Math 210B. Inseparable extensions

Since the theory of non-separable algebraic extensions is only non-trivial in positive characteristic, *for this handout we shall assume all fields have positive characteristic p.*

1. Separable and inseparable degree

Let K/k be a finite extension, and k'/k the separable closure of k in K, so K/k' is purely inseparable. This yields two refinements of the field degree: the *separable degree* $[K:k]_{\mathrm{s}} := [k':k]$ and the *inseparable degree* $[K:k]_{\mathrm{i}} := [K:k']$ (so their product is $[K:k]$, and $[K:k]_{\mathrm{i}}$ is always a p-power).

Example 1.1. Suppose $K = k(a)$, and $f \in k[x]$ is the minimal polynomial of a. Then we have $f = f_{\mathrm{sep}}(x^{p^n})$ where $f_{\mathrm{sep}} \in k[x]$ is separable irreducible over k, and a^{p^n} is a root of f_{sep} (so the monic irreducible f_{sep} is the minimal polynomial of a^{p^n} over k). Thus, we get a tower $K/k(a^{p^n})/k$ whose lower layer is separable and upper layer is purely inseparable (as $K = k(a)$!). Hence, $K/k(a^{p^n})$ has no subextension that is a nontrivial separable extension of k' (why not?), so $k' = k(a^{p^n})$, which is to say

$$[k(a):k]_{\mathrm{s}} = [k':k] = [k(a^{p^n}):k] = \deg f_{\mathrm{sep}},$$
$$[k(a):k]_{\mathrm{i}} = [K:k'] = [K:k]/[k':k] = (\deg f)/(\deg f_{\mathrm{sep}}) = p^n.$$

If one tries to prove directly that the separable and inseparable degrees are multiplicative in towers just from the definitions, one runs into the problem that in general one *cannot* move all inseparability to the "bottom" of a finite extension (in contrast with the separability). This is illustrated by:

Example 1.2. Let $k = \mathbf{F}_p(X,Y)$ be the fraction field of $\mathbf{F}_p[X,Y]$. Let $f = T^{p^2} + XT^p + Y \in k[T]$. By viewing f in $\mathbf{F}_p(X)[Y,T]$ and then in $\mathbf{F}_p(X,T)[Y]$, we see that f is irreducible in $k[T]$. Thus, it is well-posed to define $L = k(a)$ for a root a of f; this is an extension of k of degree p^2.

Clearly $f = h(T^p)$ with $h = T^p + XT + Y$ visibly separable, so the extension L/k is not separable yet contains the degree-p subextension $E := k(a^p)$ that is separable of degree p over k. We claim that E is the *unique* field strictly between L and k, so L/k *cannot* be expressed as a tower of a separable extension on top of a purely inseparable one!

Suppose that there is another intermediate extension E', so necessarily $[L:E'] = p = [E':k]$ yet E' does not contain E and so there is no room for separability: necessarily E'/k is purely inseparable. But L/k is not purely inseparable, so L/E' cannot be purely inseparable (why not?). Thus, the degree-p extension $L = E'(a)$ over E' must be separable, which is to say that the minimal polynomial h for a over this hypothetical E' is a degree-p separable irreducible polynomial over E'. Certainly $h|f$ since $f(a) = 0$ and $f \in k[T] \subset E'[T]$. But in a splitting field for f over k, there are exactly p distinct monic linear factors, each appearing with multiplicity p (why?), so the separable monic degree-p factor h of f has to be the product of those p distinct monic linear factors. In other words, necessarily $h^p = f$. It follows from staring at the definition of f that h would have to be $T^p + xT + y$ where $x^p = X$ and $y^p = Y$, so E' would have to contain a subfield $k(x,y)$ with $x^p = X$ and $y^p = Y$. But $k = \mathbf{F}_p(X,Y)$, over which the field obtained by adjoining $X^{1/p}$ and $Y^{1/p}$ has degree p^2 (why?). This is incompatible with containment in the hypothetical extension E'/k of degree p.

But here is an elementary proof using counting of embeddings that both separable and inseparable degrees are mutliplicative in towers. Since $[K:k]_{\mathrm{s}}[K:k]_{\mathrm{i}} = [K:k]$ is multiplicative in towers of finite extensions, to prove multiplicativity of the separable and inseparable degrees it suffices to treat the case of separable degrees. It suffices to prove the formula

$$[K:k]_{\mathrm{s}} = \#\,\mathrm{Hom}_k(K, \overline{k})$$

for an algebraic closure $\overline{k}/k$. Indeed, any such k-embedding j identifies $\overline{k}$ as an algebraic closure of K (!) and so if this formula is proved in general and K'/K is a finite extension then the number $\#\,\mathrm{Hom}_j(K', \overline{k})$ of embeddings of K' into $\overline{k}$ over j equals $\#\,\mathrm{Hom}_K(K', \overline{K}) = [K':K]_s$. Thus, summing over all j would yield

$$\#\,\mathrm{Hom}_k(K', \overline{k}) = \sum_j \#\,\mathrm{Hom}_j(K', \overline{k}) = \#\,\mathrm{Hom}_K(K', \overline{K}) \cdot \#\,\mathrm{Hom}_k(K, \overline{k}),$$

equivalently $[K' : k]_{\mathrm{s}} = [K' : K]_{\mathrm{s}}[K : k]_{\mathrm{s}}$ as desired.

