Peter Cholak and Juan Migliore Math 222 Wednesday, April 11, 2001
Quiz 6

Be sure to carefully write up your answers. It is suggested that you first write out a draft of your proposed questions and then carefully rewrite that draft to get your final version. You do *not* have to write the answers on this sheet of paper.

Section 7.3, Number 10 (slightly modified) (5 points):

a. For any element $a \in GF(p, P(x))$, let $b \in GF(p, P(x))$ be an element such that $b^{p-1} = a$. Show that then $(kb)^{p-1} = a$ for $1 \leq k \leq p-1$.

b. For any element $a \in GF(p, P(x))$, let $r(a)$ denote the number of distinct elements b in $GF(p, P(x))$ such that $b^{p-1} = a$. Prove that if $a \neq 0$, then $r(a) = 0$ or $p-1$. (You have to show that these are the *only* two possibilities.)

Proof. (a) We know that if $1 \leq k \leq p-1$ then $k^{(p-1)} \equiv_p 1$, so $(kb)^{p-1} = b^{p-1} = a$. For (b) we must show that *if* there exists some $b \in GF(p, P(x))$ with $b^{p-1} = a$, then $r(a) = p-1$. (If there doesn't exist any such element then $r(a) = 0$.) Let b be such an element. Then by (a), $b, 2b, \cdots, (p-1)b$ are distinct solutions of the polynomial equation $x^{p-1} - a = 0$ in $GF(p, P(x))$. But $\deg(x^{p-1} - a) = p-1$; this equation has at most $p-1$ distinct solutions by Proposition 6.7. So we get $r(a) = p-1$.

Section 8.2, Problems 35 and 36:

a. (5 points) Prove that if the set S is finite and σ is a function of S into itself, then the following are equivalent:

   (i) If x_1 and x_2 are distinct elements of S then $\sigma(x_1) \neq \sigma(x_2)$ (i.e. σ is *one-to-one*).

   (ii) If y is any element of S then there is an element x in S such that $y = \sigma(x)$ (i.e. σ is *onto*).

   (Hint: consider the set $\sigma(S) = \{\sigma(x) \mid x \in S\}$.)

b. (5 points) Show, by means of examples, that when S is an infinite set then neither of the conditions (i) or (ii) necessarily implies the other. Specifically, give an example where

   - (i) is true but (ii) is false;
   - (ii) is true but (i) is false;
   - both (i) and (ii) are true.

Solution. First we'll do (a). If (i) holds then the number of elements of $\sigma(S)$ is the same as the number of elements of S. Since $\sigma(S) \subset S$, this means $\sigma(S) = S$ (since S is finite), i.e. σ is onto. Conversely, if (ii) holds then $\sigma(S) = S$, so the number of elements is the same. So σ can't collapse any elements x_1 and x_2 to the same y, i.e. σ is one-to-one.