb{Z}[x]$ is a degree n polynomial. Let E be its splitting field. Show that the group of automorphisms of E fixing $\mathbb{Q}$ is isomorphic to a subgroup of S_n. (Hint: How does it act on the roots of $f(x)$? Don't ignore the tedious special case where $f(x)$ has multiple roots.) This is called the *Galois group* of the polynomial.

7. (a) Show that if $f(x) = x^3 - 2$, then the Galois group is isomorphic to S_3.

(b) Show that the splitting field E of $x^3 - 3x + 1$ has degree 3 over $\mathbb{Q}$. Show that Galois group of $E/\mathbb{Q}$ is isomorphic to $\mathbb{Z}/3$.

8. Find a minimal polynomial (over $\mathbb{Q}$) of $\sqrt{2} + \sqrt{3}$. (In other words, find a polynomial of minimal degree over $\mathbb{Q}$ with $\sqrt{2} + \sqrt{3}$ as a root.) Let E be the splitting field of this polynomial. Show that $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find the Galois group of E over $\mathbb{Q}$.

This set is due Friday, Dec. 3 at noon at Jarod Alper's door, 380–J.

Date: Friday, November 26, 2004.