Comments on Problem Set 2

Math 250a

October 1, 2001

3. Most people got the first part without trouble. A proof of the second part is as follows:

   We are given x, y, z relatively prime of positive degree. Assume $\deg x \leq \deg y \leq \deg z$ (the other cases can be proved using a similar argument). Take an extension field K in which x, y, and z all split. Then the polynomials x, y, and z do not share any roots (or else they would fail to be relatively prime). Let $A = x^n$, $B = y^n$, and $C = z^n$, and take $W = AB' - A'B$. By the first part of the problem, each root of x, y, or z results in a root of W, so W has at least $(n-1)(\deg x + \deg y + \deg z)$ roots (including multiplicity).

   The polynomial W is nonzero. This point is important; without it, the ensuing degree argument fails. To see why W is nonzero, write

   $$W = x^n(y^n)' - (x^n)'y^n = nx^{n-1}y^{n-1}(xy' - x'y).$$

   The scalar n is nonzero since K has characteristic 0. The polynomials x^{n-1} and y^{n-1} are obviously nonzero. Finally, since x' and y' are nonzero (again, because K has characteristic 0), it follows that $xy' - x'y$ is nonzero or else x and y would fail to be relatively prime.

   Once you know that W is nonzero, you know that it has at most $\deg A + \deg B - 1 = n(\deg x + \deg y) - 1$ roots (including multiplicity), and this contradicts the $(n-1)(\deg x + \deg y + \deg z)$ value from before, unless $n \leq 2$.

6. Here is one possible proof of the converse statement for Problem 6. Let $f \in F[X]$ be a polynomial of positive degree whose roots in a splitting field are closed under addition, and suppose each root has the same multiplicity p^e for some nonnegative integer e. We need to prove that f is a p–polynomial.

   Since F has characteristic p, it contains $\mathbf{F}_p$ as a subfield. Because the roots of f are closed under addition, they form a vector space V over $\mathbf{F}_p$. We proceed by induction on $\dim_{\mathbf{F}_p}(V)$.

   If $\dim_{\mathbf{F}_p}(V) = 0$ then $V = \{0\}$, and so $f = X^{p^e}$ is a p–polynomial.

   Suppose $\dim_{\mathbf{F}_p}(V) = n$ and assume the result holds for vector spaces of smaller dimension. Choose a subspace $V' \subset V$ of dimension $n-1$, and choose $v_0 \in V \setminus V'$. By the induction hypothesis, the polynomial $g(X) := \prod_{v \in V'}(X - v)^{p^e}$ is a p–polynomial. But then

   $$f(X) = \prod_{v \in V}(X - v)^{p^e} = \prod_{j \in \mathbf{F}_p} \prod_{v \in V'} (X - (jv_0 + v))^{p^e} = \prod_{j \in \mathbf{F}_p} g(X - jv_0) = \prod_{j \in \mathbf{F}_p} (g(X) - jg(v_0))$$

   where the last equality holds because g is a p–polynomial.

   The quantity $g(v_0)$ is nonzero since $v_0 \notin V'$, and it was proved in class that $\prod_{j \in \mathbf{F}_p}(y - j) = y^p - y$, so

   $$f(X) = g(v_0)^p \prod_{j \in \mathbf{F}_p} \left(\frac{g(X)}{g(v_0)} - j \right) = g(v_0)^p \left(\left(\frac{g(X)}{g(v_0)} \right)^p - \frac{g(X)}{g(v_0)} \right) = g(X)^p - g(X)g(v_0)^{p-1}$$

   and this a p–polynomial.

7. The instructions "determine its Galois group" mean that you should find the elements of the Galois group, in addition to determining the abstract structure of the group.