To prove the proposed formula for $[K : k]_{\mathrm{s}}$, let k'/k be the separable closure of k in K, so certainly $[K : k]_{\mathrm{s}} := [k' : k] = \#\operatorname{Hom}_k(k', \overline{k})$. Thus, we just need to check that every k-embedding $j : k' \to \overline{k}$ *extends uniquely* to a k-embedding $K \to \overline{k}$. Every element of K has a p-power contained in k', so uniqueness of p-power roots in $\overline{k}$ implies that an extension of j to K is certainly unique if it exists (e.g., if $a \in K$ and $a^{p^n} \in k'$ then the only possibility is for a to be taken to $j(a^{p^n})^{1/p^n} \in \overline{k}$). This shows that j has *at most one* extension to K, and such an extension certainly exists since j identifies $\overline{k}$ as an algebraic closure of k' (namely, as an algebraic extension that is algebraically closed) and thus the algebraic extension K/k' can be embedded into $\overline{k}$ over j.

2. Perfect closure

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 saw in class that L/k' is purely inseparable.

We fix an algebraic closure $\overline{k}$ and we let k_s denote the separable closure of k inside of $\overline{k}$. That is, k_s is the set of $x \in \overline{k}$ which are separable over k. In particular, k_s is separably closed (i.e., it has no nontrivial separable extensions, or equivalently its algebraic extensions are purely inseparable).

Whereas a separable closure is a "maximal" separable algebraic extension, for the property of perfectness we seek a "minimality" property: the "smallest" algebraic extension that is perfect. More specifically:

Proposition 2.1. *Let K/k be an algebraic extension. The following are equivalent.*

(1) *The extension K/k is perfect and purely inseparable.*
(2) *The extension K/k is perfect and is minimal as such in the sense that every perfect extension field L/k admits a k-embedding $K \hookrightarrow L$.*

Extensions satisfying this property always exist, the embedding in (2) *in unique, and any two such K/k are* uniquely *k-isomorphic. Explicitly, such an extension is $k_{\mathrm{p}} = \{a \in \overline{k} \,|\, a^{p^n} \in k \text{ for some } n \geq 0\}$.*

An extension K/k as in this result is called a *perfect closure* of k. In contrast with separable closures, which have massive automorphism group in general (the topic of "infinite Galois theory"), perfect closures have *trivial* automorphism group. In particular, it is legal to speak of "the" perfect closure (since it is unique up to *unique* isomorphism), in contrast with separable closures, normal closures, and algebraic closures.

Proof. Since the p-power map is additive in characteristic p, it is clear that the subset $k_{\mathrm{p}} \subset \overline{k}$ as explicitly defined above is a subfield of $\overline{k}$ containing k that is purely inseparable over k. Moreover, it is perfect since if $a \in k_{\mathrm{p}}$ then the pth root $a^{1/p} \in \overline{k}$ satisfies $(a^{1/p})^{p^{n+1}} = a^{p^n}$, which lies in k for sufficiently large n. Hence, $a^{1/p} \in k_{\mathrm{p}}$ too, so k_{p} is perfect as well. That is, k_{p} satisfies the properties in (1). It also satisfies the minimality property in (2). Indeed, if L/k is a perfect extension then we pick an embedding $\overline{k} \hookrightarrow \overline{L}$ over $k \to L$ and we claim that k_{p} thereby is carried into L. Indeed, for any $a \in k_{\mathrm{p}}$ we have $a^{p^n} \in k$ for some large n, yet $k \subset L$ with $L = L^p$, so the element a^{p^n} in k has a p^nth root in L. Thus, working inside $\overline{L}$, the uniqueness of p-power roots in characteristic p implies that this p^nth root in L must be a. That is, $k_{\mathrm{p}} \subset L$. This provides the k-embedding in (2).

If K/k is an algebraic extension satisfying either (1) or (2) then we claim that K is k-isomorphic to k_{p}. First suppose it satisfies (2), so there is a k-embedding $j : K \to k_{\mathrm{p}}$. But K is perfect and k_{p} is purely inseparable over k, so k_{p} is also purely inseparable over any intermediate field, such as K. In other words, the extension k_{p}/K is purely inseparable, yet also separable since K is *perfect*. The only separable algebraic extension that is purely inseparable is the trivial extension (why?), so it follows that j is an isomorphism. If instead K/k satisfies (1) then by perfectness of K we get a k-embedding $k_{\mathrm{p}} \to K$. Yet this map is a purely inseparable extension (since K/k is purely inseparable) as well as separable (since it is an algebraic extension of the field k_{p} that is a *perfect* field), so once again it must be an isomorphism.

