

§57 Norm and Trace

In this paragraph, we introduce norm and trace of elements in an extension field. These can be defined for any finite dimensional extension, but we restrict ourselves to the important case where the extension is separable.

In order to define norm and trace, we need K -homomorphisms of an extension field of K . In the case of a separable extension, these are easy to describe.

Let K be a field and E a finite dimensional separable extension of K and N a normal closure of E over K so that N is finite dimensional and Galois over K (Theorem 55.11). Let us put $|E:K| = n$. Since E is finite dimensional and hence finitely generated (Theorem 50.10) over K , there is an $a \in E$ such that $E = K(a)$ (Theorem 55.14). Let $f(x) \in K[x]$ be the (separable) minimal polynomial of a over K , so that $\deg f(x) = |K(a):K| = |E:K| = n$ (Theorem 50.7). Since N is normal over K and $f(x)$ has a root a in N , the polynomial $f(x)$ splits in N , say

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n), \quad a_1 = a, \quad a_1, a_2, \dots, a_n \in N$$

and a_1, a_2, \dots, a_n are pairwise distinct. Then $K(a)$ and $K(a_i) \subseteq N$ are K -isomorphic by Theorem 53.2, namely by the K -isomorphism

$$\begin{array}{ccc} N & & N \\ \cup & & \cup \\ \psi_i: E = K(a) = K[a] & \longrightarrow & K[a_i] = K(a_i) \\ k_0 + k_1 a + \cdots + k_{n-2} a^{n-2} + k_{n-1} a^{n-1} & \longrightarrow & k_0 + k_1 a_i + \cdots + k_{n-2} a_i^{n-2} + k_{n-1} a_i^{n-1}, \end{array}$$

where $k_0, k_1, \dots, k_{n-2}, k_{n-1} \in K$. Thus each ψ_i is a K -homomorphism from E into N . Conversely, any K -homomorphism $\psi: E \rightarrow N$ must map a to one of a_1, a_2, \dots, a_n and must coincide with one of $\psi_1, \psi_2, \dots, \psi_n$. So $\{\psi_1, \psi_2, \dots, \psi_n\}$ is the complete set of K -homomorphisms from E into N .

We give a generalization of this result.

57.1 Lemma: Let K be a field and E a finite dimensional separable extension of K . Let L be an intermediate field of E/K and let N be a normal closure of K over E . If $\varphi: L \rightarrow N$ is a K -homomorphism, then φ can be extended in exactly $|E:L|$ ways to a K -homomorphism $E \rightarrow N$.

$$\left. \begin{array}{l} N \\ E \\ L \\ K \end{array} \right| \begin{array}{l} \\ \psi_i: a \rightarrow a_i, l \rightarrow l\varphi \quad (i = 1, 2, \dots, m; l \in L) \\ \varphi \\ \end{array}$$

Proof: Since E is finitely generated and separable over K , it is a simple extension of K , say $E = K(a)$ (Theorem 55.14). Let $|E:L| = m$ and $g(x) \in L[x]$ the minimal polynomial of a over L so that $\deg g(x) = m$. Let $f(x)$ be the minimal polynomial of a over K . Then $f(x)$ splits in N because the irreducible polynomial $f(x) \in K[x]$ has a root in N and N is normal over K . Since $g(x)$ divides $f(x)$ (in $L[x]$; Lemma 50.5), the roots of $g(x)$ are all in N . Let $a = a_1, a_2, \dots, a_m \in N$ be the roots of $g(x)$. Then any extension $\psi: E \rightarrow N$ (ψ a K -homomorphism) of φ must send a to one of a_1, a_2, \dots, a_m and any l in L to $l\varphi$, and thus must coincide with one of the mappings

$$\begin{aligned} \psi_i: E = L(a) = L[a] &\longrightarrow L[a_i] = L(a_i) \subseteq N \\ l_0 + l_1 a + \dots + l_{m-2} a^{m-2} + l_{m-1} a^{m-1} &\rightarrow (l_0 \varphi) + (l_1 \varphi) a_i + \dots + (l_{m-2} \varphi) a_i^{m-2} + (l_{m-1} \varphi) a_i^{m-1} \end{aligned}$$

$(l_0, l_1, \dots, l_{m-2}, l_{m-1} \in L)$, where $i = 1, 2, \dots, m$; and these mappings ψ_i are indeed extensions of φ (since $\psi_i: l_0 \rightarrow l_0 \varphi$) and field homomorphisms (cf. Lemma 53.1, Theorem 53.2). Thus $\{\psi_1, \psi_2, \dots, \psi_m\}$ is the complete set of K -homomorphisms from E into N which are extensions of φ . \square

We can now give the definition of norm and trace.

