

A NOTE ON SEPARABILITY

BERNDT E. SCHWERTDFEGER

Dedicated to Carmen

ABSTRACT. This note gathers key notions and proofs around *separability*.

© 2003–2015 Berndt E. Schwerdtfeger

v1.1, 2015-03-04

1. SEPARABILITY

1.1. **Notation.** An algebraic closure of a field K is denoted by \bar{K} . The polynomial ring over a field K is denoted by $K[X]$ (we reserve X for this purpose).

If t is algebraic over K and $K[X] \rightarrow K[t] \rightarrow 0$ is the canonical mapping, its kernel is generated by a unique irreducible polynomial $g = \text{Irr}(t, K)$ of the form $g = X^d + a_1 X^{d-1} + \dots + a_d$ where $d = [K(t) : K]$ is the degree of the field extension.

If $\sigma : K \rightarrow \bar{K}$ is a morphism (necessarily injective), we denote its effect on field elements also by $\sigma(a) = a^\sigma$. We extend this operation to the polynomial ring $K[X]$ by applying it to the coefficients: $g^\sigma = X^d + a_1^\sigma X^{d-1} + \dots + a_d^\sigma$.

1.2. **An illustrative example.** Let $E = \mathbf{F}_2(t)$ be the field of rational functions in t over the prime field of characteristic 2. Now consider the subfield $K = \mathbf{F}_2(t^2)$. We have $t \notin K$, but $t^2 \in K$, therefore $\text{Irr}(t, K) = X^2 - t^2 = g \in K[X]$. The irreducible polynomial $g \in K[X]$ splits in $E[X]$ into two identical linear factors:

$$g = (X - t)^2$$

That the two roots of g can't be separated lies in the fact that $-t = t$, there are no primitive square roots of unity to *separate* them. A polynomial with unseparable roots is called *inseparable*.

The same circumstance obviously happens in any characteristic $p > 1$: we are missing the q^{th} roots of unity for any power $q = p^\mu$ of p . The reason for this phenomenon of *inseparability* is the missing of some roots of unity in positive characteristic p .

1.3. **Separable polynomials.** Let K be any field and \bar{K} an algebraic closure.

Let us systematically analyse the separability of roots of an irreducible polynomial $g \in K[X]$. A root t is a multiple root if and only if $g'(t) = 0$. But as g is irreducible and $\deg g' < \deg g$, we must have $g' = 0$.

Definition 1.1. An irreducible polynomial $g \in K[X]$ is called *separable* if $g' \neq 0$ and *inseparable* if $g' = 0$.

2010 *Mathematics Subject Classification.* Primary 12F10; Secondary 12F15.

Key words and phrases. separability, separation by roots of unity, simple extensions.

If a field K has no inseparable polynomials it is called *perfect*. In characteristic $\text{char } K = 0$ there are no inseparable polynomials, so these fields are perfect.

In $\text{char } K = p > 1$ an inseparable polynomial g has the form $g = h(X^p)$. If h is inseparable we can continue this process until we arrive at $g = h(X^q)$ with $h' \neq 0$ for some $q = p^\mu, \mu \geq 1$.

If the field K is finite, then $h(X^q) = (h^{1/q}(X))^q$ and g would be reducible, so finite fields are perfect as well. The same argument shows that algebraically closed fields are perfect, but this is obvious a priori as the only irreducible polynomials are linear by definition and therefore have only simple roots.

If $g = h(X^q)$ with $q = p^\mu, \mu \geq 0$ and $h' \neq 0$ we call $\deg h$ the *separable* degree of g and q its *inseparable* degree, $\deg g = \deg_{\text{sep}} g \cdot \deg_{\text{ins}} g$. The separable degree is the number of its roots and the inseparable degree is the common multiplicity of its roots.