To prove the uniqueness results (for embeddings and isomorphisms over k), it suffices to handle the case of embeddings. If $j : K \to L$ is a k-embedding then for each $a \in K$ we have $a^{p^n} \in k$ for some $n \geq 0$, so

$j(a^{p^n}) = a^{p^n}$ inside L. But $j(a^{p^n}) = j(a)^{p^n}$, so $j(a) \in L$ has to be a p^nth root of a^{p^n} when viewed in L via $k \to L$. By uniqueness of p-power roots in characteristic p, it follows that $j(a)$ is uniquely determined. ■

Example 2.2. Let $k = k_0(t)$ where k_0 is perfect of characteristic p (e.g., a finite field of p-power size). It is hopeless to describe $\overline{k}$ or k_s, but k_{p} is very easy to describe: it is $\bigcup_{n \geq 0} k_0(t^{1/p^n})$. Indeed, for any $f = \sum a_i t^i \in k_0[t]$, we have $a_i = b_i^{p^n}$ for some $b_i \in k_0$ since k_0 is perfect, so $f = h^{p^n}$ for $h = \sum b_i (t^{1/p^n})^i$. Passing to ratios of polynomials, we see that $k_0(t^{1/p^n}) = k^{1/p^n}$ inside $\overline{k}$. This gives the assertion. (Beware that if we do not assume k_0 to be perfect then we need to adjoin all k_0^{1/p^n} as well to get k_{p}.)

Here is an amusing way to build up $\overline{k}$ from separable and purely inseparable parts:

Proposition 2.3. *The natural map $\mu : k_s \otimes_k k_{\mathrm{p}} \to \overline{k}$ defined by $a \otimes b \mapsto ab$ is an isomorphism. More generally, if k'/k is a separable algebraic extension then $k' \otimes_k k_{\mathrm{p}}$ is a field that is a perfect closure of k'.*

Proof. The key is to show that $K := k' \otimes_k k_{\mathrm{p}}$ is a field. Granting this, we can conclude as follows. Clearly the field K is purely inseparable over k' (since any finite sum of elementary tensors has a big p-power than visibly lies in k', depending on the elements of k_{p} which appear in the elementary tensors), yet it is also a perfect field since it is visibly an algebraic extension of the perfect field k_{p}. This gives that K is a perfect closure of k' (in view of the properties which we have shown uniquely characterize the perfect closure).

When $k' = k_s$ then K would be the perfect closure of a separably closed field, so K is both perfect and separably closed (as any algebraic extension of a separably closed field is separably closed; why?), forcing it to be algebraically closed. In other words, μ would be an algebraic extension map between algebraically closed fields, so μ is indeed an isomorphism.

It remains to show that K is a field. Each element of K is a finite sum of elementary tensors, and so lies in $k_0' \otimes_k k_{\mathrm{p}}$ for a finite separable extension k_0'/k contained in k_s. It suffices to show that each $k_0' \otimes_k k_{\mathrm{p}}$ is a field. By the primitive element theorem, $k_0' = k(a) = k[a]$ for some a separable over k, say with minimal polynomial f. Then $k_0' = k[x]/(f)$, so $k_0' \otimes_k k_{\mathrm{p}} = k_{\mathrm{p}}[x]/(f)$. Thus, it suffices to show that the separable irreducible monic $f \in k[x]$ remains irreducible over k_{p}. Suppose there is a factorization $f = f_1 f_2$ with each $f_j \in k_{\mathrm{p}}[x]$ monic. We shall prove that $f_j \in k[x]$ for both j, so this is a trivial factorization. By monicity, the coefficients of each f_j are elementary symmetric functions in the roots of f_j, which in turn are roots of f, so each is *separable* over k! Yet these coefficients lie in the extension k_{p}/k that is purely inseparable and hence has *no* nontrivial separable subextensions over k. This forces the coefficients of f_1 and f_2 to both lie in k, as desired. ■

A more concrete way to think about the preceding proposition is this: if k' is an extension of k inside $\overline{k}$, then the compositum $k'k_{\mathrm{p}}$ formed inside $\overline{k}$ is the perfect closure of k'. Indeed, the natural map $k' \otimes_k k_{\mathrm{p}} \to \overline{k}$ was just shown to always be an isomorphism onto k'_{p}, yet clearly the image as a field has to coincide with $k'k_{\mathrm{p}}$. But this "compositum" viewpoint adapts to situations in which separability of k' is dropped (so $k' \otimes_k k_{\mathrm{p}}$ generally fails to be a field):

