Math 603 Problem Set #9 Due Mon., April 11, 2005

1. Let $F = \mathbb{Z}/p\mathbb{Z}$, let $L = F(x, y)$, and let $K = F(x^p, y^p)$. Show that L is a finite field extension of K, but that there are infinitely many fields between K and L. Is $L = K[\alpha]$ for some $\alpha \in L$? Is L separable over K?

2. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\Phi_n(x)$ be the minimal polynomial of ζ_n over $\mathbb{Q}$.
a) Find the roots of $\Phi_n(x)$. Show that $\deg \Phi_n(x) = \phi(n)$, where

$$\phi(n) = \#\{m \in \mathbb{Z} \,|\, 1 \leq m \leq n,\ (m, n) = 1\}.$$

b) Show that $\prod_{\substack{d|n \\ d>0}} \Phi_d(x) = x^n - 1$, and deduce that $\sum_{\substack{d|n \\ d>0}} \phi(d) = n$.
c) Let $K_n = \mathbb{Q}(\zeta_n)$. What is $[K_n : \mathbb{Q}]$? [Hint: Observe $K_n \approx \mathbb{Q}[x]/(\Phi_n(x))$.]
d) Show that K_n is Galois over $\mathbb{Q}$.

3. Let K be a field, and let $x_1, \ldots, x_n$ be transcendentals (variables) over K. For $i = 1, \ldots, n$ let s_i be the ith elementary symmetric polynomial in $x_1, \ldots, x_n$. (Thus $s_1, \ldots, s_n$ are algebraically independent.)
a) Show that $K(x_1, \ldots, x_n)$ is the splitting field over $K(s_1, \ldots, s_n)$ of the polynomial $Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \cdots + (-1)^n s_n$.
b) Show that the extension $K(s_1, \ldots, s_n) \subset K(x_1, \ldots, x_n)$ is Galois.
c) Show that the Galois group G is the symmetric group S_n. [Hint: Show that $S_n \subset G$ and that $\#G = [K(x_1, \ldots, x_n) : K(s_1, \ldots, s_n)] \leq n!$.]

4. Let L be a normal field extension of K, and let K_0 be the maximal purely inseparable extension of K contained in L. View L as contained in a fixed algebraic closure $\bar{K}$ of K.
a) Let $\beta \in L$, and let $\beta_1, \ldots, \beta_n \in \bar{K}$ be the distinct images of β under the K-embeddings $L \hookrightarrow \bar{K}$ (listing each image only *once*, regardless of multiplicity). Let $f(x) = \prod(x - \beta_i)$. Show that $f(x) \in K_0[x]$. [Hint: Show $f(x) \in L[x]$, and then show that the coefficients of f are mapped to themselves under each K-embedding $L \hookrightarrow \bar{K}$.]
b) In part (a), show that $f(x)$ is the minimal polynomial of β over K_0. [Hint: Show that every β_i is a root of the minimal polynomial.]
c) Conclude that L is separable over K_0.

5. Let $K = \mathbb{F}_p(t)$ and let $L = K[\sqrt[2p]{t}]$, where p is an odd prime number.
a) Find the maximal separable extension K' of K in L, and the maximal purely inseparable extension K_0 of K in L.
b) Show *explicitly* in this example that L is the compositum of K' and K_0, by expressing $\sqrt[2p]{t}$ as a combination of elements from K' and K_0.
c) What if instead $p = 2$?

The following problems are optional.

6. Prove "Fermat's Last Theorem" for the ring $\mathbb{C}[t]$ (rather than for $\mathbb{Z}$, as usual). That is, show that if $n > 2$ then there is no choice of relatively prime non-constant polynomials $p(t), q(t), r(t) \in \mathbb{C}[t]$ such that $p^n + q^n = r^n$. Do this in steps, as follows:

a) Show that if such polynomials exist, then they are *pairwise* relatively prime.

b) For these p, q, r and their derivatives p', q', r', show that

$$\begin{pmatrix} p & q & r \\ p' & q' & r' \end{pmatrix} \begin{pmatrix} p^{n-1} \\ q^{n-1} \\ -r^{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

c) Show that $M \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^{n-1}}$, where $M = \begin{pmatrix} q & r \\ q' & r' \end{pmatrix} \begin{pmatrix} q^{n-1} & 0 \\ 0 & -r^{n-1} \end{pmatrix}$. Deduce that $\det(M) \equiv 0 \pmod{p^{n-1}}$ and hence that $\det \begin{pmatrix} q & r \\ q' & r' \end{pmatrix} \equiv 0 \pmod{p^{n-1}}$.

d) Conclude that $p^{n-1} \mid (qr' - rq')$, and similarly that $q^{n-1} \mid (rp' - pr')$ and that $r^{n-1} \mid (pq' - qp')$.

e) Examining the degrees of p, q, r, deduce that one of the polynomials $qr' - rq'$, $rp' - pr'$ and $pq' - qp'$ is identically 0.

f) Derive a contradiction and thereby show the desired conclusion. [Hint: First show that the derivative of r/q is not identically 0.]

7. a) Let $n > 2$, and let K and L respectively be the fraction fields of $\mathbb{C}[t]$ and of $\mathbb{C}[x, y]/(x^n + y^n - 1)$. Show that there is no isomorphism $\Phi : L \to K$ of $\mathbb{C}$-algebras (i.e. fixing the elements of $\mathbb{C}$). [Hint: Problem 6.]

b) Interpret the conclusion of part (a) geometrically, in terms of two varieties not being isomorphic. [Note: The fields K and L are each of transcendence degree 1 over $\mathbb{C}$.]

8. a) Show that every purely inseparable extension is normal.

b) More generally, show that if M is normal over N, and N is purely inseparable over K, then M is normal over K.

c) Let $n > 1$, let $p > n$ be prime, and let K be a field of characteristic p. Also let $\mathcal{M} = \mathcal{L}[\sqrt[p]{x_1}]$, where $\mathcal{L} = K(x_1, \ldots, x_n)$. In the notation of Problem 3 above, show that $\mathcal{M}$ is not normal over $\mathcal{K} = K(s_1, \ldots, s_n)$.

d) In the situation of part (c), let $\mathcal{N}$ be the maximal purely inseparable extension of $\mathcal{K}$ contained in $\mathcal{M}$. Show that $\mathcal{N} = \mathcal{K}$. [Hint: If not, show that $[\mathcal{N} : \mathcal{K}] = p$, and deduce that $\mathcal{M} = \mathcal{L}\mathcal{N}$. Conclude that $\mathcal{M}$ is Galois over $\mathcal{N}$, and then use part (b) to obtain a contradiction.]

e) Deduce that the conclusion of Problem 4(c) above does not necessarily hold if the given field extension is not normal.