Math 594. Inseparable degree

Let L/k be an algebraic extension of fields. Let $k' \subseteq L$ be the maximal subextension over k which is separable over k (concretely, k' is the set of $x \in L$ which are separable over k). We noted in class that L/k' is purely inseparable (so $L = k'$ in characterstic 0), and we defined $[L : k]_{\rm s} = [k' : k]$ and $[L : k]_{\rm i} = [L : k']$, the *separable* and *inseparable* degrees of L over k (one or both of which may be infinite). By the degree formula (which is valid without finiteness restrictions), $[L : k] = [L : k]_{\rm s}[L : k]_{\rm i}$. The condition $[L : k]_{\rm i} = 1$ says $L = k'$, or equivalently that L is separable over k. The condition $[L : k]_{\rm s} = 1$ says $k' = k$, so L is purely inseparable over k.

In class we saw that the separable degree can be described in terms of counting the number of k-embeddings of L into an algebraic closure of k, or more generally into a normal extension of k into which L has at least one k-embedding (e.g., we can work with k-embeddings into a normal closure of L over k). This point of view made it easy to prove multiplicativity of separable degree in a tower by counting maps. However, for multiplicativity of inseparable degree in a tower we lacked a counting device and so were only able to handle the case of finite degree towers by means of the expression $[L : k]_{\rm i} = [L : k]/[L : k]_{\rm s}$, with both numerator and denominator on the right side shown to be multipliciative in towers. Of course, we expect the inseparable degree to be multiplicative in towers $L'/L/k$ without requiring $[L' : L]$ or $[L : k]$ to be finite (infinite degree extensions may still have finite inseparable degree, for example).

In this handout, we give a different way to describe both inseparable and separable degrees in terms of degrees of more tractable field extensions whose behavior in towers is very easy. This will enable us to give a very easy proof of the multiplicativity of inseparable degree in a tower, as well as a proof for separable degree which does not involve counting maps (and works directly, without any need to "reduce to the finite case", as was required for the argument in class). The key will be to work with separable and perfect closures of k.

Since the theory of separable and inseparable degree is only non-trivial in positive characteristic (in characteristic zero, inseparable degree is always 1 and separable degree is the same as field extension degree), for this entire handout we shall assume k has positive characteristic p. We fix an algebraic closure $\overline{k}$ and we let k_s and k_p denote the separable and perfect closures of k inside of $\overline{k}$. That is, k_s is the set of $x \in \overline{k}$ which are separable over k, and k_p is the set of $x \in \overline{k}$ for which $x^{p^n} \in k$ for some $n \geq 0$. In particular, k_p is a perfect field (all of its algebraic extensions are separable) and k_s is separably closed (all of its algebraic extensions are purely inseparable).

1. Separable degree and perfect closure

Let $L'/L/k$ be a tower of algebraic extensions. We would like to prove that

$$[L' : k]_{\rm s} = [L' : L]_{\rm s}[L : k]_{\rm s}.$$

Pick a k-embedding of L' into $\overline{k}$, so we may (and do) view our tower as an extension of fields inside of $\overline{k}$: that is, $k \subseteq L \subseteq L' \subseteq \overline{k}$. This also serves to identify $\overline{k}$ as an algebraic closure of each of L and L' (as it is an algebraically closed and algebraic extension of each). It also makes sense to form the composites k_pL and k_pL' of k_p with each of L and L' over k inside of $\overline{k}$. We therefore have a rising tower $k_p \subseteq k_pL \subseteq k_pL' \subseteq \overline{k}$.

Lemma 1.1. *The extension k_pL of L is a perfect closure of L inside of its algebraic closure $\overline{k}$.*

Proof. Any element of k_pL is a ratio of a finite sum of product of elements of k_p and L. Moreover, any element of k_p has a sufficiently high p-power which lies in k. Thus, since the pth power map commutes with formation of sums, products, and ratios in characteristic p, we conclude that raising an element in k_pL to a sufficiently high p-power brings us into L. That is, k_pL is a purely inseparable extension of L. Hence, it must lie inside of the perfect closure of L within the algebraic closure $\overline{k}$. However, k_pL is also an algebraic extension of the perfect field k_p, so it is perfect. Thus, k_pL has to be the perfect closure of L within $\overline{k}$. ■