57.2 Definition: Let K be a field and E a finite dimensional separable extension of K . Let $a \in E$. Choose a normal closure N of K over E and let $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ be the set of all K -homomorphisms from E into N (so $k = |E:K|$). The *norm of $a \in E$ over K* is denoted by $N_{E/K}(a)$ and is defined as

$$N_{E/K}(a) = (a\varphi_1)(a\varphi_2)\dots(a\varphi_k).$$

The trace of $a \in E$ over K is denoted by $T_{E/K}(a)$ and is defined as

$$T_{E/K}(a) = a\varphi_1 + a\varphi_2 + \dots + a\varphi_k.$$

$N_{E/K}(a)$ and $T_{E/K}(a)$ therefore depend on E, K as well as a . It seems as though $N_{E/K}(a)$ and $T_{E/K}(a)$ depended also on the normal closure N we choose, but they actually do not depend on N . This will be proved shortly (Lemma 57.4(3)).

In case E is Galois over K , the normal closure N is equal to E and then we have

$$N_{E/K}(a) = (a\varphi_1)(a\varphi_2)\dots(a\varphi_k), \quad T_{E/K}(a) = a\varphi_1 + a\varphi_2 + \dots + a\varphi_k,$$

where $\{\varphi_1, \varphi_2, \dots, \varphi_k\} = \text{Aut}_K E$.

57.3 Examples: (a) Consider the extension \mathbb{C} over \mathbb{R} . Now \mathbb{C} is Galois over \mathbb{R} and $\text{Aut}_{\mathbb{R}} \mathbb{C} = \{\iota, \varphi\}$, where φ is the conjugation mapping. Thus $N_{\mathbb{C}/\mathbb{R}}(a + bi) = (a + bi)(a + bi)\varphi = (a + bi)(a - bi) = a^2 + b^2$ and $T_{\mathbb{C}/\mathbb{R}}(a + bi) = (a + bi) + ((a + bi)\varphi) = (a + bi) + (a - bi) = 2a$ for any $a + bi \in \mathbb{C}$ ($a, b \in \mathbb{R}$).

(b) $\mathbb{Q}(\sqrt{2})$ is a Galois extension of \mathbb{Q} and $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \{\iota, \varphi\}$, where φ is the homomorphism $\sqrt{2} \rightarrow -\sqrt{2}$. Thus $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a + b\sqrt{2}) = (a + b\sqrt{2})(a + b\sqrt{2})\varphi = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ and $T_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a + b\sqrt{2})\varphi = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a$ for any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ($a, b \in \mathbb{Q}$).

(c) $\mathbb{Q}(\sqrt[3]{2})$ is a separable extension of \mathbb{Q} , but not Galois over \mathbb{Q} . A normal closure of \mathbb{Q} over $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$. There are exactly three \mathbb{Q} -homomorphisms from $\mathbb{Q}(\sqrt[3]{2})$ into $\mathbb{Q}(\sqrt[3]{2}, \omega)$, namely $\sqrt[3]{2} \rightarrow \sqrt[3]{2}$ (the identity), $\sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega$ and $\sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega^2$. So $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$

$$\begin{aligned} &= (a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)(a + b\sqrt[3]{2}\omega + c(\sqrt[3]{2})^2\omega^2)(a + b\sqrt[3]{2}\omega^2 + c(\sqrt[3]{2})^2\omega) \\ &= \dots = a^3 + 2b^3 + 4c^3 - 2abc \end{aligned}$$

and $T_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$

$$= (a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) + (a + b\sqrt[3]{2}\omega + c(\sqrt[3]{2})^2\omega^2) + (a + b\sqrt[3]{2}\omega^2 + c(\sqrt[3]{2})^2\omega)$$

$$= 3a$$

for any $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$ ($a, b, c \in \mathbb{Q}$).

In these examples, norm and trace are found to be in the base field. This is always true. In fact, the norm and trace of an element are essentially coefficients of the minimal polynomial of that element. In particular, they are independent of the normal closure that we use in their definition. We now prove these assertions.

57.4 Lemma: *Let K be a field and E a finite dimensional separable extension of K . Let a, b be arbitrary elements of E .*

$$(1) N_{E/K}(ab) = N_{E/K}(a)N_{E/K}(b) \text{ and } T_{E/K}(a + b) = T_{E/K}(a) + T_{E/K}(b).$$

$$(2) \text{ If } b \in K, \text{ then } N_{E/K}(b) = b^{|E:K|} \text{ and } T_{E/K}(b) = |E:K|b.$$

(3) *If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$ is the minimal polynomial of b over K , then*

$$N_{E/K}(b) = ((-1)^n a_0)^{|E:K(b)|} \text{ and } T_{E/K}(b) = |E:K(b)|(-a_{n-1}).$$

Proof: Let N be a normal closure of K over E and let $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ be the set of all K -homomorphisms from E into N . In view of the comments above, their number k is the number of roots of the minimal polynomial of a primitive element of the extension E/K , hence $k = |E:K|$ (or use Lemma 57.1 with $L = K$).

