1

Finite Étale Algebras over Fields

We give a brief introduction to *finite étale algebras* over a given field K: these are direct products $L_1 \times \cdots \times L_q$ of finite separable field extensions $L_1, \ldots, L_q$ of K. Such algebras play a central role in this monograph. A convenient reference is Lenstra (2001, chap. 11), where also finite étale algebras over arbitrary commutative rings are discussed. Other suitable references for finite étale algebras over fields are Cohen (2000, §2.1.2) and Bourbaki (1981, chap. 5). For technical convenience, we restrict ourselves to the case that K has characteristic 0.

1.1 Terminology for Rings and Algebras

We agree here on the terminology for rings and algebras to be used throughout this book.

By a *ring* we will always mean a commutative ring with unit element. We denote the zero element and unit element of a ring A by 0_A and 1_A, or just by 0 and 1 if it is clear in which ring we are working. The additive group of a ring A is denoted by A^+, and its unit group (group of multiplicatively invertible elements) by A^*.

A subring of A is always supposed to have the same unit element as A. For a homomorphism of rings $\varphi : A \to B$, we always require that $\varphi(1_A) = 1_B$.

An *integral domain* is a commutative ring with unit element and without divisors of zero. The *quotient field* of an integral domain A consists of the quotients a/b with $a, b \in A$, $b \neq 0$, where two quotients a/b, c/d are identified if $ad = bc$.

A module over a ring A is always assumed to satisfy $1_A m = m$ for every element m of the module.

Let A be a ring and B a commutative, associative A-algebra with unit element, B is a commutative ring whose additive group has an A-module structure. If

$\alpha_1, \ldots, \alpha_r \in B$, we denote by $A[\alpha_1, \ldots, \alpha_r]$ the smallest subring of B containing A and $\alpha_1, \ldots, \alpha_r$. It consists of all polynomial expressions $g(\alpha_1, \ldots, \alpha_r)$ with $g \in A[X_1, \ldots, X_r]$. We say that $\alpha \in B$ is *integral* over A if there is a monic polynomial $f \in A[X]$ with $f(\alpha) = 0$. The elements in B that are integral over A form a subring of B, the *integral closure* of A in B. In case that $A = K$ is a field, we use the term 'algebraic' instead of 'integral' and call the ring of elements of B algebraic over K the *algebraic closure* of K in B.

An integral domain A is said to be *integrally closed* if every element of the quotient field of A that is integral over A in fact belongs to A.

Let K be a field, and Ω a commutative, associative K-algebra with unit element. We define the *degree* of Ω over K, notation $[\Omega : K]$, to be the dimension of Ω as a K-vector space in case this is finite.

Let $\alpha \in \Omega$ be algebraic over K. Then the set of polynomials $g \in K[X]$ with $g(\alpha) = 0$ forms a non-zero ideal of $K[X]$. This ideal is principal. Any generator of this ideal is called a *minimal polynomial* of α over K. The unique monic generator of this ideal is called the *monic minimal polynomial* of α over K, notation f_α. The degree of f_α is called the *degree* of α over K. Since the K-algebra homomorphism $g \mapsto g(\alpha)$ from $K[X]$ to $K[\alpha]$ has kernel (f_α), one has

$$K[\alpha] \cong K[X]/(f_\alpha), \quad [K[\alpha] : K] = \deg f_\alpha. \tag{1.1.1}$$

In particular, if Ω is finite dimensional over K, then every $\alpha \in \Omega$ is algebraic over K and $[K[\alpha] : K] \leq [\Omega : K]$.

1.2 Finite Field Extensions

Let K be a field of characteristic 0. We fix an algebraic closure $\overline{K} \supset K$ of K. We recall that a finite extension L of K is a field extension of K that has finite dimension over K when viewed as a K-vector space. This dimension is then denoted by $[L : K]$ and called the *degree* of L over K.

Let L be a finite extension of K. Then there exists an irreducible monic polynomial $f \in K[X]$ such that $L \cong K[X]/(f)$. If $[L : K] = n$, then there are precisely n distinct injective homomorphisms from L to $\overline{K}$ leaving the elements of K fixed; these are called the *K-isomorphisms* of L into $\overline{K}$. We usually denote these K-isomorphisms by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ and call the images $\alpha^{(1)}, \ldots, \alpha^{(n)}$ of $\alpha \in L$ under these K-isomorphisms the *conjugates* of α over K.

