Math 210B. Differential criterion and primitivity

In this handout we review the role of derivatives to detect separability (to be generalized later using modules of differentials) and look at the Primitive Element Theorem from two viewpoints.

1. Derivatives

Let $f \in k[X]$ be a nonzero element, with degree $d \geq 0$. Recall that f is called *separable* if it has d distinct roots in a splitting field. In this handout, we will prove a "differential criterion" for separability. This admits vast generalizations of much use in algebraic geometry.

Recall that for $g, h \in k[X]$ not both zero, we define $\gcd(g, h)$ to be the unique monic generator of the ideal (g, h). It is easy to check (do it!) that this is exactly the monic common factor of g and h with largest degree. (One can mull over whether it is appropriate to declare $\gcd(0, 0) = 0$, but this is not a good idea. Best to avoid gcd's when both arguments vanish.) If we want to keep track of k in the notation, we may write $\gcd_k(g, h)$ instead. As a preliminary step, we first check that it isn't necessary to keep track of k:

Lemma 1.1. *If L/k is an extension of fields and $g, h \in k[X]$ are not both zero then for $d := \gcd_k(g, h) \in k[X]$ we have $d = \gcd_L(g, h)$ in $L[X]$.*

Proof. Write $g = Gd$ and $h = Hd$ for $G, H \in k[X]$ not both zero, so $\gcd_k(G, H) = 1$. It suffices to prove that $\gcd_L(G, H) = 1$. But we know (using that $k[X]$ is a PID) that there exist $F_1, F_2 \in k[X]$ such that $F_1G + F_2G = 1$. This identity persists in $L[X]$, so certainly G and H cannot share a common monic factor with positive degree in $L[X]$. ■

Here is the main result:

Proposition 1.2. *For nonzero $f \in k[X]$, f is separable if and only if $\gcd(f, f') = 1$.*

Beware that if $\deg(f) > 0$ then f' might vanish when $\mathrm{char}(k) = p > 0$ (namely, when $f = h(X^p)$ for some h), so for efficient uniform proofs it is important that we allow for gcd's in which one of the two arguments vanishes (provided the other does not).

Proof. In view of the lemma above, it is harmless to replace k with a splitting field of f, and we may also assume f is monic. Thus, we have $f = \prod(X - r_i)$ for some $r_i \in k$, and we want to show that the list of r_i's has no repetition if and only if $\gcd(f, f') = 1$.

First suppose there is no repetition. Assuming $\gcd(f, f') \neq 1$, we seek a contradiction. Such nontriviality of the gcd implies that some irreducible factor of f also divides f' (this makes sense even if $f' = 0$), which is to say some $X - r_{i_0}$ divides f' (equivalently, $f'(r_{i_0}) = 0$). We claim that r_{i_0} occurs more than once in the list of roots (with multiplicity). By relabeling we can assume $i_0 = 1$, so $f = (X - r_1)h$ where $h = \prod_{i>1}(X - r_i)$. Then by the Leibnitz Rule, $f' = (X - r_1)h' + h$. Evaluating at r_1 which we assume is a root of f' too, we get $0 = f'(r_1) = h(r_1) = \prod_{i>1}(r_1 - r_i)$. Thus, $r_1 = r_i$ for some $i > 1$, giving the repetition that we claimed.

Conversely, assuming $\gcd(f, f') = 1$, we need to show that the list of roots of f (with multiplicity) has no repeated root. Assume to the contrary that some root appears at least twice, which is to say $f = (X - r)^2 g$ for some g. Then $f' = 2(X - r)g + (X - r)^2 g' = (X - r)(2g + (X - r)g')$, so $X - r$ is a common factor of f and f'. This contradicts that $\gcd(f, f') = 1$. ■

As an illustration, assume f is a monic *irreducible* in $k[X]$ (so $\deg(f) > 0$). Thus, $\gcd(f, f')$ is equal to 1 or f, so by the Proposition such an f fails to be separable if and only if $f | f'$. By considering degrees, this divisibility occurs if and only if $f' = 0$. Such vanishing is impossible if $\mathrm{char}(k) = 0$, but can occur if $\mathrm{char}(k) = p > 0$ and $f = h(X^p)$ for $h \in k[X]$ that clearly must

be irreducible. Conversely, by HW1 Exercise 6(i), for monic irreducible $h \in k[X]$ and $\mathrm{char}(k) = p > 0$, $h(X^p)$ is irreducible if and only if $h \notin k^p[X]$ (impossible if $k = k^p$, as for finite k). The phenomenon of non-separable irreducible polynomials is a ubiquitous fact of life over fields of positive characteristic.

2. Primitive extensions

For a primitive algebraic extension $k(a)/k$ there are two topics we wish to address: (i) showing that all separable finite extensions are primitive, (ii) giving an "intrinsic" characterization of exactly which finite extensions are primitive. The first of these is by far the more important one in applications, but the second is amusing nonetheless. For both proofs, the case of finite fields will be treated separately.