$$\begin{aligned} (1) \text{ Clearly } N_{E/K}(ab) &= (ab\varphi_1)(ab\varphi_2)\cdots(ab\varphi_k) \\ &= (a\varphi_1 b\varphi_1)(a\varphi_2 b\varphi_2)\cdots(a\varphi_k b\varphi_k) \\ &= (a\varphi_1)(b\varphi_1)(a\varphi_2)(b\varphi_2)\cdots(a\varphi_k)(b\varphi_k) \\ &= (a\varphi_1)(a\varphi_2)\cdots(a\varphi_k)(b\varphi_1)(b\varphi_2)\cdots(b\varphi_k) \\ &= N_{E/K}(a)N_{E/K}(b) \end{aligned}$$

$$\begin{aligned} \text{and } T_{E/K}(a + b) &= (a + b)\varphi_1 + (a + b)\varphi_2 + \cdots + (a + b)\varphi_k \\ &= (a\varphi_1 + b\varphi_1) + (a\varphi_2 + b\varphi_2) + \cdots + (a\varphi_k + b\varphi_k) \\ &= a\varphi_1 + b\varphi_1 + a\varphi_2 + b\varphi_2 + \cdots + a\varphi_k + b\varphi_k \\ &= (a\varphi_1 + a\varphi_2 + \cdots + a\varphi_k) + (b\varphi_1 + b\varphi_2 + \cdots + b\varphi_k) \\ &= T_{E/K}(a) + T_{E/K}(b). \end{aligned}$$

(2) If $b \in K$, then $b\varphi_i = b$ for all $i = 1, 2, \dots, k$ and

$$N_{E/K}(b) = (b\varphi_1)(b\varphi_2)\dots(b\varphi_k) = bb\dots b = b^k$$

$$T_{E/K}(b) = b\varphi_1 + b\varphi_2 + \dots + b\varphi_k = b + b + \dots + b = kb.$$

(3) Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in K[x]$ be the minimal polynomial of b over K and let $b = b_1, b_2, \dots, b_n$ be the roots of $f(x)$ in N . Then $n = |K(b):K|$ and $f(x) = (x - b_1)(x - b_2)\dots(x - b_n)$. Thus

$$b_1 + b_2 + \dots + b_n = -a_{n-1} \text{ and } b_1b_2\dots b_n = (-1)^na_0.$$

Let us write $|E:K(b)| = s$ so that $k = sn$. There are exactly n K -homomorphisms $\alpha_1, \alpha_2, \dots, \alpha_n$ from $K(b)$ into N (namely $\alpha_i: b \rightarrow b_i$). The restriction to $K(b)$ of any φ_j ($j = 1, 2, \dots, k$) is one of these $\alpha_1, \alpha_2, \dots, \alpha_n$, and each α_i ($i = 1, 2, \dots, n$) can be extended to precisely s K -homomorphisms from E into N (Lemma 57.1). Let these extensions of α_i be $\alpha_i^{(1)}, \alpha_i^{(2)}, \dots, \alpha_i^{(s)}$. In this way, we obtain ns K -homomorphisms $\alpha_i^{(m)}: E \rightarrow N$ ($i = 1, 2, \dots, n; m = 1, 2, \dots, s$). Since $ns = k$, we get

$$\{\varphi_1, \varphi_2, \dots, \varphi_k\} = \{\alpha_i^{(m)}: i = 1, 2, \dots, n \text{ and } m = 1, 2, \dots, s\}.$$

Thus

$$\begin{aligned} N_{E/K}(b) &= (b\varphi_1)(b\varphi_2)\dots(b\varphi_k) = \prod_{i=1}^n \prod_{m=1}^s b\alpha_i^{(m)} = \prod_{i=1}^n (b\alpha_i)^s \\ &= \prod_{i=1}^n (b_i)^s = \left(\prod_{i=1}^n b_i\right)^s = ((-1)^na_0)^s \end{aligned}$$

$$\begin{aligned} \text{and } T_{E/K}(b) &= b\varphi_1 + b\varphi_2 + \dots + b\varphi_k = \sum_{i=1}^n \sum_{m=1}^s b\alpha_i^{(m)} = \sum_{i=1}^n s(b\alpha_i) \\ &= s \sum_{i=1}^n b_i = s(-a_{n-1}). \end{aligned} \quad \square$$

We have already mentioned that $N_{E/K}(a)$ and $T_{E/K}(a)$ depend on the fields E and K . It is clear from the definition or from Lemma 57.4(3) that $N_{E/K}(a)$ and $T_{E/K}(a)$ will be distinct from $N_{L/K}(a)$ and $T_{L/K}(a)$ and also from $N_{E/L}(a)$ and $T_{E/L}(a)$ if L is an intermediate field (with $a \in L$ in the first case).

Norm and trace behave very reasonably through intermediate fields: we have $N_{E/K} = N_{L/K} \circ N_{E/L}$ and $T_{E/K} = T_{L/K} \circ T_{E/L}$ for any intermediate field L of E/K . This is the content of the next theorem. Although we know the structure of extensions of homomorphisms in the separable case, we

give a new argument that works in more general situations.