Explicitely, when $g = X^d + a_1 X^{d-1} + \dots + a_d$ and $h = X^f + b_1 X^{f-1} + \dots + b_f$, then $d = q \cdot f$ and for $q > 1$ (the inseparable case) we have

$$\begin{aligned} a_{qr} &= b_r & 1 \leq r \leq f \\ a_{qr+s} &= 0 & 0 \leq r < f, 1 \leq s < q \end{aligned}$$

and in particular $a_1 = 0$.

2. SEPARABLE FIELD EXTENSIONS

2.1. Separable elements and extensions. Let E/K be a finite field extension.

Definition 2.1. An element $t \in E$ is called *separable* resp. *inseparable* over K , if $g = \text{Irr}(t, K)$ is separable resp. inseparable.

E/K is called *separable*, if each $t \in E$ is separable over K , otherwise *inseparable*.

The *separable degree* of E/K is defined as $[E : K]_{\text{sep}} = \text{card Hom}_K(E, \bar{K})$, the number of morphisms into an algebraic closure.

Proposition 2.1. *The separable degree is multiplicative in towers: Let $E/F/K$ be a tower of fields, then*

$$[E : K]_{\text{sep}} = [E : F]_{\text{sep}} [F : K]_{\text{sep}}$$

Proof. The restriction

$$\begin{aligned} \text{Hom}_K(E, \bar{K}) &\longrightarrow \text{Hom}_K(F, \bar{K}) \\ \sigma &\longmapsto \tau = \sigma|_F \end{aligned}$$

is surjective (see LANG [2, V, Th. 2.8]) and its fiber contains $[E : F]_{\text{sep}}$ elements. \square

Proposition 2.2. *For a simple algebraic extension $E = K(t)$ we have*

$$[E : K]_{\text{sep}} = \deg_{\text{sep}} \text{Irr}(t, K)$$

and this also implies that $[E : K]_{\text{sep}} \mid [E : K]$.

Proof. Let $g = \text{Irr}(t, K)$, we have $g = h(X^q)$, $h' \neq 0$ with $q = p^\mu, \mu \geq 0$ (in fact $\mu = 0$ exactly when t is separable, i.e. g has distinct roots).

$$d = \deg g = [E : K] = q \cdot f, \quad f = \deg h = \deg_{\text{sep}} g.$$

h has f roots in \bar{K} : $h = (X - \beta_1) \cdots (X - \beta_f)$.

Let $\alpha_1, \dots, \alpha_f$ be the unique elements in \bar{K} with $\alpha_i^q = \beta_i$, then

$$g = h(X^q) = (X^q - \beta_1) \cdots (X^q - \beta_f) = (X - \alpha_1)^q \cdots (X - \alpha_f)^q$$

We see that $f = [E : K]_{sep}$, as for any $\sigma \in \text{Hom}_K(E, \overline{K})$ we must have $\sigma(t) = \alpha_i$ for some $i, 1 \leq i \leq f$, qed. \square

Corollary 2.3. $[E : K]_{sep} \mid [E : K]$ holds for arbitrary finite extensions E/K .

Proof. By induction on n , if $E = K(t_1, \dots, t_n)$, let $F = K(t_2, \dots, t_n)$, so $E = F(t_1)$ and $[E : F]_{sep} \mid [E : F]$ by prop. 2.2. By induction hypothesis $[F : K]_{sep} \mid [F : K]$ and we conclude $[E : K]_{sep} = [E : F]_{sep}[F : K]_{sep} \mid [E : F][F : K] = [E : K]$. \square

The quotient of the field degree and its separable degree

$$q = [E : K]_{ins} = [E : K] / [E : K]_{sep}$$

is called its *inseparable degree* and is obviously multiplicative in towers as well.

Proposition 2.4. Let t/K be separable, then $K(t)/K$ is separable.

Proof. We have to show, that any $x \in E = K(t)$ is separable. By assumption and proposition 2.2 we have $[E : K]_{ins} = 1$, hence $[E : K(x)]_{ins}[K(x) : K]_{ins} = 1$, but $[K(x) : K] = [K(x) : K]_{sep}$ by 2.2 means x/K is separable. \square

2.2. Simple extensions.

Proposition 2.5. A finite extension E/K is simple if and only if there are only a finite number of intermediate fields.