Proposition 2.4. *Let K/k be any algebraic extension inside $\overline{k}$. The compositum Kk_{p} is the perfect closure of K inside $\overline{k}$.*

Proof. Certainly Kk_{p} is perfect, since it is an algebraic extension of the perfect field k_{p}. Yet it is purely inseparable over K because every element of Kk_{p} is a rational expression involving only *finitely many* elements of k_{p}. This expression is clearly carried into K when we apply a huge p-power (enough to bring into k the finitely many elements of k_{p} that arise). Hence, in view of the unique characterization of perfect closures, we are done. ■

Here is a companion result:

Proposition 2.5. *If k'/k is a purely inseparable extension then $k_s \otimes_k k'$ is a field that is a separable closure of k'. More generally, if k'/k is an arbitrary subfield of $\overline{k}$ over k then the compositum $k_s k'$ inside $\overline{k}$ is the separable closure of k' in $\overline{k}$ (so it is a separable closure of k').*

Proof. The method of proof of Proposition 2.3 carries over to show that $k_s \otimes_k k'$ is a field (by replacing k_s/k with a finite subextension to which the primitive element theorem may be applied, and using that k'/k is purely inseparable). Its image in $\overline{k}$ under the map $a \otimes b \mapsto ab$ after choosing a k-embedding of k' into $\overline{k}$ is therefore a subfield of $\overline{k}$ that must be the compositum $k_s k'$. Hence, it suffices to show that for an arbitrary extension k'/k inside $\overline{k}$, the compositum $k_s k'$ coincides with the separable closure k'_s of k' in $\overline{k}$.

Since $k \subseteq k'$, certainly all elements of $\overline{k}$ separable over k are separable over k'. This forces $k_s \subseteq k'_s$, so $k_s k' \subseteq k'_s$. Clearly $k_s k'$ is a separable algebraic extension of k' (since k_s/k is separable algebraic), and it sits between k' and k'_s, so to conclude equality with k'_s we just need to check that $k_s k'$ is separably closed. But $k_s k'$ is an algebraic extension of the separably closed field k_s, so it *must* be separably closed (as $\overline{k}$ is a common algebraic closure of everything in sight and it is purely inseparable over k_s, hence also purely inseparable over the extension $k_s k'$ of k_s). ∎

We conclude with a nifty interpretation of the separable and inseparable degrees via composites with perfect and separable closures, from which the multiplicativity of separable and inseparable degrees can be seen in another way (as a special case of ordinary multiplicativity of field degrees). Briefly, the idea is that forming the compositum with k_{p} eats up all of the inseparable data and leaves behind only the separable degree, whereas forming the compositum with k_s eats up the separable part and only leaves behind the inseparable degree.

Theorem 2.6. *For L/k an arbitrary finite extension inside $\overline{k}$, we have*

$$[L : k]_{\mathrm{s}} = [L_{\mathrm{p}} : k_{\mathrm{p}}] = [Lk_{\mathrm{p}} : k_{\mathrm{p}}], \;\; [L : k]_{\mathrm{i}} = [L_s : k_s] = [Lk_s : k_s].$$

Proof. The second equality in both cases comes from our descriptions of separable and perfect closures as composite fields above. Thus, it suffices to prove the equality of first and third terms in both cases.

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 $k_{\mathrm{p}}L/k_{\mathrm{p}}k'/k_{\mathrm{p}}$. Since $Lk_{\mathrm{p}}/k_{\mathrm{p}}k'$ is a purely inseparable extension (as L/k' is purely inseparable) and the field $k_{\mathrm{p}}k'$ is perfect (being algebraic over the perfect field k_{p}), we conclude that the extension $Lk_{\mathrm{p}}/k'k_{\mathrm{p}}$ is trivial (i.e., degree 1)! Thus, $[Lk_{\mathrm{p}} : k_{\mathrm{p}}] = [k'k_{\mathrm{p}} : k]$. 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 $[L : k] = [k_{\mathrm{p}}L : k_{\mathrm{p}}]$. But this is clear, since we have seen earlier that for separable L/k,

$$k_{\mathrm{p}}L = Lk_{\mathrm{p}} \simeq L \otimes_k k_{\mathrm{p}},$$

and the right side clearly has k_{p}-dimension equal to $[L : k]$.

Next we show that $[L : k]_{\mathrm{i}} = [Lk_s : k_s]$. Once again using k', by definition $[L : k]_{\mathrm{i}} = [L : k']$ yet $k_s = k'_s$ since $k' \subset k_s$ (as k'/k is separable inside $\overline{k}$). Thus, we can replace k with k' to reduce to the case that L/k is purely inseparable. Then our tensor product computations give that $Lk_s = L \otimes_k k_s$, which visibly has k_s-dimension equal to $[L : k]$. ∎