Comments on Problem Set 5

Math 250a

October 22, 2001

Problem 4. For the first part of the problem, the thing to do here is to show first that the characteristic polynomial of M_a is $p(X)^k$, where $p(X)$ is the minimal polynomial of a over F, and $k := n/d$, $d := \deg p(X)$.

One shows this by taking a basis $\{b_1, b_2, \ldots, b_k\}$ of $E/F(a)$, so that

$$\{b_1, ab_1, a^2b_1, \ldots, a^{d-1}b_1, b_2, ab_2, \ldots, a^{d-1}b_2, \ldots, a^{d-1}b_k\}$$

is a basis for E/F. With respect to this basis, the matrix for M_a is a block diagonal matrix with k blocks, each block being equal to the matrix of PS1 Problem 1 (iii). The characteristic polynomial of each such block is $p(X)$, and that of the matrix as a whole is $p(X)^k$.

Next you have to argue that $p(X)^k$ is equal to $\prod_{i=1}^{n}(X - \eta_i(a))$. By Theorem 4.4, there are exactly d homomorphisms τ_j from $F(a)$ to K fixing F, and these necessarily map a to some $\eta_i(a)$. We have $p(X) = \prod_{j=1}^{d}(X - \tau_j(a))$. For each η_i, there are k homomorphisms from E to K fixing F which map a to $\eta_i(a)$. Since $dk = n$, these account for all the homomorphisms from E to K fixing F. So for each $\tau_j(a)$, there are exactly k different i's with $\eta_i(a) = \tau_j(a)$, and we see that $p(X)^k = \prod_{i=1}^{n}(X - \eta_i(a))$.

Problem 6. The pairing is between $\mathrm{Gal}(L/F)$ and F, and is defined by $\langle g, a\rangle := g(u) - u$, where $u \in K$ is chosen so that $u^p - u - a = 0$. It descends to a perfect pairing between $\mathrm{Gal}(K/F)$ and F/F', where F' is the additive subgroup of F consisting of all elements of the form $b^p - b$ for some $b \in F$.

Many people used the notation $F^p - F$ for the object F', but, strictly speaking, $F^p - F$ consists of all elements of F of the form $a^p - b$ for some $a, b \in F$, which is not the object you want here.

Problem 7. Nobody got the following point right, so this note is for everybody.

Part of the problem asks you to prove that, if the cocycles $a_{\sigma,\tau}$ of $\mathcal{G}$ and $b_{\sigma,\tau}$ of $\mathcal{G}'$ differ by a coboundary δf, then there is an isomorphism $\mathcal{G} \cong \mathcal{G}'$ which fixes A and G. The correct isomorphism is given by defining $\eta : \mathcal{G} \longrightarrow \mathcal{G}'$, $\eta(au_\sigma) := af(\sigma)u'_\sigma$. This η is well defined since every element of $\mathcal{G}$ is equal to au_σ for some unique $a \in A$ and $\sigma \in G$.

The function η is clearly the identity on G, since it maps a coset of $\mathcal{G}/A$ to the same coset in $\mathcal{G}'/A$. However, A is a different story. Some sort of argument is required to prove that η is the identity on A. It is **not** obvious from the definition—remember that neither $f(\sigma)$ nor u'_σ is guaranteed to be the identity when σ is the identity. Probably the most efficient way to proceed is to prove first that η is a homomorphism (which most of you did successfully), and then observe that $a\eta(u_\sigma) = \eta(au_\sigma) = \eta(a)\eta(u_\sigma)$, so comparing both sides yields $a = \eta(a)$.

An alternate approach is to define $\eta(u_\sigma) := f(\sigma)u'_\sigma$ and then declare by fiat that $\eta(a) = a$ for $a \in A$. This is fine, provided you check that η is well–defined, which, for the purposes of this problem, means checking that if $a' = u_\sigma a u_\sigma^{-1}$, then $\eta(a')$, which on the one hand is supposedly a', actually is still a' if you compute $\eta(u_\sigma a u_\sigma^{-1})$ out as $\eta(u_\sigma)a\eta(u_\sigma^{-1})$.