Proof. Let $E = K(t)$ be simple and $g = \text{Irr}(t, K)$ its irreducible polynomial. Let $F \subset E$ be an intermediate field and $h = \text{Irr}(t, F) = \sum_i b_i X^i$ the irreducible polynomial of t over F . Define $F' = K(b_1, \dots, b_f) \subset F$. As h is irreducible over F , hence also over F' . As $E = F'(t)$ we have $[E : F] = [E : F']$, therefore $F = F'$ and F is determined by the divisor h of g . As these divisors in $E[X]$ are finite in number, we get only finitely many fields F .

Assume there are only a finite number of fields $F: E \supset F \supset K$. In case K is finite, we already know E is generated by a $q-1$ st root of unity ($q = \text{card } E$). We will assume that K is infinite. Let $s, t \in E$ and $a \in K$ and consider the fields $F_a = K(s + at)$, they are finite in number and we can find $a, b \in K, a \neq b$ with $F_a = F_b$. From $s + at, s + bt \in F_a$ we conclude that their difference $(a-b)t$, hence also $s, t \in F_a$ and $F_a = K(s, t)$. From this we can conclude that any subfield generated by two elements over K can be generated by one element. Hence, by induction, that any finitely generated field, in particular E itself, can be generated by one element. \square

Proposition 2.6. Let E/K be finite, separable, then it is a simple extension.

Proof. Let $E = K(t_1, \dots, t_n)$ and consider $g_i = \text{Irr}(t_i, K)$ and form the product $g = \prod_i g_i$ in $E[X]$. A suitable splitting field of g is normal and separable, hence Galois, and there only finitely many intermediate fields, in particular between E and K . \square

2.3. Characteristic Polynomial. The *characteristic polynomial* of $t \in E^\times$ is by definition

$$\chi(t, E/K) = \det(X - t_{E/K}) \in K[X]$$

where $t_{E/K} \in GL_K(E)$ is the K -linear map

$$\begin{array}{ccc} t_{E/K}: E & \longrightarrow & E \\ x & \longmapsto & t \cdot x \end{array}$$

If $n = [E : K]$ is the degree, then

$$\chi(t, E/K) = X^n - \text{Tr}_{E/K}(t)X^{n-1} + \dots + (-1)^n N_{E/K}(t)$$

Proposition 2.7. Let $g_{t/K} = \text{Irr}(t, K)$ be the irreducible polynomial of t over K (the minimal polynomial), let $d = \deg g$, $e = \frac{n}{d} = [E : K(t)]$. Then we have

$$\chi(t, E/K) = g_{t/K}^e$$

Proof. Let $\alpha_1, \dots, \alpha_e$ be a basis of $E/K(t)$: $E = K(t)\alpha_1 + \dots + K(t)\alpha_e$, then we have $E = K\alpha_1 + Kt\alpha_1 + \dots + Kt^{d-1}\alpha_1 + K\alpha_2 + Kt\alpha_2 + \dots + Kt^{d-1}\alpha_e$ and the matrix of $t_{E/K} : E \rightarrow E$ in this basis splits into e equal boxes of $d \times d$ matrices

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_d \\ 1 & 0 & \dots & 0 & 0 & -a_{d-1} \\ 0 & 1 & \dots & 0 & 0 & -a_{d-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & -a_2 \\ 0 & 0 & \dots & 0 & 1 & -a_1 \end{pmatrix}$$

when $g = X^d + a_1X^{d-1} + \dots + a_d$. Now, the characteristic polynomial of this matrix is exactly g , qed. \square

Corollary 2.8. $\text{Tr}_{E/K}(t) = e \cdot (t_1 + \dots + t_d)$ if $g = (X - t_1) \dots (X - t_d)$.

Corollary 2.9. Let $t \in E$ be inseparable over K , then $\text{Tr}_{E/K}(t) = 0$.