If $M \supset L \supset K$ is a tower of finite extensions, then $[M : K] = [M : L] \cdot [L : K]$, and every K-isomorphism of L into $\overline{K}$ can be extended in precisely $[M : L]$ ways to a K-isomorphism of M into $\overline{K}$.

We introduce the characteristic polynomial, trace, norm and discriminant with respect to a finite field extension L/K. The *characteristic polynomial*, *trace* and *norm* of $\alpha \in L$ relative to the extension L/K are defined by

$$\mathscr{X}_{L/K;\alpha}(X) := \prod_{i=1}^{n}(X - \alpha^{(i)}),$$
$$Tr_{L/K}(\alpha) := \sum_{i=1}^{n}\alpha^{(i)}, \quad N_{L/K}(\alpha) := \prod_{i=1}^{n}\alpha^{(i)},$$

respectively, where again, $n = [L : K]$ and $\alpha^{(1)}, \dots, \alpha^{(n)}$ denote the conjugates (in $\overline{K}$) of α over K. The characteristic polynomial of α over K is a power of the monic minimal polynomial of α over K, therefore its coefficients belong to K. Consequently, for any symmetric polynomial $P \in K[X_1, \dots, X_n]$ we have $P(\alpha^{(1)}, \dots, \alpha^{(n)}) \in K$. So in particular, $Tr_{L/K}(\alpha), N_{L/K}(\alpha)$ belong to K. Notice that $Tr_{L/K}$ is K-linear and $N_{L/K}$ is multiplicative. Further, for $a \in K$ we have $Tr_{L/K}(a) = na, N_{L/K}(a) = a^n$. The trace and norm are transitive with respect to towers of field extensions, that is, if M is a finite extension of L, we have for $\alpha \in M$,

$$Tr_{M/K}(\alpha) = Tr_{L/K}\big(Tr_{M/L}(\alpha)\big), \quad N_{M/K}(\alpha) = N_{L/K}\big(N_{M/L}(\alpha)\big).$$

We mention that the above defined characteristic polynomial of α is equal to the characteristic polynomial of the K-linear map $x \mapsto \alpha x$ from L to L. Thus, $Tr_{L/K}(\alpha)$ is the trace, and $N_{L/K}(\alpha)$ the determinant of this map.

We define the *discriminant* of a tuple $\omega_1, \dots, \omega_n \in L$ by

$$D_{L/K}(\omega_1, \dots, \omega_n) := \det\Big(Tr_{L/K}(\omega_i\omega_j)\Big)_{i,j=1,\dots,n}$$
$$= \Big(\det\Big(\omega_j^{(i)}\Big)_{i,j=1,\dots,n}\Big)^2.$$

This quantity clearly belongs to K. Further, the discriminant is non-zero if and only if $\{\omega_1, \dots, \omega_n\}$ form a K-basis of L.

The *discriminant* of $\alpha \in L$ is defined by

$$D_{L/K}(\alpha) := D_{L/K}(1, \alpha, \dots, \alpha^{n-1}).$$

By Vandermonde's identity, this can be expressed otherwise as

$$D_{L/K}(\alpha) = \prod_{1\le i<j\le n}(\alpha^{(i)} - \alpha^{(j)})^2.$$

This quantity is non-zero if and only if $L = K(\alpha)$.

1.3 Basic Facts on Finite Étale Algebras over Fields

Let for the moment K be any field and take finite field extensions $L_1, \dots, L_q$ of K. The direct (K-algebra) product of $L_1, \dots, L_q$, notation $L_1 \times \cdots \times L_q$, is defined as the set of tuples

$$\big\{(\alpha_1, \dots, \alpha_q) : \alpha_1 \in L_1, \dots, \alpha_q \in L_q\big\},$$

endowed with coordinatewise addition, multiplication and scalar multiplication with elements of K. The zero element and unit element of $L_1 \times \cdots \times L_q$ are $(0, \dots, 0)$ and $(1, \dots, 1)$, respectively, while the unit group of this algebra consists of the tuples $(\alpha_1, \dots, \alpha_q)$ with $\alpha_i \neq 0$ for $i = 1, \dots, q$. The elements $\neq (0, \dots, 0)$ outside the unit group are the zero divisors of the algebra.