Theorem 2.1 (Primitive Element Theorem)**.** *Let k'/k be a finite separable extension. There exists $a \in k'$ such that $k' = k(a)$.*

Proof. If k is finite then so is k', so we know ${k'}^\times = k' - \{0\}$ is cyclic. A generator a of this cyclic group then does the job. Hence, we may and do now assume that k is infinite.

We may write $k' = k(a_1, \ldots, a_n)$ and we shall induct on n. Since

$$k' = k(a_1)(a_2, \ldots, a_n),$$

using induction easily reduces the problem to the case of two generators: $k' = k(a, b)$. We consider elements $c = a + bt$ with $t \in k$. We will use the infinitude of k to find t so that $k' = k(a + tb)$.

Let L/k be a Galois closure of the finite separable k'/k, so $[k' : k]$ is the number of k-embeddings of k' into L. For each $t \in k$ we let $K_t = k(a + tb) \subseteq k'$. Since K_t is a subfield of k' over k, we have $K_t = k'$ if and only if $[K_t : k] = [k' : k]$. Hence, it suffices to find t so that the distinct k-embeddings $k' \to L$ are distinct on K_t, which amounts to being distinct on $a + bt$.

For any k-embedding $i : K_t \to L$, we have $i(a + tb) = i(a) + ti(b)$ since $t \in k$. We seek $t \in k$ such that for every pair of distinct k-embeddings $i, i' : k' \rightrightarrows L$ the elements

$$i(a) + ti(b), i'(a) + ti'(b) \in L$$

are distinct. That is, we want

$$(i(a) - i'(a)) + t(i(b) - i'(b)) \neq 0$$

in L. If $i(b) - i'(b) = 0$ (so $i(b) = i'(b)$) then necessarily $i(a) - i'(a) \neq 0$ since i and i' are not the same on $k' = k(a, b)$. Thus, we just need to focus on pairs $\{i, i'\}$ such that $i(b) - i'(b) \neq 0$. But then the ratios

$$\frac{-(i(a) - i'(a))}{i(b) - i'(b)} \in L$$

make sense and range through just finitely many values in L as we vary $\{i, i'\}$. Since k is *infinite*, we can certainly find $t \in k$ avoiding those finitely many values in L. ∎

By HW1 Exercise 3 that there are examples of finite extensions of fields which have *infinitely many* intermediate fields. We now show that finiteness of the set of intermediate fields is closely related to primitivity:

Theorem 2.2. *A finite extension k'/k is primitive if and only if it has finitely many intermediate fields.*

Proof. First assume that there are finitely many intermediate fields. To show that k'/k is primitive, we write $k' = k(a_1, \ldots, a_n)$ and we induct on n (the case $n = 1$ being trivial). The subfield $k(a_2, \ldots, a_n)$ certainly also has only finitely many intermediate fields between it and k, so by induction this field is primitive: it is $k(b)$ for some b, so $k' = k(a, b)$ for $a = a_1$. This brings us to the key case of 2 generators. We may assume as well that k is infinite, since we have already seen in the previous proof that finite extensions of finite fields are always primitive.

We again consider the family of candidate generates $a + tb$ with $t \in k$. Let $K_t = k(a + tb)$. We seek to show that $K_t = k'$ for many t. As we vary t through the *infinitely many* values in k, the intermediate fields K_t vary through just finitely many possibilities precisely because we are assuming that k'/k has only finitely many intermediate fields. It follows that there must be some distinct $t, t' \in k$ such that $K_t = K_{t'}$. But then this intermediate extension of k contains $(a + tb) - (a + t'b) = (t - t')b$. Since $t - t' \in k^\times$, it follows that the common intermediate field $K_t = K_{t'}$ contains $(t-t')b$ as well as $1/(t-t') \in k^\times$, so it contains b and therefore also $(a+tb)-tb = a$. This forces the primitive extension K_t to coincide with $k(a, b) = k'$.

Now for the converse: we assume $k' = k(a)$ and we shall "bound" the possible intermediate extensions to be within a finite set of possibilities. Let $f \in k[x]$ be the (monic) minimal polynomial of a over k. To each L we associate the minimal polynomial f_L of a over L, which is a monic factor of f in $k'[x]$. We just have to show that if $L, L' \subseteq k'$ are two subfields over k and $f_L = f_{L'}$ inside $k'[x]$ then $L = L'$ inside k' (not just an abstract k-isomorphism between L and L', but literal equality as subfields of k' containing k). To do this, we give a simple mechanism to reconstruct L from f_L.

Consider the coefficients: $f_L = \sum c_i x^i$. These coefficients c_i all lie in L (as f_L is a minimal polynomial over $L[x]$), so they generate over k a subfield $K := k(c_1, \ldots) \subseteq L$. I claim that this inclusion is an equality, which will finish the proof. We have have to show that $[K : k] = [L : k]$. Since f_L is irreducible over L, and so also is irreducible over its subfield K, the expressions $k' = k(a) = L(a)$ and $k' = k(a) = K(a)$ force

$$[k' : L] = \deg(f_L) = [k' : K].$$

Dividing this common value into $[k' : k]$ then gives $[K : k] = [L : k]$ as desired. ∎