We shall write L_p to denote k_pL (the perfect closure of L within $\overline{k}$, by the lemma), and likewise $L'_p = k_pL$ (this perfect closure is also equal to the compositum L_pL' of L_p and L' over L, by applying the Lemma with the ground field L with algebraic closure $\overline{k}$ and intemediate extension L'). Consider the following theorem:

Theorem 1.2. *For L/k an algebraic extension of k inside of an algebraic closure $\overline{k}$, $[L:k]_{\mathrm{s}} = [k_pL : k_p] = [L_p : k_p]$.*

We will prove this theorem in a moment. But let us first see how it effortlessly yields multiplicativity of separable degree for a tower of field extensions. In the situation $L'/L/k$ within $\overline{k}$ as above, the theorem and multiplicativity of field degree yield

$$[L':k]_{\mathrm{s}} = [L'_p : k_p] = [L'_p : L_p][L_p : k_p] = [L':L]_{\mathrm{s}}[L:k]_{\mathrm{s}},$$

as desired (of course, for the equality $[L'_p : L_p] = [L:L]_{\mathrm{s}}$ we apply the theorem to the extension L'/L inside of the algebraic closure $\overline{k}$ of L). Hence, multiplicativity of separable degree is "explained" as a special case of multiplicativity of field degree upon forming compositums with a perfect closure k_p to stick everything on top of a perfect field so as to "eat up" the inseparable part of L/k (as all algebraic exentions of k_p are separable). The key point is that forming a compositum with k_p over k yields the perfect closure for *any* algebraic extension L of k inside of $\overline{k}$; this is what allows us to compute L'_p as either a compositum k_pL over k or as a compositum L_pL' over L.

Proof. We express L/k as a tower $L/k'/k$ where k'/k is separable and L/k' is purely inseparable. Thus, we have a tower $k_pL/k_pk'/k_p$. Since k_pL/k_pk' is a purely inseparable extension (as L/k' is purely inseparable) and the field k_pk' is perfect (being algebraic over the perfect field k_p), we conclude that the extension k_pL/k_pk' is trivial (i.e., degree 1). Thus, $[k_pL : k_p] = [k_pk' : k]$. But *by definition* $[L:k]_{\mathrm{s}} = [k':k]$. Hence, by renaming k' as L we may reduce to the case in which L/k is a separable extension (so all subextensions over k are also separable). In this case, we wish to prove $[L:k] = [k_pL : k_p]$.

Assuming we have the result when $[L:k]$ is finite, then when $[L:k]$ is infinite we can find *finite* subextensions $k'_{(n)} \subseteq L$ with $[k'_{(n)} : k] > n$ for any $n > 0$ (why?), so $[k_pL : k_p] \geq [k_pk'_{(n)} : k_p] = [k'_{(n)} : k] > n$ for all $n > 0$, using the result in the finite case applied to $k'_{(n)}/k$ for the equality step. This forces $[k_pL : k_p]$ to be infinite too. Thus, it suffices to consider the case when $[L:k]$ is finite. By expressing L/k as a finite tower of primitively generated extensions

$$k \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_n = L$$

with $k_i = k_{i-1}(a_i)$ for $1 \leq i \leq n$, we have

$$k_p \subseteq k_pk_1 \subseteq \dots k_pk_n = k_pL$$

with $k_pk_i = (k_pk_{i-1})(a_i)$ for $1 \leq i \leq n$. Moreover, k_pk_i *is* the perfect closure of k_i within the algebraic closure $\overline{k}$ of k_i. Thus, by multiplicativity of field degree in a tower it is enough to treat the case of a primitively generated separable extension $L = k(a)$.

With $L = k(a)$ separable over k, say of degree d, we need to prove that $[k_p(a) : k_p] = d$. Since field degree for a primitive extension is equal to the degree of the minimal polynomial of the primitive generator over the ground field, we are reduced to the following problem: if $f \in k[T]$ is a separable irreducible (monic) polynomial, we must show that f is irreducible over k_p. By monicity, if f admits a non-trivial factorization over k_p then we can take the factorization to be one involving monic factors (why?). Thus, it suffices to show that if $f = gh$ is a monic factorization in $k_p[T]$, then $g, h \in k[T]$ (so the factorization must be trivial, by irreducibility of f over k). The idea will be to prove that the coefficients of g and h are separable over k. Since these coefficients are (by hypothesis) in k_p, they are both separable and purely inseparable over k, and hence must lie in k!