Proof. If t is inseparable, then $g_{t/K} = \text{Irr}(t, K) = X^d + a_1X^{d-1} + \dots + a_d$ has $a_1 = 0$ and therefore $\text{Tr}_{E/K}(t) = -ea_1 = 0$. \square

Theorem 2.10. E/K is separable \iff the trace $\text{Tr}_{E/K} : E \rightarrow K$ is $\neq 0$.

Proof. " \Rightarrow " is a consequence of the linear independance of characters (see A.2 below); " \Leftarrow " is Corollary 2.9. \square

APPENDIX A. INDEPENDANCE OF CHARACTERS

We recall ARTIN's formulation of the independance of characters:

Theorem A.1. Let $\sigma_1, \dots, \sigma_n : G \rightarrow K^\times$ be n different characters from a group G into the multiplicative group of a field K . Then they are linearly independent.

Proof. (See ARTIN [1, II.E, Satz 12] or LANG [2, VI, Th. 4.1]) By induction on n . For $n = 1$ this is clear. Let $n > 1$ and assume the result for less than n characters. Let $a_1\sigma_1 + \dots + a_n\sigma_n = 0$ be a linear dependance. In particular we have for $x \in G$

$$(1) \quad a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0$$

Let $t \in G$ be such that $\sigma_1(t) \neq \sigma_n(t)$ and replace x by tx in the relation (1):

$$(2) \quad a_1\sigma_1(t)\sigma_1(x) + \dots + a_n\sigma_n(t)\sigma_n(x) = 0$$

Now multiply the relation (1) by $\sigma_n(t)$

$$(3) \quad a_1\sigma_n(t)\sigma_1(x) + \dots + a_n\sigma_n(t)\sigma_n(x) = 0$$

and subtract (3) from (2) giving

$$a_1(\sigma_1(t) - \sigma_n(t))\sigma_1(x) + \dots + a_{n-1}(\sigma_{n-1}(t) - \sigma_n(t))\sigma_{n-1}(x) = 0$$

which by induction gives in particular $a_1(\sigma_1(t) - \sigma_n(t)) = 0$, that is $a_1 = 0$. Again, by induction, we conclude $a_2 = \dots = a_n = 0$. \square

Corollary A.2. For a separable extension E/K the trace is not trivial $\text{Tr}_{E/K} \neq 0$.

Corollary A.3. Let $\text{Hom}_K(E, \bar{K}) = \{\sigma_1, \dots, \sigma_d\}$ and assume E/K separable with base $E = K\omega_1 \oplus \dots \oplus K\omega_d$, then $\det \sigma_i(\omega_j) \neq 0$.

Proof. Consider a finite normal extension F/K such that $E \subset F$. The σ_i map E into F and we look at the vector $\omega = (\omega_1, \dots, \omega_d) \in F^d$ and its images $v_i = \sigma_i(\omega)$ for $1 \leq i \leq d$. A relation $\sum_i a_i v_i = 0$ implies $\sum_i a_i \sigma_i = 0$, hence by theorem A.1 the linear independence of the vectors $v_1, \dots, v_d \in F^d$, which is equivalent to the non-vanishing of the determinant. \square

Corollary A.4. *For a separable extension E/K the map*

$$\begin{aligned} E \times E &\longrightarrow K \\ (x, y) &\longmapsto \operatorname{Tr}_{E/K}(xy) \end{aligned}$$

is bilinear and non-degenerate.

Proof. For each $x \in E$ the map $\lambda_x : E \rightarrow K$, $\lambda_x(y) = \operatorname{Tr}_{E/K}(xy)$ defines a map $E \rightarrow E^\vee$, $x \mapsto \lambda_x$ with trivial kernel. Since $\dim_K E = \dim_K E^\vee$ it is an isomorphism, hence the result. \square

REFERENCES

- [1] Emil Artin, *Galoissche Theorie*, Harri Deutsch, Zürich und Frankfurt/Main, 1965.
- [2] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, 2002.