57.5 Lemma: *Let K be a field and E a finite dimensional separable extension of K . Let a be an arbitrary element of E . Then*

$$N_{E/K}(a) = N_{L/K}(N_{E/L}(a)) \text{ and } T_{E/K}(a) = T_{L/K}(T_{E/L}(a)).$$

Proof: (The assertion is meaningful, for $N_{E/L}(a)$ is an element of L by Lemma 57.4(3), thus we can take the norm of $N_{E/L}(a) \in L$ over K . The claim is that this is equal to the norm of $a \in E$ over K . Similarly for the trace.)

$$\begin{array}{ccc} & E & \\ & \downarrow N_{E/L} & \\ N_{E/K} & L & \\ & \downarrow N_{L/K} & \\ & K & \end{array}$$

The proof has been foreshadowed in Lemma 57.4. Let N be a normal closure of E over K . Then N is Galois over K by Theorem 55.11 and N is Galois over L by Theorem 54.25(1). We choose a field M such that

(i) $E \subseteq M \subseteq N$; (ii) M is Galois over L ; (iii) A is not Galois over L for any field A with $E \subseteq A \subset M$. This is possible because N/K is Galois, N/E is also Galois and so N/E is separable (Theorem 55.10) and there are only finitely many intermediate fields of N/E (Theorem 55.15). M is a normal closure of L over E . Likewise, we choose a field R such that (i) $L \subseteq R \subseteq N$; (ii) R is Galois over K ; (iii) A is not Galois over L for any field A with $L \subseteq A \subset R$. Thus R is a normal closure of K over L .

We put $|E:K| = k$, $|E:L| = s$ and $|L:K| = n$ so that $k = sn$. Let

$\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ be the set of all K -homomorphisms from E into N ,
 $\{\beta_1, \beta_2, \dots, \beta_s\}$ the set of all L -homomorphisms from E into $M \subseteq N$ and
 $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ the set of all K -homomorphisms from L into $R \subseteq N$.

Then

$$\begin{aligned} N_{E/K}(a) &= (a\varphi_1)(a\varphi_2)\dots(a\varphi_k), \\ N_{E/L}(a) &= (a\beta_1)(a\beta_2)\dots(a\beta_s), \\ N_{L/K}(b) &= (b\alpha_1)(b\alpha_2)\dots(b\alpha_n) \end{aligned}$$

for any $a \in E$, $b \in L$.

N is a splitting field of a polynomial $f(x) \in K[x]$ over K (Theorem 55.11 and Theorem 55.7) and therefore N is a splitting field of $f(x)$ over L and over $L\alpha_i$ (Example 53.5(e)). The isomorphism $\alpha_i: L \rightarrow L\alpha_i (\subseteq N)$ can be extended to an isomorphism $\alpha_i^{(1)}: N \rightarrow N$ (Theorem 53.7). Here of course $\alpha_i^{(1)}: N \rightarrow N$ is a K -homomorphism.

We claim $\{\varphi_1, \varphi_2, \dots, \varphi_k\} = \{\beta_j \alpha_i^{(1)}: i = 1, 2, \dots, n; j = 1, 2, \dots, s\}$. Since $k = ns$, we must merely show that $\beta_j \alpha_i^{(1)} \neq \beta_{j'} \alpha_{i'}^{(1)}$ when $(i, j) \neq (i', j')$. Indeed, if $\beta_j \alpha_i^{(1)}|_L = \beta_{j'} \alpha_{i'}^{(1)}|_L$, then the restriction of $\beta_j \alpha_i^{(1)}$ and $\beta_{j'} \alpha_{i'}^{(1)}$ to L must be equal and since β_j and $\beta_{j'}$ fix each element in L , we get $\alpha_i^{(1)}|_L = \alpha_{i'}^{(1)}|_L$, so $\alpha_i = \alpha_{i'}$ and $i' = i$. Then, as $\alpha_i^{(1)}$ is one-to-one, $i' = i$ and $\beta_j \alpha_i^{(1)} = \beta_{j'} \alpha_i^{(1)}$ imply that $\beta_{j'} = \beta_j$ and $j' = j$. This establishes the claim.

Thus, since $N_{E/L}(a) \in L$ by Lemma 57.5(3), we get

$$\begin{aligned} N_{E/K}(a) &= (a\varphi_1)(a\varphi_2)\dots(a\varphi_k) = \prod_{i=1}^n \prod_{j=1}^s a\beta_j \alpha_i^{(1)} \\ &= \prod_{i=1}^n \left(\prod_{j=1}^s a\beta_j \right) \alpha_i^{(1)} = \prod_{i=1}^n (N_{E/L}(a)) \alpha_i^{(1)} = \prod_{i=1}^n (N_{E/L}(a)) \alpha_i \\ &= N_{L/K}(N_{E/L}(a)) \end{aligned}$$

and similarly $T_{E/K}(a) = T_{L/K}(T_{E/L}(a))$. □

57.6 Definition: Let E be a field and let $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ be a finite set of field automorphisms of E . If, for any $a_1, a_2, \dots, a_k \in E$,

$$a_1(b\varphi_1) + a_2(b\varphi_2) + \dots + a_k(b\varphi_k) = 0 \text{ for all } b \in E$$

implies $a_1 = a_2 = \dots = a_k = 0$, then $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is said to be *linearly independent*.