Definition A *finite étale K-algebra* is a K-algebra that is isomorphic to a direct product of finitely many finite separable extensions of K. ■

In the remainder of this chapter, K will be a field of characteristic 0. We fix an algebraic closure $\overline{K}$ of K. Let Ω be a finite étale K-algebra, there exist a finite number of finite (automatically separable) extensions $L_1, \dots, L_q$ of K and a K-algebra isomorphism

$$\varphi : \Omega \xrightarrow{\sim} L_1 \times \cdots \times L_q. \tag{1.3.1}$$

We denote by 0_Ω, 1_Ω, the zero element and unit element of Ω. The *degree* $[\Omega : K]$ of Ω over K, the dimension of Ω as a K-vector space, is equal to $[\Omega : K] = \sum_{i=1}^{q} [L_i : K]$.

We can embed K into Ω by means of $a \mapsto a \cdot 1_\Omega$. It will be often convenient to view K as a subalgebra of Ω by identifying $a \in K$ with $a \cdot 1_\Omega$. In that case, the zero element and unit element of Ω are simply the zero element 0 and unit element 1 of K.

If K is a finite extension of some subfield E, then Ω may be viewed as a finite étale E-algebra as well, and

$$[\Omega : E] = [\Omega : K] \cdot [K : E],$$

where $[K : E]$ is the degree of K over E.

Below we give another characterization of finite étale K-algebras. A polynomial $f \in K[X]$ of degree n is called *separable* if over an extension of K it factorizes as $a(X - \alpha_1) \cdots (X - \alpha_n)$ with distinct $\alpha_1, \dots, \alpha_n$. Recall that we are assuming throughout that K is of characteristic 0.

Proposition 1.3.1 *Let Ω be a finite-dimensional K-algebra. Then the following two statements are equivalent:*

(i) Ω *is a finite étale* K*-algebra with* $[\Omega : K] = n$.
(ii) There is a separable polynomial $f \in K[X]$ *of degree* n *such that* $\Omega \cong K[X]/(f)$.

We denote the K-algebra $K[X]/(f)$ by $\Omega(f)$.

Proof (i)⇒(ii). Suppose that $\Omega \cong L_1 \times \cdots \times L_q$, where $L_1, \ldots, L_q$ are finite extensions of K. Since K is of characteristic 0, we can choose distinct irreducible monic polynomials $f_1, \ldots, f_q \in K[X]$ such that $L_i \cong K[X]/(f_i)$ for $i = 1, \ldots, q$. Let $f = f_1 \cdots f_q$. Then f has degree $\sum_{i=1}^{q} \deg f_i = n$, f is separable, and by the Chinese Remainder Theorem for polynomials,

$$\Omega \cong K[X]/(f_1) \times \cdots \times K[X]/(f_q) \cong K[X]/(f).$$

(ii)⇒(i). Suppose that $\Omega \cong K[X]/(f)$ for some separable polynomial $f \in K[X]$ of degree n which we may assume to be monic. Then f can be expressed as a product $f_1 \cdots f_q$ of distinct monic irreducible polynomials in $K[X]$ and then $K[X]/(f)$ is a direct product of $K[X]/(f_i)$ $(i = 1, \ldots, q)$ which are all finite extensions of K. □

Corollary 1.3.2 *Let* Ω *be a finite étale* K*-algebra. Then there is* $\theta \in \Omega$ *such that* $\Omega = K[\theta]$.

Such an element θ is called a *primitive element* of Ω over K.

Proof There is a K-algebra isomorphism $\varphi : \Omega \xrightarrow{\sim} K[X]/(f)$, with $f \in K[X]$ separable. Take for θ the inverse under φ of the residue class of X modulo f. Then $\Omega = K[\theta]$. □

By a *K-homomorphism* from a finite étale K-algebra Ω to an extension field L of K we mean a non-trivial K-algebra homomorphism from Ω to L. Such a K-homomorphism cannot be injective if Ω is not a field.

