Day 1: Primer on Field Extensions

Tom Gannon

August 14, 2017

1 Introduction

Today we'll show that the *separable closure* of a field extension K/F (i.e. the set of elements separable over F) is a field. We will further show that this separable closure L has the property that K/L is a *purely inseparable extension*, which we'll define shortly. A good reference for this is Keith Conrad's blurb *Separable Extensions*, which you can find by googling it.

1.1 Primer on Separability

For the whole day, we'll fix a field F, which we'll refer to the "base" or the "ground" field whenever I feel like changing it up and typing more letters out than just typing the letter F. Moreover, we'll fix an algebraic closure $\overline{F}$ that all the action of today is going to be taking place in–meaning that any field extension we refer to is implicitly assumed to be a subset of $\overline{F}$. If you want a proof that such a thing exists, it's in Dummit and Foote. We'll start off with some basics regarding this:

Definition 1.1. *We say that an element $\alpha \in \overline{F}$ is* ***separable*** *over F if the minimal polynomial of α over F, say $q(x)$, does not have α as a multiple root–that is, $(x-\alpha)^2 \nmid q(x)$. We say a field extension K/F is* ***separable*** *if every element in K is separable over F.*

It isn't too hard to check whether a given element is separable once you know its minimal polynomial:

Exercise 1.2. *Assume $p(x) \in F[x]$ has root α. Show $p(x)$ has a multiple root α (that is, $(x-\alpha)^2 | p(x)$ if and only if the (formal) derivative $p'(x)$ has α as a root). (Hint: Show that the product rule formally holds and write $p(x) = q(x)(x-a)$).*

For a topic that is not analysis, the derivative comes up a lot more than you might think. For example:

Exercise 1.3. *Fix $\alpha \in \overline{F}$, and let $q(x) \in F[x]$ denote the minimal polynomial of α. Show that $q(x)$ has α as a multiple root if and only if $q'(x) = 0$. Conclude that no irreducible polynomial over a field of characteristic zero has a multiple root, and classify those polynomials with coefficients in a field of characteristic p which have derivative zero.*

In particular, every polynomial over $\mathbb{Q}$ is separable.

1.2 Primer on Morphisms of Fields

Morphisms of fields $F_1 \to F_2$ are just ring morphisms–that is, maps that preserve the addition and multiplication structure of the ring. By convention, we'll require our ring maps send $1 \to 1$. With this convention, we have an interesting phenomenon:

Exercise 1.4. *Show that any map of fields is an embedding/injection.*

We'll use the two terms embedding and injection interchangeably. This result suggests that field embeddings are the things we should look closer at. One natural question is, if K/F is a finite dimensional field extension, how many different ways can we embed K in a different way into some subfield of $\overline{F}$ (meaning, for example, that the identity and conjugation maps $\mathbb{C} \to \mathbb{C}$ represent distinct maps)?

2 Primer on Separable Closure

Exercise 2.1. *(Bound on Embeddings) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are at most n distinct embeddings $K \hookrightarrow \overline{F}$ which fix F pointwise. (Hint: Let $K = F(\alpha_1, ..., \alpha_n)$ and proceed by induction on n, noting that $n = [K : F] = [F(\alpha_1, ..., \alpha_n) : F(\alpha_1, ..., \alpha_{n-1})]...[F(\alpha_1) : F]$. Most of the work should be done in the base case.)*

Exercise 2.2. *(Separability Maximizes Embeddings) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are **exactly** n distinct embeddings $K \hookrightarrow \overline{F}$ which fix F pointwise if and only if K/F is separable. (Hint: Most of the work you did in the last exercise–argue wherever you wrote "$\leq$", you should argue why equality holds.)*

Exercise 2.3. *(Sneakily proving that a field is separable if and only if some set of generators is separable, except it's not that sneaky because I'm putting it in these parenthesis) Let K/F be an $n \in \mathbb{N}^{>0}$ dimensional extension of fields. Show that there are **exactly** n distinct embeddings $K \hookrightarrow \overline{F}$ which fix F pointwise if and only if $K = F(\alpha_1, ..., \alpha_n)$ and each α_i is separable over F. (Again, you did of the work you did in the last exercise. For "only if," argue by contrapositive and argue why "$<$" needs to occur somewhere).*

Oh but look! If you put those last two exercises together in the obvious way, you get:

Corollary 2.4. *A finite dimensional field extension K/F is separable if and only if some generating set of K/F contains only separable elements.*

Exercise 2.5. *Show that if $\alpha, \beta \in \overline{F}$ are separable over F, then $\alpha \pm \beta$, $\alpha\beta$ and α^{-1} are also separable over F. (If you want some algebra fun, you can argue α^{-1} is separable over F directly, but the others are not so easy to do directly).*

Corollary 2.6. *The **separable closure** K_{sep} of a field extension K/F, defined to be the set of all elements of K separable over F, is a field.*

Definition 2.7. *We define the **separability degree** of an extension K/F to be the degree of $[K_{sep} : F]$.*

3 Primer on Purely Inseparable Extensions

Definition 3.1. *A field extension E/L is said to be **purely inseparable** over L if $p := char(L)$ is nonzero*[1] *and for all $\alpha \in E, \alpha$ raised to the power p^n for some n is in L (written more normally, this means there is some $n \in \mathbb{N}^{>0}$ such that $\alpha^{p^n} \in L$, but I always would misread that as $(\alpha^p)^n \in L$, which isn't the same thing) or $E = L$.*[2]

Exercise 3.2. *(Alternate Definition of Purely Inseparable Extensions) Show that equivalently a purely inseparable extension E/L with $p := char(L) > 0$ is an extension where for all $\alpha \in E$, the minimal polynomial of α over E is $x^{p^n} - \alpha^{p^n}$ (again "alpha raised to a power that is itself a power of p") for some $n \in \mathbb{N}$.*

Exercise 3.3. *(Alternate Definition of Purely Inseparable Extensions) Show that equivalently a purely inseparable extension E/L is an extension where for all $\alpha \in E$, if α is separable over E then $\alpha \in L$.*

To close this fun off, you should prove the below theorem (which is actually just one finishing step):

Theorem 3.4. *(Field Extensions Split into Separable and Purely Inseparable Extensions) Given any finite dimensional extension K/F, then there exists an intermediate field L with $F \subset L \subset K$ where L/F is separable and K/L is purely inseparable.*

This idea will be used a lot. Want to prove something is true for all field extensions? Can you prove it for a separable field extension and a purely inseparable one and then show that if your statement is true for L/F and K/L then it's true for K/F.

[1] Fun fact! One way to view the characteristic of a field L is to view it as number n such that $n\mathbb{Z}$ is the kernel of the unique map $\mathbb{Z} \to L$. This explains why the characteristic of $\mathbb{Q}$ is said to be 0 instead of what you might have thought would be natural at first, "characteristic ∞".

[2] This is a technical condition you don't really need to worry about–it's just stated to make the last theorem of this paper sound more clean. Also, two footnotes in one definition! How cool is that?!