Equivalently, $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is linearly independent provided, for each k -tuple (a_1, a_2, \dots, a_k) of elements from E , where at least one a_i is distinct from 0, there is a $b \in E$ such that

$$a_1(b\varphi_1) + a_2(b\varphi_2) + \dots + a_k(b\varphi_k) \neq 0.$$

57.7 Lemma: Let E be a field and let $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ be a finite set of field automorphisms of E . If $\varphi_1, \varphi_2, \dots, \varphi_k$ are pairwise distinct, then $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is linearly independent.

Proof: (cf. Lemma 54.15; note that we do not assume $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is a group.) Suppose, by way of contradiction, $\varphi_1, \varphi_2, \dots, \varphi_k$ are distinct automorphisms of E and that $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is not linearly independent. Then there are elements a_1, a_2, \dots, a_k , not all zero, in E such that

$$a_1(b\varphi_1) + a_2(b\varphi_2) + \dots + a_k(b\varphi_k) = 0 \quad \text{for all } b \in E. \quad (1)$$

Let r be the smallest number of nonzero components a_i in all the k -tuples $(a_1, a_2, \dots, a_k) \in E \times E \times \dots \times E \setminus \{(0, 0, \dots, 0)\}$ satisfying (1) and choose a k -tuple (c_1, c_2, \dots, c_k) with exactly r nonzero components. We have $r > 1$. Renumbering the automorphisms, we may assume c_1, \dots, c_r are distinct from zero and (in case $r < k$) $c_{r+1} = \dots = c_k = 0$.

Then
$$c_1(b\varphi_1) + c_2(b\varphi_2) + \dots + c_r(b\varphi_r) = 0 \quad \text{for all } b \in E. \quad (2)$$

Since $\varphi_1, \varphi_2, \dots, \varphi_k$ are distinct, $\varphi_1 \neq \varphi_2$ and there is a $u \in E$ with $u\varphi_1 \neq u\varphi_2$. Writing ub in place of b in (2) and using $(ub)\varphi_i = u\varphi_i \cdot u\varphi_i$, we get

$$c_1(u\varphi_1)(b\varphi_1) + c_2(u\varphi_2)(b\varphi_2) + \dots + c_r(u\varphi_r)(b\varphi_r) = 0 \quad \text{for all } b \in E. \quad (3)$$

Multiplying (2) by $u\varphi_1$, we obtain

$$c_1(u\varphi_1)(b\varphi_1) + c_2(u\varphi_1)(b\varphi_2) + \dots + c_r(u\varphi_1)(b\varphi_r) = 0 \quad \text{for all } b \in E. \quad (4)$$

Subtraction gives

$$[c_2(u\varphi_2 - u\varphi_1)](b\varphi_2) + \dots + [c_r(u\varphi_r - u\varphi_1)](b\varphi_r) = 0 \quad \text{for all } b \in E.$$

where at least $c_2(u\varphi_2 - u\varphi_1) \neq 0$. Hence there is a k -tuple

$$(0, c_2(u\varphi_2 - u\varphi_1), \dots, c_r(u\varphi_r - u\varphi_1), 0, \dots, 0) \neq (0, 0, \dots, 0)$$

with at most $r - 1$ nonzero components satisfying (1), contrary to the definition of r . Therefore $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ is linearly independent. \square

We now characterize all elements with trace 0 and all elements with norm 1 in case of a Galois extension with a finite cyclic group. The second part of Theorem 57.9 (formulated for finite dimensional extension of \mathbb{Q}) is the theorem with number 90 in D. Hilbert's (1862-1943) famous report on algebraic number theory and is known as "Hilbert's theorem 90". It is the beginning of cohomology theory.

57.8 Definition: Let E/K be a field extension. If E is algebraic and Galois over K , and if the Galois group $\text{Aut}_K E$ is cyclic, then E is called a *cyclic extension of K* and E/K is said to be *cyclic*.

57.9 Theorem: Let E/K be a finite dimensional cyclic extension and let σ be a generator of $\text{Aut}_K E$. Let $a \in E$.

- (1) $T_{E/K}(a) = 0$ if and only if there is an element $b \in E$ with $a = b - b\sigma$.
- (2) $N_{E/K}(a) = 1$ if and only if there is an element $b \in E \setminus \{0\}$ with $a = b / b\sigma$.

Proof: Let $|E:K| = n$. Then $|\text{Aut}_K E| = n$ by the fundamental theorem of Galois theory and $\text{Aut}_K E = \{1, \sigma, \sigma^2, \dots, \sigma^{n-2}, \sigma^{n-1}\}$, with $\sigma^n = 1$ and $o(\sigma) = n$. For convenience, we write T instead of $T_{E/K}$ and N instead of $N_{E/K}$.