Proposition 1.3.3 *Let* Ω *be a finite étale* K*-algebra with* $[\Omega : K] = n$. *Then there are precisely* n *distinct* K*-homomorphisms from* Ω *to* $\overline{K}$. *Moreover, an element of* Ω *is uniquely determined by its images under these homomorphisms.*

Proof We give two different constructions that will both be used later.

First choose a monic, separable polynomial $f \in K[X]$ such that $\Omega \cong K[X]/(f)$. Let θ be the inverse image of the residue class of X under this isomorphism so that $\Omega = K[\theta]$ and $f(\theta) = 0$. The polynomial f has n distinct zeros in $\overline{K}$, say $\theta^{(1)}, \ldots, \theta^{(n)}$, and each assignment $\theta \mapsto \theta^{(i)}$ $(i = 1, \ldots, n)$ defines a K-homomorphism from Ω to $\overline{K}$. On the other hand, a K-homomorphism from Ω to $\overline{K}$ necessarily has to map θ to a zero of f in $\overline{K}$, so there are no other K-homomorphisms.

For the other construction, choose finite extensions $L_1, \dots, L_q$ of K and an isomorphism $\varphi : \Omega \xrightarrow{\sim} L_1 \times \cdots \times L_q$. For $i = 1, \dots, q$, there are precisely $n_i := [L_i : K]$ distinct K-isomorphisms L_i into $\overline{K}$, $\sigma_{i,1}, \dots, \sigma_{i,n_i}$ say. For $\alpha \in \Omega$, write $\varphi(\alpha) = (\alpha_1, \dots, \alpha_q)$ where $\alpha_i \in L_i$ for $i = 1, \dots, q$. This gives rise to precisely n distinct K-homomorphisms $\alpha \mapsto \sigma_{ij}(\alpha_i)$ $(i = 1, \dots, q,\ j = 1, \dots, n_i)$ from Ω to $\overline{K}$. The images $\sigma_{ij}(\alpha_i)$ of these homomorphisms determine $\alpha_1, \dots, \alpha_q$, and hence α, uniquely, since for $i = 1, \dots, q$, $j = 1, \dots, n_i$ the map σ_{ij} is injective on L_i. □

Let Ω be a finite étale K-algebra and denote by $x \mapsto x^{(i)}$ $(i = 1, \dots, n)$ the K-homomorphisms of Ω to $\overline{K}$. The images of Ω under these K-homomorphisms are finite extension fields of K. In fact, if Ω is isomorphic to a direct product $L_1 \times \cdots \times L_q$ of finite field extensions of K, these are the conjugates of $L_1, \dots, L_q$ over K. In case that $\Omega \cong K[X]/(f)$ with $f \in K[X]$ separable, the compositum of these extension fields is the splitting field of f over K.

Example Let $f = X(X^2 + X + 1)$ and $\Omega = \mathbb{Q}[X]/(f)$. Then $\Omega = K[\theta]$, where $\theta := X \pmod f$. We have $\Omega \cong \mathbb{Q} \times \mathbb{Q}(\rho)$, where ρ is a primitive cube root of unity, and the three $\mathbb{Q}$-homomorphisms of Ω are given by $\theta \mapsto 0, \theta \mapsto \rho, \theta \mapsto \rho^2$.

Below we use that every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ permutes the K-homomorphisms of Ω, $x \mapsto \sigma(x^{(i)})$ $(i = 1, \dots, n)$ is a permutation of $x \mapsto x^{(i)}$ $(i = 1, \dots, n)$.