Let

$$f = \prod (T - r_i)$$

be the factorization of the separable f into distinct monic linears in $\overline{k}[T]$. By *unique factorization into monics*, each of the *monic* g and h in $k_p[T]$ must be a product of some of the $(T - r_j)$'s. But each $r_j \in \overline{k}$ has minimal polynomial f over k and hence is *separable* over k. It follows that the coefficients of any product among the $(T - r_j)$'s are also separable over k (recall that within an ambient extension field, sums and products of elements separable over the base field are again separable over the base field). Thus, the coefficients of g and h are must be separable over k, and we have seen above that this forces $g, h \in k_p[T]$ to lie in $k[T]$, as desired. ∎

2. Inseparable degree and separable closure

We now carry out a similar development for inseparable degree, using separable closure instead of perfect closure. The replacement of Lemma 1.1 is:

Lemma 2.1. *Let L/k be an extension inside of $\overline{k}$. Then k_sL is the separable closure of L inside of the algebraic closure $\overline{k}$ of L.*

Proof. Since k_s is separable over k, clearly k_sL is separable over L. It therefore remains to prove that k_sL is itself separably closed, which is to say that it admits no non-trivial separable extensions. Equivalently, we want the algebraic closure $\overline{k}$ of k_sL to be a purely inseparable extension. But $\overline{k}$ is even purely inseparable over the subfield k_s, so it is certainly purely inseparable over k_sL. ∎

Motivated by this lemma, we shall write L_s to denote the compositum k_sL of k_s and L over k inside of $\overline{k}$. The lemma shows that this is the separable closure of L within the algebraic closure $\overline{k}$. Here is the analogue of Theorem 1.2:

Theorem 2.2. *Let L/k be an extension inside of $\overline{k}$. Then $[L : k]_{\mathrm{i}} = [k_sL : k_s] = [L_s : k_s]$.*

Once this theorem is proved, the multiplicativity of inseparable degrees in a tower drops right out by essentially the same argument as used in the previous section, the one change being that we use separable closures instead of perfect closures. The idea of this theorem is that forming the compositum $k_sL$with k_s over k "eats up" the separable part of L/k, leaving behind exactly the inseparable part.

Proof. We again consider the tower $L/k'/k$ with k'/k separable and L/k' purely inseparable. This yields the tower $k_sL/k_sk'/k_s$ with k_sk'/k_s separable since k'/k is separable. But k_s is separably closed, so $k_sk' = k_s$ (more concretely, the separable extension k'/k within $\overline{k}$ has to sit inside of the separable closure k_s/k, so $k' \subseteq k_s$ and hence $k_sk' = k_s$). Since $k_sk' = k'_s$ by the lemma and $[L : k]_{\mathrm{i}} = [L : k']$ *by definition*, we may rename k' as k so as to reduce to the case in which L/k is purely inseparable (note the similarity with the proof of Theorem 1.2, except now we argue from the bottom up instead of from the top down).

For L/k purely inseparable algebraic we wish to prove that $[L : k] = [L_s : k_s]$. Just as in the proof of Theorem 1.2, it suffices to treat the case when $[L : k]$ is finite, and we can even reduce to the case when $L = k(a)$ is primitively generated. Since L/k is purely inseparable, a has a minimal polynomial of the form $T^{p^r} - b$ for some $r \geq 0$ and some $b \in k$, so $[L : k] = p^r$. We may assume $r > 0$, so b is *not* a pth power in k. What we must show is that $[k_s(a) : k_s] = p^r$, or in other words that $T^{p^r} - b \in k_s[T]$ is irreducible. By HW9, Exercise 3, it suffices to show that b is not a pth power in k_s. Hence, our problem comes down to proving that if $b \in k$ is not a pth power, then b is not a pth power in k_s. But this is obvious: if $x \in k_s$ satisfies $x^p = b$, then x is both separable and purely inseparable over k, so $x \in k$, contradicting the assumption that $b \in k$ is not a pth power in k. ∎