(1) If $a = b - b\sigma$, then we have a telescoping sum:

$$\begin{aligned} T(a) &= a + a\sigma + a\sigma^2 + \dots + a\sigma^{n-2} + a\sigma^{n-1} \\ &= (b - b\sigma) + (b - b\sigma)\sigma + (b - b\sigma)\sigma^2 + \dots + (b - b\sigma)\sigma^{n-2} + (b - b\sigma)\sigma^{n-1} \\ &= (b - b\sigma) + (b\sigma - b\sigma^2) + (b\sigma^2 - b\sigma^3) + \dots + (b\sigma^{n-2} - b\sigma^{n-1}) + (b\sigma^{n-1} - b\sigma^n) \\ &= b - b\sigma^n = b - b = 0. \end{aligned}$$

Conversely, assume that $T(a) = 0$. We first find an element c in E with $T(c) = 1$. Since $o(\sigma) = n$, the automorphisms $1, \sigma, \sigma^2, \dots, \sigma^{n-2}, \sigma^{n-1}$ are distinct and $\{1, \sigma, \sigma^2, \dots, \sigma^{n-2}, \sigma^{n-1}\}$ is linearly independent by Lemma 57.7. So there is a $u \in E$ with

$$T(u) = u + u\sigma + u\sigma^2 + \dots + u\sigma^{n-2} + u\sigma^{n-1} \neq 0.$$

Let $c = u/T(u)$. Since $T(u) \in K$ and E is Galois over K , we have $(T(u))^{\sigma^j} = T(u)$ for any $j = 0, 1, 2, \dots, n-1$ and thus

$$\begin{aligned} T(c) &= \frac{u}{T(u)} + \left(\frac{u}{T(u)}\right)\sigma + \left(\frac{u}{T(u)}\right)\sigma^2 + \dots + \left(\frac{u}{T(u)}\right)\sigma^{n-2} + \left(\frac{u}{T(u)}\right)\sigma^{n-1} \\ &= \frac{u}{T(u)} + \left(\frac{u\sigma}{T(u)\sigma}\right) + \left(\frac{u\sigma^2}{T(u)\sigma^2}\right) + \dots + \left(\frac{u\sigma^{n-2}}{T(u)\sigma^{n-2}}\right) + \left(\frac{u\sigma^{n-1}}{T(u)\sigma^{n-1}}\right) \end{aligned}$$

$$\begin{aligned}
&= \frac{u}{T(u)} + \frac{u\sigma}{T(u)} + \frac{u\sigma^2}{T(u)} + \cdots + \frac{u\sigma^{n-2}}{T(u)} + \frac{u\sigma^{n-1}}{T(u)} \\
&= \frac{T(u)}{T(u)} = 1.
\end{aligned}$$

We put $b = ac + (a + a\sigma)(b\sigma) + (a + a\sigma + a\sigma^2)(b\sigma^2) + (a + a\sigma + a\sigma^2 + a\sigma^3)(b\sigma^3) + \cdots + (a + a\sigma + a\sigma^2 + \cdots + a\sigma^{n-2})(b\sigma^{n-2}) \in E$.

Then

$$\begin{aligned}
b - b\sigma &= ac + (a + a\sigma)(c\sigma) + (a + a\sigma + a\sigma^2)(c\sigma^2) \\
&\quad + (a + a\sigma + a\sigma^2 + a\sigma^3)(c\sigma^3) \\
&\quad + \cdots + (a + a\sigma + a\sigma^2 + \cdots + a\sigma^{n-2})(c\sigma^{n-2}). \\
&\quad - (a\sigma)(c\sigma) - (a\sigma + a\sigma^2)(c\sigma^2) - (a\sigma + a\sigma^2 + a\sigma^3)(c\sigma^3) \\
&\quad - (a\sigma + a\sigma^2 + a\sigma^3 + a\sigma^4)(c\sigma^4) \\
&\quad - \cdots - (a\sigma + a\sigma^2 + a\sigma^3 + \cdots + a\sigma^{n-1})(c\sigma^{n-1}) \\
&= ac + a(c\sigma) + a(c\sigma^2) + \cdots + a(c\sigma^{n-2}) - (a\sigma + a\sigma^2 + \cdots + a\sigma^{n-1})(c\sigma^{n-1}) \\
&= ac + a(c\sigma) + a(c\sigma^2) + \cdots + a(c\sigma^{n-2}) - (T(a) - a)(c\sigma^{n-1}) \\
&= ac + a(c\sigma) + a(c\sigma^2) + a(c\sigma^3) + \cdots + a(c\sigma^{n-1}) = aT(c) = a.
\end{aligned}$$

Hence $a = b - b\sigma$ for some $b \in E$ when $T(a) = 0$.