Corollary 1.3.4 *Let $f \in K[X]$, and $\alpha \in \Omega$. Then $f(\alpha) = 0 \iff f(\alpha^{(i)}) = 0$ for $i = 1, \dots, n$.*

Proof Apply the last assertion of Proposition 1.3.3 to $f(\alpha)$. □

Corollary 1.3.5 *Let $\alpha \in \Omega$ and let $\alpha^{(i)}$ $(i \in I)$ be the distinct elements among $\alpha^{(1)}, \dots, \alpha^{(n)}$. Then for the monic minimal polynomial of α over K we have $f_\alpha(X) = \prod_{i \in I}(X - \alpha^{(i)})$.*

Proof Let $g(X) := \prod_{i \in I}(X - \alpha^{(i)})$. The elements of $\mathrm{Gal}(\overline{K}/K)$ permute $\alpha^{(i)}$ $(i \in I)$. Hence g is invariant under the action of $\mathrm{Gal}(\overline{K}/K)$ and so it belongs to $K[X]$. Now apply Corollary 1.3.4. □

Corollary 1.3.6 *Suppose $[\Omega : K] = n$. Let $f \in K[X]$ be a non-zero polynomial of degree m. Then f has at most m^n zeros in Ω.*

Proof Let $\beta_1, \dots, \beta_r$ be the distinct zeros of f in $\overline{K}$. Let β be any zero of f in Ω. Then by Corollary 1.3.4 we have $\beta^{(i)} \in \{\beta_1, \dots, \beta_r\}$ for $i = 1, \dots, n$. So for the tuple $(\beta^{(1)}, \dots, \beta^{(n)})$, hence for β, there are at most $r^n \le m^n$ possibilities. □

The upper bound m^n in the above lemma is best possible. For instance, let $\Omega = K \times \cdots \times K$ (n-fold direct product) and $f = (X - a_1) \cdots (X - a_m)$, where $a_1, \ldots, a_m$ are distinct elements of K. Then all $(b_1, \ldots, b_n)$ with $b_i \in \{a_1, \ldots, a_m\}$ for $i = 1, \ldots, n$ give zeros of f in Ω.

1.4 Resultants and Discriminants of Polynomials

In this section we recall the basic properties of the resultant of two polynomials and the discriminant of a polynomial. In the next section, we introduce the discriminant of a basis of an étale algebra and show how the discriminant of a polynomial can be interpreted as such.

Let K be a field and

$$f = a_0 X^n + \cdots + a_n, \quad g = b_0 X^m + \cdots + b_m \in K[X]$$

two polynomials of degrees $n > 0$, $m > 0$, respectively. We define the *resultant* of f and g to be the determinant of order $m + n$ given by

$$R(f, g) = \begin{vmatrix} a_0 & \cdots & a_n & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_n \\ b_0 & \cdots & b_m & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_m \end{vmatrix}, \tag{1.4.1}$$

where the first $m = \deg g$ rows consist of the coefficients of f, and the last $n = \deg f$ rows of the coefficients of g. In case that one of f, g (but not both) has degree 0, we can still use the above determinant to define $R(f, g)$: if $f = a_0$ is constant we obtain $R(f, g) = a_0^m$, while if $g = b_0$ we obtain $R(f, g) = b_0^n$. If both f, g are constant, we define $R(f, g) := 1$.

We recall some properties of the resultant. Assume again that f and g have degrees $n > 0$, $m > 0$, respectively. Then

$$R(f, g) = 0 \iff f, g \text{ have a common zero in } \overline{K}, \tag{1.4.2}$$

where $\overline{K}$ denotes an algebraic closure of K. Indeed, by straightforward linear algebra, $R(f, g) = 0$ if and only if there exist polynomials $u, v \in K[X]$ of degrees at most $m - 1$, $n - 1$, respectively, not both 0, such that $uf + vg = 0$, and the latter holds if and only if f, g have a root in common. Writing

$$f = a_0(X - \theta_1) \cdots (X - \theta_n), \quad g = b_0(X - \rho_1) \cdots (X - \rho_m)$$

with $\theta_1, \dots, \theta_n, \rho_1, \dots, \rho_m \in \overline{K}$, one deduces easily that

$$\begin{aligned} R(f,g) &= a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\theta_i - \rho_j) \\ &= a_0^m g(\theta_1) \cdots g(\theta_n) \\ &= (-1)^{mn} b_0^n f(\rho_1) \cdots f(\rho_m). \end{aligned} \tag{1.4.3}$$

