Separability of finite field extensions

J. Lubin

The aim is to show as quickly as possible that within a larger field Φ, the set of elements separable over a field k is itself a field.

Definition 1. Let α be an element that is algebraic over the field k. Then α is *separable* over k if the minimal polynomial for α over k, $\mathrm{Irr}\bigl(\alpha, k[X]\bigr)$, has no repeated roots.

Definition 2. Let $K \supset k$ be a finite-degree extension of fields. Then the *separable degree* of the extension, written $[K\colon k]_s$, is the number of distinct k-morphisms of K into an algebraically closed field $\Omega \supset k$.

It should be clear that this number (or cardinality) does not depend on the choice of Ω, and that an algebraic closure of k will suffice. We will see further on that $[K\colon k]_s \leq [K\colon k]$.

Definition 3. If $K \supset k$ is a finite-degree extension of fields, then the extension is *separable* if the separable degree is equal to the field extension degree.

Proposition 1. *Let α be an element algebraic over the field k. Then α is separable over k if and only if $k(\alpha)$ is a separable extension of k.*

Indeed, say that $\bigl[k(\alpha)\colon k\bigr] = n$ and the roots of the degree-n polynomial $\mathrm{Irr}\bigl(\alpha, k[X]\bigr)$ are distinct, say $\{\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n\}$, all lying in some algebraically closed field Ω. Then each k-morphism of $k[X]$ sending X to α_i has the same kernel, namely $\bigl(\mathrm{Irr}\bigl(\alpha, k[X]\bigr)\bigr)$, and we have induced n distinct k-morphisms of $k(\alpha)$ into Ω. There will be no others, cause α certainly must go to some root of $\mathrm{Irr}\bigl(\alpha, k[X]\bigr)$.

On the other hand, if $k(\alpha)$ is separable over k, the n distinct k-morphisms of this field into Ω must each send α to a root of the minimal polynomial, and each of these morphisms is entirely determined by the image of α. Thus the images of α under the various morphisms all are different.

Lemma 2. *Let Ω be a field containing k and K, where $K \supset k$ is a finite-degree extension, and let σ be any automorphism of Ω. Then $[K\colon k]_s = \bigl[\sigma(K)\colon \sigma(k)\bigr]_s$.*

Recall that if Ω is an algebraically closed field, then any morphism $k \to \Omega$ may be extended to an algebraic extension $K \supset k$.

Proposition 3. *Let $L \supset K \supset k$ be an extension of fields with $[L\colon k] < \infty$. Then $[L\colon k]_s = [L\colon K]_s \cdot [K\colon k]_s$.*

Let Ω be an algebraically closed extension of L, and let $\varphi\colon K \to \Omega$ be a k-morphism. Then φ may be extended to $\varphi'\colon L \to \Omega$, and the number of $\varphi'(K)$-morphisms of $\varphi'(L)$ into Ω is $\bigl[\varphi'(L)\colon \varphi'(K)\bigr]_s = [L\colon K]_s$. Count up all the k-morphisms of L into Ω, and get $[K\colon k]_s \cdot [L\colon K]_s$.

Corollary 4. *Let $L \supset K \supset k$ with $[L\colon k] < \infty$. If $K \supset k$ and $L \supset K$ are separable extensions, then so is $L \supset k$.*

Notice now that for a simple extension $k(\alpha) \supset k$, we certainly have the inequality $\bigl[k(\alpha)\colon k\bigr]_s \le \bigl[k(\alpha)\colon k\bigr]$. Then the multiplicativity of separable degree implies:

Proposition 5. *For a finite extension $K \supset k$, the inequality $[K\colon k]_s \le [K\colon k]$ holds.*

Corollary 6. *Let $L \supset k$ with $[L\colon k] < \infty$. If L is separable over k, then so are the extensions $L \supset K$ and $K \supset k$.*

Theorem 7. *Let $K \supset k$ be a finite extension. Then K is separable over k if and only if every element of K is separable over k.*

First, suppose that K is separable over k. Then $k(\alpha) \supset k$ is separable, so that α is a separable element. On the other hand, suppose that every element $\alpha \in K$ is separable over k. Take a finite generating set $\{\beta_1, \cdots, \beta_m\}$ for K over k and consider the chain of simple extensions

$$K_0 = k \subset K_1 \subset \cdots \subset K_{m-1} \subset K_m = K\,,$$

where $K_i = K_{i-1}(\beta_i)$ for $1 \le i \le m$. Since β_i is separable over k, the roots of $\operatorname{Irr}\bigl(\beta_i, k[X]\bigr)$ are simple; but $\operatorname{Irr}\bigl(\beta_i, K_{i-1}[X]\bigr)$ is a factor of that, and so its roots are simple. Thus $K_i \supset K_{i-1}$ is separable, and the whole tower is separable.

The same kind of argument shows:

Theorem 8. *Let $K \supset k$ be a finite separable extension, and let $F \supset k$ be an extension, with both K and F contained in a field Ω. Then FK is separable over F.*

For, if we take a tower of simple extensions between k and K, as we did in the previous proof, the corresponding elements give a tower of simple extensions between F and FK. Since the minimal polynomial for β_i over $F(\beta_1, \cdots, \beta_{i-1})$ is a factor of the minimal polynomial for β_i over $k(\beta_1, \cdots, \beta_{i-1})$, this simple extension is separable as well. So the total extension $F \subset FK$ is separable.

Theorem 9. *Let $K \supset k$ and $L \supset k$ be finite separable extensions. Then KL is separable over k.*

Follows directly from Corollary 4 and Theorem 8.

Corollary 10. *If α and β are separable over k, the field $k(\alpha, \beta)$ is separable over k.*

Corollary 11. *If $K \supset k$ is an algebraic extension of fields, the set of elements of K that are separable over k is a field.*

We may call this field the *maximal separable extension* of k in K.

Corollary 12. *Let $K \supset k$ be an algebraic extension of fields, and let k^s be the maximal separable extension of k in K. If k^s is finite over k, then $[k^s : k] = [K : k]_s$.*

Perhaps this requires a proof. Maximality of k^s in K means that every k-morphism of k^s into an algebraically closed field has exactly one extension to K. Thus $[K : k^s]_s = 1$. The result follows from multiplicativity of the separable degree and the fact that $[k^s : k] = [k^s : k]_s$.