(2) If $a = b/b\sigma$ for some $b \in E \setminus \{0\}$, then

$$\begin{aligned}
N(a) &= \frac{b}{b\sigma} \cdot \left(\frac{b}{b\sigma}\right)\sigma \cdot \left(\frac{b}{b\sigma}\right)\sigma^2 \cdots \left(\frac{b}{b\sigma}\right)\sigma^{n-2} \cdot \left(\frac{b}{b\sigma}\right)\sigma^{n-1} \\
&= \frac{b}{b\sigma} \cdot \frac{b\sigma}{b\sigma^2} \cdot \frac{b\sigma^2}{b\sigma^3} \cdots \frac{b\sigma^{n-2}}{b\sigma^{n-1}} \cdot \frac{b\sigma^{n-1}}{b\sigma^n} = \frac{b}{b} = 1.
\end{aligned}$$

Conversely, assume $N(a) = 1$. Then of course $a \neq 0$. From Lemma 57.7, it follows that there is a $d \in E$ for which

$$\begin{aligned}
b := (a)d + (a \cdot a\sigma)d\sigma + (a \cdot a\sigma \cdot a\sigma^2)d\sigma^2 + \cdots + (a \cdot a\sigma \cdot a\sigma^2 \cdots a\sigma^{n-2})d\sigma^{n-2} \\
+ (a \cdot a\sigma \cdot a\sigma^2 \cdots a\sigma^{n-2} \cdot a\sigma^{n-1})d\sigma^{n-1}
\end{aligned}$$

is distinct from 0. Then we get

$$\begin{aligned}
a(b\sigma) &= a(a\sigma)d\sigma + a(a\sigma \cdot a\sigma^2)d\sigma^2 + a(a\sigma \cdot a\sigma^2 \cdot a\sigma^3)d\sigma^3 \\
&\quad + \cdots + a(a\sigma \cdot a\sigma^2 \cdot a\sigma^3 \cdots a\sigma^{n-1})d\sigma^{n-1} + a(a\sigma \cdot a\sigma^2 \cdot a\sigma^3 \cdots a\sigma^{n-1} \cdot a\sigma^n)d\sigma^n \\
&= b - (a)d + a \cdot N(a) \cdot d\sigma^n = b - ad + a \cdot 1 \cdot d = b.
\end{aligned}$$

Since $b \neq 0$, also $b\sigma \neq 0$ and $a(b\sigma) = b$ gives $a = b/b\sigma$. □

We close this paragraph with two applications of Theorem 57.9. We describe cyclic extensions. The degree is the characteristic in the first case and relatively prime to the characteristic in the second case.

57.10 Theorem: *Let K be a field of characteristic $p \neq 0$ and let E be a cyclic extension of K with $|E:K| = p$. Then there is an $a \in K$ such that $f(x) = x^p - x - a \in K[x]$ is irreducible in $K[x]$ and $E = K(t)$ for any root t of $f(x)$.*

Proof: By hypothesis, E is Galois over K and $\text{Aut}_K E$ is cyclic of order p , say $\text{Aut}_K E = \langle \sigma \rangle$. Then $T_{E/K}(1) = 1 + 1\sigma + 1\sigma^2 + \dots + 1\sigma^{p-1} = p = 0$, so $1 = b - b\sigma$ for some $b \in E$ (Theorem 57.9(1)). Let $u = -b$. Then $u\sigma = 1 + u$ and we get $u^p\sigma = (u\sigma)^p = (1 + u)^p = 1^p + u^p = 1 + u^p$. Hence

$$(u^p - u)\sigma = u^p\sigma - u\sigma = (1 + u^p) - (1 + u) = u^p - u$$

and $u^p - u$ is fixed by σ and thus by all automorphisms in $\text{Aut}_K E$. Since E is Galois over K , this gives $u^p - u \in K$. Let us put $u^p - u = a$. Thus u is a root of $f(x) = x^p - x - a \in K[x]$.

It remains to show that $f(x)$ is irreducible over K and that $E = K(t)$ for any root t of $f(x)$. Since b is not fixed by σ , we see $b \notin K$, so $u \notin K$ and thus $K \subset K(u) \subseteq E$. But $|E:K| = p$ is prime and so there is no intermediate field of E/K distinct from K and E . This forces $K(u) = E$. Then $\deg f(x) = p = |E:K| = |K(u):K| = \text{degree of the minimal polynomial of } u \text{ over } K$. Since the minimal polynomial of u over K divides $f(x)$, we deduce that $f(x)$ is the minimal polynomial of u over K . In particular, $f(x)$ is irreducible in $K[x]$.

Now for any $j \in \mathbb{F}_p \subseteq K$, there holds $j^p = j$ and consequently

$$f(u + j) = (u + j)^p - (u + j) - a = u^p + j^p - u - j - a = u^p - u - a = 0.$$

So $u, u + 1, u + 2, \dots, u + p - 1 \in E$ are roots of $f(x)$. Since $f(x)$ has p roots, any root t of $f(x)$ is equal to $u + j$ for some $j \in \mathbb{F}_p$. So we get $K(t) = K(u + j) = K(u) = E$ for any root t of $f(x)$. \square

57.11 Theorem: *Let K be a field and let E be a cyclic extension of K of degree $|E:K| = n$. Assume that either $\text{char } K = 0$ or $\text{char } K \neq 0$ but $\text{char } K$ does not divide n . Assume, in addition, that $x^n - 1$ splits in K . Then there is an $a \in K$ such that $f(x) = x^n - a \in K[x]$ is irreducible in $K[x]$ and $E = K(u)$ for any root u of $f(x)$.*