We define the *discriminant* of a linear polynomial to be equal to 1, and the discriminant of a polynomial

$$f = a_0 X^n + \cdots + a_n = a_0 (X - \theta_1) \cdots (X - \theta_n) \in K[X]$$

of degree $n \geq 2$ (where $\theta_1, \dots, \theta_n \in \overline{K}$ and $a_0 \neq 0$) to be

$$D(f) := a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2. \tag{1.4.4}$$

Notice that $D(f) = 0$ if and only if f has a zero in $\overline{K}$ of multiplicity at least 2. Denoting by f', the derivative of f, we have

$$\begin{aligned} R(f,f') &= a_0^{n-1} f'(\theta_1) \cdots f'(\theta_n) \\ &= a_0^{2n-1} \prod_{i=1}^{n} \prod_{j=1,\, j \neq i}^{n} (\theta_i - \theta_j) = (-1)^{n(n-1)/2} a_0 D(f), \end{aligned}$$

hence $D(f) = (-1)^{n(n-1)/2} a_0^{-1} R(f,f')$. We obtain an expression for $R(f,f')$ as a determinant of order $2n-1$ by substituting f' for g in (1.4.1). By subtracting in this determinant n times the first row from the n-th row, and then developing with respect to the first column, we obtain

$$D(f) = (-1)^{1+n(n-1)/2} \Delta, \tag{1.4.5}$$

where Δ is the determinant of order $2n-2$ given by

$$\begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_n & & \\ & \ddots & & & & \ddots & \\ & & a_0 & a_1 & \cdots & \cdots & a_n \\ a_1 & 2a_2 & \cdots & na_n & & & \\ na_0 & (n-1)a_1 & \cdots & a_{n-1} & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & na_0 & (n-1)a_1 & \cdots & a_{n-1} \end{vmatrix},$$

with on the first $n-2$ rows $a_0, \dots, a_n$, on the $(n-1)$-th row $a_1, 2a_2, \dots, na_n$, and on the last $n-1$ rows $na_0, \dots, a_{n-1}$. This shows that $D(f)$ is a homogeneous polynomial of degree $2n-2$ in $\mathbb{Z}[a_0, \dots, a_n]$.

Now suppose that $f = f_1 \cdots f_r$, where $f_1, \dots, f_r$ are non-constant polynomials in $K[X]$. Then one deduces easily from (1.4.3) and (1.4.4) that

$$D(f) = \prod_{i=1}^{r} D(f_i) \cdot \prod_{1 \le i < j \le r} R(f_i, f_j)^2. \tag{1.4.6}$$

1.5 Characteristic Polynomial, Trace, Norm, Discriminant

We generalize the notions of characteristic polynomial, trace, norm and discriminant defined above from finite field extensions to finite étale K-algebras by taking K-homomorphisms instead of K-isomorphisms. Let Ω be a finite étale K-algebra. We view K as a K-subalgebra of Ω. Suppose that $[\Omega : K] = n$. Let $x \mapsto x^{(i)}$ $(i = 1, \dots, n)$ denote the K-homomorphisms from Ω to $\overline{K}$. Further, let $\varphi, L_1, \dots, L_q$ be as in (1.3.1).

Take $\alpha \in \Omega$. We define the *characteristic polynomial* of α over K by

$$\mathscr{X}_{\Omega/K;\alpha}(X) := \prod_{i=1}^{n} (X - \alpha^{(i)}).$$

Since $\mathrm{Gal}(\overline{K}/K)$ permutes $\alpha^{(1)}, \dots, \alpha^{(n)}$, the polynomial $\mathscr{X}_{\Omega/K;\alpha}$ is invariant under the action of $\mathrm{Gal}(\overline{K}/K)$ and so it belongs to $K[X]$. By Corollary 1.3.4, this implies $\mathscr{X}_{\Omega/K;\alpha}(\alpha) = 0$.

