Math 121. Structure of general finite extensions

Recall that an extension of fields F'/F in characteristic $p > 0$ is called *purely inseparable* if for all $a \in F'$ some $a^{p^n} \in F$ with $n \geq 0$ (depending on a). In class we saw that this is equivalent to the condition that every such a has minimal polynomial over F of the form $X^{p^e} - c \in F[X]$ for some $e \geq 0$ and $c \in F$. We also discussed basic properties of purely inseparable extensions, including some characterizations of the purely inseparable property.

In this handout, we prove one of those characterizations (see Proposition 0.1) and we analyze the associated notions of separable and inseparable degree for a finite extension of fields. We end the handout with yet *another* characterization of pure inseparability, in terms of counting embeddings into a sufficiently large normal extension of the ground field. First, we prove the result (mentioned in class) which explains the terminology "purely inseparable".

Proposition 0.1. *Let F'/F be a finite extension of fields with characteristic $p > 0$. Then it is purely inseparable if and only if the only subextension $K \subset F'$ over F separable over F is $K = F$.*

Proof. The easier direction is "$\Leftarrow$", as follows. For any $a \in F'$, its minimal polynomial $m_a \in F[X]$ has the form $m_a = (m_a)_{\mathrm{sep}}(X^{p^e})$ for some $e \geq 0$ and separable irreducible $(m_a)_{\mathrm{sep}} \in F[X]$, so a^{p^e} is separable over F (as it has $(m_a)_{\mathrm{sep}}$ as its minimal polynomial over F). Thus, $F(a^{p^e})$ is a subextension separable over F, so by hypothesis it is equal to F. This says $a^{p^e} \in F$, so we recover the definition of what it means to say that F'/F is purely inseparable.

Now consider the converse, so F'/F is purely inseparable. Let $K \subset F'$ be a subfield separable over F. We want to show that $K = F$. Choose $a \in K$, so $m_a \in F[X]$ is separable. But $a \in F'$ with F'/F purely inseparable, so (as we saw in class) a has minimal polynomial of the form $X^{p^n} - b \in F[X]$ for some $n \geq 0$ and $b \in F$. Hence, $m_a(X) = X^{p^n} - b$, yet such a polynomial cannot be separable if $n > 0$ (why not?). Thus, $n = 0$, so $m_a = X - b$. This forces $a = b \in F$. Hence, we have shown that $K = F$ as desired. ∎

Let L/k be a finite extension of fields in characteristic $p > 0$, and let $L_0 \subset L$ be the maximal separable subextension over k. In class we defined the *separable degree* and *inseparable degree*:

$$[L : k]_{\mathrm{s}} = [L_0 : k], \;\; [L : k]_{\mathrm{i}} = [L : L_0];$$

their product is $[L : L_0][L_0 : k] = [L : k]$. For example, if $L = k(a)$ with $m_a = (m_a)_{\mathrm{sep}}(X^{p^e})$ (so $\deg m_a = p^e \deg(m_a)_{\mathrm{sep}}$) then $L_0 = k(a^{p^e})$ with a^{p^e} having minimal polynomial $(m_a)_{\mathrm{sep}}$ over k, so

$$[L : k]_{\mathrm{s}} = [L_0 : k] = \deg(m_a)_{\mathrm{sep}} = (1/p^e) \deg m_a = (1/p^e)[k(a) : k] = (1/p^e)[L : k]$$

and $[L : k]_{\mathrm{i}} = [L : k]/[L : k]_{\mathrm{s}} = p^e$.

In this handout, we want to prove the multiplicativity of these two refinements of the field degree. That is, if $L'/L/k$ is a tower of finite extensions in characteristic $p > 0$ then we claim that

$$[L' : k]_{\mathrm{s}} = [L' : L]_{\mathrm{s}}[L : k]_{\mathrm{s}}, \;\; [L' : k]_{\mathrm{i}} = [L' : L]_{\mathrm{i}}[L : k]_{\mathrm{i}}.$$

Note that if we multiply the left sides of these two equations then we get $[L' : k]$, and if we multiply the right sides then we get $[L' : L][L : k] = [L' : k]$ too, so in fact the two equations are equivalent to each other. (That is, if either holds then dividing it into the formula $[L' : k] = [L' : L][L : k]$ will give the other equation.)