Proof: By hypothesis, $\text{Aut}_K E$ is a cyclic group, say $\text{Aut}_K E = \langle \sigma \rangle$, and $o(\sigma) = |\text{Aut}_K E| = |E:K| = n$. All roots of the polynomial $x^n - 1$, which splits in K , are simple since its derivative $nx^{n-1} \neq 0$ in view of the assumption on $\text{char } K$. Thus there are exactly n distinct roots of $x^n - 1$ in K . Since $r^n = s^n = 1$ implies $(rs)^n = 1$, the roots of $x^n - 1$ make up a subgroup of K^\times . Any finite subgroup of K^\times is cyclic (Theorem 52.18), so the roots of $x^n - 1$ form a cyclic group of order n . Let $r \in K$ be a generator of this group so that the n roots of $x^n - 1$ are $1, r, r^2, \dots, r^{n-1}$.

We have $N_{E/K}(r) = r^n = 1$ (Lemma 57.4(2)) and so there is a $b \in E$ with $r = b/b\sigma$ (Theorem 57.9(2)). Let $u = 1/b$. Then $u \in E \setminus \{0\}$ and $u\sigma = ur$. This implies $u^n \sigma = (u\sigma)^n = (ur)^n = u^n r^n = u$, so u^n is fixed by σ , so by $\text{Aut}_K E$, and therefore $u^n \in K$. Let us put $u^n = a$.

Then $x^n - a \in K[x]$ and this polynomial has n roots $u, ur, ur^2, \dots, ur^{n-1}$ in $K(u)$, which are all distinct. So $x^n - a$ splits in $K(u)$, but not in a proper subfield of $K(u)$ containing K , since any intermediate field of $K(u)/K$, in which $x^n - a$ splits, must contain the root u and hence must be identical with $K(u)$. Thus $K(u)$ is a splitting field of $x^n - a$ over K . Since the roots of $x^n - a$ are distinct, the irreducible factors of $x^n - a$ are separable over K and thus $K(u)$ is Galois over K (Theorem 55.7). In particular, $|\text{Aut}_K K(u)| = |K(u):K|$.

Any K -automorphism $\sigma^j \in \text{Aut}_K E$ ($j = 0, 1, 2, \dots, n-1$) sends u to $ur^j \in K(u)$, thus the restriction of σ^j to $K(u)$ is a K -automorphism of $K(u)$ (Theorem 42.22). Since $u\sigma^i = ur^i \neq ur^j = u\sigma^j$ when $i, j \in \{0, 1, 2, \dots, n-1\}$ and $i \neq j$, we see that these K -automorphisms of $K(u)$ are distinct. Hence there are at least n K -automorphisms of $K(u)$. This implies $|K(u):K| = |\text{Aut}_K K(u)| \geq n$. From $n = |E:K| \geq |K(u):K| \geq n$, we get $|K(u):K| = n$, whence $E = K(u)$.

Finally, since the minimal polynomial of u over K divides $x^n - a$ and $\deg(x^n - a) = n = |K(u):K| = \text{degree of the minimal polynomial of } u \text{ over } K$, we deduce that $x^n - a$ is the minimal polynomial of u over K and $x^n - a$ is irreducible in $K[x]$. Moreover, any root t of $x^n - a$ is equal to ur^j for some $j = 0, 1, 2, \dots, n-1$ and, since $r \in K$, we get $K(t) = K(ur^j) = K(u) = E$ for any root t of $x^n - a$. \square

Exercises

1. Let K be a field and let E be a finite dimensional separable extension of K . Prove that, for any $k \in K$, there is an $a \in E$ such that $T_{E/K}(a) = k$.
2. Let $K \subseteq L \subseteq E \subseteq N$ be fields and assume that N is normal over K . If s is the cardinal number of L -homomorphisms from E into N and n is the cardinal number of K -homomorphisms from L into N , prove that sn is the cardinal number of K -homomorphisms from E into N .
3. Let K be a field of characteristic $p \neq 0$ and $f(x) = x^p - x - a \in K[x]$. Show that $f(x)$ either splits in K or is irreducible in $K[x]$.
4. Let K be a field of characteristic $p \neq 0$ and $f(x) = x^p - x - a \in K[x]$. Prove that if $f(x)$ is irreducible in $K[x]$ and u a root of $f(x)$, then $K(u)$ is a cyclic extension of K of degree p .
5. Let K be a field and $n \in \mathbb{N}$. Assume that either $\text{char } K = 0$ or $\text{char } K \neq 0$ but $\text{char } K$ does not divide n . Assume that $x^n - 1$ splits in K . Prove that, if $a \in K$ and u a root of $f(x) = x^n - a \in K[x]$, then $K(u)$ is a cyclic extension of K and $|K(u):K|$ divides n and $u^{|K(u):K|} \in K$.