Let $\varphi(\alpha) = (\alpha_1, \dots, \alpha_q)$ with $\alpha_i \in L_i$ for $i = 1, \dots, q$. From the second construction in the proof of Theorem 1.3.3, we infer at once that

$$\mathscr{X}_{\Omega/K;\alpha}(X) = \prod_{j=1}^{q} \mathscr{X}_{L_j/K;\alpha_j}(X). \tag{1.5.1}$$

The *trace* and *norm* of α over K are defined by

$$Tr_{\Omega/K}(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}, \quad N_{\Omega/K}(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)}.$$

Completely analogously to the case of field extensions, the above defined characteristic polynomial of α is equal to the characteristic polynomial of the K-linear map $x \mapsto \alpha x$ from Ω to Ω, and $Tr_{\Omega/K}(\alpha)$, $N_{\Omega/K}(\alpha)$ are the trace and determinant of this map, respectively.

Both the trace and norm of α belong to K, and from the definitions of trace and norm it follows at once that

$$Tr_{\Omega/K}(a\alpha + b\beta) = aTr_{\Omega/K}(\alpha) + bTr_{\Omega/K}(\beta),$$
$$N_{\Omega/K}(\alpha\beta) = N_{\Omega/K}(\alpha)N_{\Omega/K}(\beta)$$

for $a, b \in K$, $\alpha, \beta \in \Omega$, and moreover that

$$Tr_{\Omega/K}(a) = na, \quad N_{\Omega/K}(a) = a^n \quad \text{for } a \in K\,.$$

Further, if $\varphi(\alpha) = (\alpha_1, \ldots, \alpha_q)$ with $\alpha_i \in L_i$ for $i = 1, \ldots, q$, we have

$$Tr_{\Omega/K}(\alpha) = \sum_{j=1}^{q} Tr_{L_j/K}(\alpha_j), \quad N_{\Omega/K}(\alpha) = \prod_{j=1}^{q} N_{L_j/K}(\alpha_j). \tag{1.5.2}$$

Again completely similarly as for field extensions, we define the *discriminant* over K of a tuple $(\omega_1, \ldots, \omega_n)$ in Ω (where as before $n := [\Omega : K]$) by

$$D_{\Omega/K}(\omega_1, \ldots, \omega_n) = \det\left(Tr_{\Omega/K}(\omega_i\omega_j)_{i,j=1,\ldots,n}\right)$$
$$= \left(\det\left(\omega_j^{(i)}\right)_{i,j=1,\ldots,n}\right)^2.$$

Assume that $\{\omega_1, \ldots, \omega_n\}$ is a K-basis of Ω, and let $\theta_1, \ldots, \theta_n \in \Omega$. Then $\theta_i = \sum_{j=1}^{n} a_{ij}\omega_j$ with $a_{ij} \in K$ for $i, j = 1, \ldots, n$. We call $M := (a_{ij})_{i,j=1,\ldots,n}$ the *coefficient matrix of* $\theta_1, \ldots, \theta_n$ *with respect to* $\omega_1, \ldots, \omega_n$. Then we have the *basis transformation formula for discriminants*,

$$D_{\Omega/K}(\theta_1, \ldots, \theta_n) = (\det M)^2 \cdot D_{\Omega/K}(\omega_1, \ldots, \omega_n)\,. \tag{1.5.3}$$

Now let $\omega_{i,1}, \ldots, \omega_{i,n_i} \in L_i$ for $i = 1, \ldots, q$, and let $\omega_1, \ldots, \omega_n \in \Omega$ be the elements

$$\varphi^{-1}\left((0, \ldots, \omega_{ij}, \ldots, 0)\right) \quad (i = 1, \ldots, q,\ j = 1, \ldots, n_i) \tag{1.5.4}$$

in some order, with ω_{ij} on the i-th place, and 0 on the other places. Then

$$D_{\Omega/K}(\omega_1, \ldots, \omega_n) = \prod_{i=1}^{q} D_{L_i/K}\left(\omega_{i,1}, \ldots, \omega_{i,n_i}\right). \tag{1.5.5}$$

The *discriminant* of $\alpha \in \Omega$ over K is defined by

$$D_{\Omega/K}(\alpha) := D_{\Omega/K}\left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right). \tag{1.5.6}$$

Then by Vandermonde's identity,

$$D_{\Omega/K}(\alpha) = \prod_{1 \le i < j \le n} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2. \tag{1.5.7}$$