Hence, to prove both of these equations it suffices to prove the equation for separable degree. To do this, we will *not* use the definition of separable degree, but rather will use the alternative description established in class: for any finite extension of fields F'/F and extension K/F' normal over F (e.g., K could be a normal closure of F' over F),

$$[F' : F]_{\mathrm{s}} = \#\,\mathrm{Hom}_F(F', K).$$

Remark 0.2. Before we prove the multiplicativity of separable degree using this alternative formula, let's explain why we cannot expect to succeed by using just the definitions alone. The first layer L/k decomposes as a tower $L/L_0/k$ where L_0/k is separable and L/L_0 is purely inseparable. The second layer L'/L likewise decomposes as a tower $L'/L'_0/L$ with L'_0/L separable and L'/L'_0 purely inseparable. So overall, L'/k decomposes as a 4-step tower of extensions

$$L' \supseteq L'_0 \supseteq L \supseteq L_0 \supseteq k$$

in which the top layer is purely inseparable and bottom layer of separable, but whose middle two layers are "in the wrong order": $L'_0/L/L_0$ with L'_0/L separable and L/L_0 purely inseparable.

The difficulty is that L'_0/L_0 is being decomposed in the "wrong way" relative to what we need, with a separable layer (namely, L'_0/L) on top of a purely inseparable one (namely, L/L_0). Although we know that both separability and pure inseparability are preserved in towers, we cannot access this fact to get a handle on the (degree of the) maximal separable subextension of L' over k because we are handed the field L between L'_0 and L_0 but what we'd really like to have is the maximal separable subfield of L'_0 over L_0. It is exactly this conundrum which we will bypass by studying separable degree in terms of counting field embeddings (by the formula recalled above).

Having now understood why we cannot expect to prove the equality $[L' : k]_{\mathrm{s}} = [L' : L]_{\mathrm{s}}[L : k]_{\mathrm{s}}$ just using the definitions, we shall establish it by counting field embeddings. Choose an extension k'/L' that is normal over k (e.g., a normal closure of L' over k). Thus, k'/k is a normal extension into which L' admits a k-embeddings (by design) and so also L does too (since L is a subfield of L' over k). Note also that since k'/k is normal, k' is normal over all intermediate fields (why?), so in particular under *any* k-embedding $j : L \to k'$ we have that k' is thereby normal over L.

Now we can applying out interpretations of the separable degrees of L'/k, L'/L, and L/k using the single normal extension k'/k. Firstly, $[L' : k]_{\mathrm{s}} = \#\operatorname{Hom}_k(L', k')$. To count this number of k-embeddings $L' \to k'$, we build them in two steps: we first make a k-embedding $j : L \to k'$ and then we lift this j to an embedding $\widetilde{j} : L' \to k'$ over L (viewing k' as an extension of L *via* j). We denote the set of such $\widetilde{j}$'s over one such j as $\operatorname{Hom}_{L,j}(L', k')$, so

$$[L : k]_{\mathrm{s}} = \#\operatorname{Hom}_k(L', k') = \sum_{j \in \operatorname{Hom}_k(L,k')} \#\operatorname{Hom}_{L,j}(L', k').$$

The number of such j's is $[L : k]_{\mathrm{s}}$, and for each such j the size of $\operatorname{Hom}_{L,j}(L', k')$ is exactly $[L' : L]_{\mathrm{s}}$! Hence, $[L : k]_{\mathrm{s}}$ is a sum of $[L : k]_{\mathrm{s}}$ copies of the number $[L' : L]_{\mathrm{s}}$; i.e., $[L : k]_{\mathrm{s}} = [L : k]_{\mathrm{s}}[L' : L]_{\mathrm{s}}$. This completes our proof of multiplicativity for separable (and inseparable) degrees.

Corollary 0.3. *Let L/k be a finite extension in characteristic $p > 0$, and let k'/L be an extension normal over k. Then L/k is purely inseparable if and only if the given k-embedding $j : L \to k'$ is the only one.*

Note that we are *not* focusing on uniqueness of the image $j(L) \subset k'$ as we vary across all possible k-embeddings of L into a normal extension k'/k admitting at least one such embedding (that is actually our old criterion for *normality* of L/k!). Rather, we are focuding on uniqueness for the *map* j itself, a much much stronger condition (and correspondingly, purely inseparable extensions are extremely special examples of normal extensions).

Proof. By the counting interpretation of separable degree, the uniqueness for the map is exactly the condition that $[L : k]_{\mathrm{s}} = 1$. But by definition, $[L : k]_{\mathrm{s}} = [L_0 : k]$, so uniqueness says exactly that $L_0 = k$, which is to say that L/k has no nontrivial separable subextensions. By Proposition 0.1, this says exactly that L/k is purely inseparable. ∎