Mathematics 3360
Separable polynomials
Ken Brown, Cornell University, April 2010

Let $f(x)$ be a polynomial of degree $n \geq 1$ with coefficients in a field F. When we form a splitting field $K \supseteq F$ of f, it is of interest to know whether or not f will split into n *distinct* linear factors. In other words, we're asking whether f has n distinct roots in K. In this case we say that f is *separable*. The other possibility is that the factorization of f will have a repeated linear factor. Can we predict in advance which case will occur? It turns out that we can, using ideas from calculus.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, we define the *derivative* of f by

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Note that no limits are needed since we're only dealing with polynomials. The factors $n, n-1, \ldots$ that occur in the definition are to be interpreted via the (unique) ring homomorphism $\mathbb{Z} \to F$. Recall that if F has characteristic 0, this homomorphism is 1–1, so that its image is an isomorphic copy of $\mathbb{Z}$. If F has characteristic p, on the other hand, then the image is an isomorphic copy of $\mathbb{F}_p$, and we can think of $n, n-1, \ldots$ as representing their classes mod p.

It is possible to verify that all the usual differentiation rules remain valid in this algebraic setting. For example, we have the product rule

$$(fg)' = f'g + fg'.$$

The purpose of this handout is to prove the following criterion for separability:

Theorem 1. *f is separable if and only if f and its derivative f' are coprime in $F[x]$.*

So we have a simple test (via the Euclidean algorithm), that doesn't require actually constructing the splitting field.

Example 1. Let $F = \mathbb{Q}$ and $f(x) = x^3 - 2$. Then $f'(x) = 3x^2$, which is coprime to $f(x)$, since the only irreducible factor of f' is x, which does not divide f. Therefore f has 3 distinct roots in a suitable extension field. (If you're familiar with the geometry of the complex numbers, you probably knew this already. In fact, you can draw a picture that shows the 3 complex roots.)

Example 2. Let $F = \mathbb{F}_p$ and $f(x) = x^p - x$. Then $f'(x) = -1$, which is trivially coprime to f. So f has p distinct roots in some extension field. In fact, the roots are already in $\mathbb{F}_p$ and consist of all the elements of $\mathbb{F}_p$ by Fermat's theorem.

Example 3. Let $\mathbb{F} = \mathbb{F}_p$ and $f(x) = x^q - x$, where $q = p^k$ for some integer $k \geq 1$. Then the same argument as in Example 2 shows that f separable and so has q distinct roots in some extension field. This time the result is much less obvious. The splitting field turns out to be the field $\mathbb{F}_q$ with q elements, and the separability result that we've just noticed is the first step in the proof that this field exists.

The proof of the theorem uses the following result, which might look familiar from calculus (graphing, Taylor's theorem,...).

Lemma 1. *Given $f(x) \in F[x]$ and $a \in F$, f is divisible by $(x-a)^2$ if and only if $f(a) = 0$ and $f'(a) = 0$.*

Proof. Suppose f is divisible by $(x-a)^2$, and write

$$f(x) = (x-a)^2 g(x)$$

with $g(x) \in F[x]$. Obviously $f(a) = 0$. To see that $f'(a) = 0$, compute $f'(x)$:

$$f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x).$$

Setting $x = a$, we get $f'(a) = 0$.

Conversely, suppose $f(a) = f'(a) = 0$. Since $f(a) = 0$, we can write

$$f(x) = (x-a)h(x)$$

with $h(x) \in F[x]$. Then

$$f'(x) = 1 \cdot h(x) + (x-a)h'(x),$$

and hence $f'(a) = h(a)$. But we're given that $f'(a) = 0$, so $h(a) = 0$ and $h(x)$ is divisible by $x - a$. Therefore $f(x)$ is divisible by $(x-a)^2$. □

Proof of the theorem. Let $K \supseteq F$ be a splitting field for f. Then f is separable if and only if no root a of f in K is repeated, i.e., if and only if there is no root a of f in K such that $f(x)$ is divisible by $(x-a)^2$. By the lemma, this holds if and only if f and f' have no common root in K, i.e., if and only if f and f' have no common linear factor in $K[x]$. Since f splits into linear factors in $K[x]$, all the irreducible divisors of f in $K[x]$ are linear, so f and f' have no common linear factor if and only if they are coprime in $K[x]$. Finally, observe that two polynomials in $F[x]$ are coprime in $K[x]$ if and only if they are coprime in $F[x]$, since their greatest common divisor can be computed by the Euclidean algorithm, which yields the same answer whether we think of the polynomials as being in $F[x]$ or in $K[x]$. □

Exercise 1. Let F be a field of characteristic 0. If $f(x)$ is an irreducible polynomial in $F[x]$, show that f is separable. Make sure your proof uses the assumption that F has characteristic 0; if it doesn't, you've been careless about an important detail.

Exercise 2. Let F be a field of characteristic p, and let $f(x) = x^p - a$ with $a \in F$.

(a) Show that f is not separable.

(b) Prove the stronger result that if K is a splitting field of f, then $f(x)$ has a single root $\alpha \in K$ of multiplicity p, i.e., $f(x) = (x-\alpha)^p$ in $K[x]$. [Hint: There is a really nice version of the binomial theorem in characteristic p; see Theorem 17 on p. 192 of your text.]