Pacific Journal of Mathematics

THE NORM FUNCTION OF AN ALGEBRAIC FIELD EXTENSION

HARLEY M. FLANDERS

Vol. 3, No. 1 March 1953

THE NORM FUNCTION OF AN ALGEBRAIC FIELD EXTENSION

HARLEY FLANDERS

1. Introduction. Let k be an algebraic field, K a finite extension field of degree n over k, and $\omega_1, \cdots, \omega_n$ a linear basis of K over k. (For the standard results of field theory which we have used in this paper, the reader is referred to the texts [2; 4; 5].) If $X = (X_1, \cdots, X_m)$ is a set of indeterminates over K, then $[K(X) : k(X)] = n$, and in fact $\omega_1, \cdots, \omega_n$ is a basis of $K(X)$ over $k(X)$. We set $m = n$ and form the so-called *general element*

$$\Xi = \omega_1 X_1 + \cdots + \omega_n X_n$$

of K over k. We may, without confusion, use the symbol $N_{K/k}$ both for the norm function of K/k and for that of $K(X)/k(X)$. The *general norm of K over k* is the polynomial

$$N(X) = N(X_1, \cdots, X_n) = N_{K/k}(\Xi) \in k[X].$$

We propose here to discuss the factorization of this polynomial and the possibility of characterizing the norm function $N_{K/k}$ of K/k intrinsically. We are indebted to Professor E. Artin for a helpful suggestion communicated orally.

2. Factorization of the general norm. If we take a new basis $\eta_1, \cdots, \eta_n$, we simply effect a nonsingular linear transformation on the n variables X_i; hence nothing essential is changed. The possibility of selecting a convenient basis will be used to advantage in the proofs below. Our first result, while not complete, admits a simple proof; consequently we give it before giving a more general result.

THEOREM 1. *Let $K = k(\theta)$ be a simple extension of k. Then the general norm $N(X)$ is irreducible in $k[X]$.*

Proof. Let $f(X) = (X - \theta_1) \cdots (X - \theta_n)$ be the minimum function of $\theta = \theta_1$ over k, and take $1, \theta, \cdots, \theta^{n-1}$ as a basis of K over k. Then

Received January 29, 1952.
Pacific J. Math. 3 (1953), 103-113

$$N(X) = \prod_{i=1}^{n} \left(X_1 + \theta_i X_2 + \cdots + \theta_i^{n-1} X_n \right).$$

Since this is a complete factorization of $N(X)$ into linear factors, it follows that any factor of $N(X)$ must be the product of a constant and certain of the linear factors displayed. Consequently, if $G(X)$ is an irreducible factor of $N(X)$ in $k[X]$ with

$$\deg G(X) = r \qquad (1 \leq r \leq n),$$

then, by properly renumbering and adjusting the coefficient of X_1^r, we have

$$G(X) = \prod_{i=1}^{r} \left(X_1 + \theta_i X_2 + \cdots + \theta_i^{n-1} X_n \right).$$

It follows that $G(X, -1, 0, \cdots, 0) \in k[X]$. But this means that

$$\prod_{i=1}^{r} (X - \theta_i) \in k[X].$$

Since $f(X)$ is irreducible over k, we must have $r = n$.

We can generalize this theorem as follows.

THEOREM 2. *Let* $[K : k] = n$, *and let* $m = \max \{[k(\theta) : k]$ *for* $\theta \in K\}$. *Then* m *divides* n, *and the complete factorization in* $k[X]$ *of the general norm* $N(X)$ *of* K *over* k *is given by*

$$N(X) = [F(X)]^{n/m},$$

where $F(X)$ *is an irreducible polynomial in* $k[X]$.

Proof. If K/k is a separable extension, then it is a simple one and Theorem 1 applies. Consequently, we may assume that k has finite characteristic p, and that K/k is inseparable. Let S be the maximal separable subfield of K over k, and let $s = [S : k]$, so that $n = sp^u$. We let e denote the least whole number such that $K^{p^e} \subset S$. Then $1 \leq e \leq u$ and it is known [2; 4; 5] that $m = sp^e$. Finally, we let α be a generator of S/k, thus $S = k(\alpha)$; and let

$$\Omega_1 = 1, \Omega_2, \cdots, \Omega_{p^u}$$

be a linear basis of K/S with

$$(\Omega_j)^{p^e} = \beta_j \in S.$$

The general element Ξ of K/k is given by

$$\Xi = \sum \alpha^i \Omega_j X_{ij} \qquad (i = 0, \cdots, s-1;\ j = 1, \cdots, p^u),$$

and the general norm by

$$N(X) = [F(X)]^{p^{u-e}}$$

with

$$F(X) = N_{S/k}\left(\sum \alpha^{ip^e} \beta_j X_{ij}^{p^e}\right).$$

This is the case because

$$N_{K/k} = N_{S/k} \circ N_{K/S}$$

and

$$N_{K/S}\, A = A^{p^u} = (A^{p^e})^{p^{u-e}} \quad \text{for} \quad A \in K.$$

We next assert that the polynomial

$$\Pi(X) = \Xi^{p^e} = \sum \alpha^{ip^e} \beta_j X_{ij}^{p^e}$$

is irreducible in the ring $S[X]$. Suppose this is not the case and let $\Gamma(X)$ be an irreducible factor. We normalize the coefficient of the highest power of X_{01} in $\Gamma(X)$; we may thus write

$$\Gamma(X) = \Xi^{p^f v},$$

where $0 \leq f < e$ and $(v, p) = 1$. We clearly have

$$(p^f v,\ p^e) = p^f,$$

and so there exist rational integers a, b such that

$$p^f va + p^e b = p^f.$$

This implies that

$$\Xi^{p^f} = (\Xi^{p^f v})^a \, (\Xi^{p^e})^b \in S[X];$$

hence

$$\Xi^{p^f} \in S[X], \sum \alpha^{ip^f} (\Omega_j)^{p^f} X_{ij}^{p^f} \in S[X].$$

Thus, for each i and j $(i = 0, \cdots, s-1;\ j = 1, \cdots, p^u)$, we have

$$\alpha^{ip^f} (\Omega_j)^{p^f} \in S.$$

In particular, setting $i = 0$, we obtain

$$(\Omega_j)^{p^f} \in S \text{ for } j = 1, \cdots, p^u.$$

Hence $K^{p^f} \subset S$, a contradiction of the definition of e.

It will be convenient in the remainder of the proof to have a "sufficiently large" field at our disposal. We form the splitting field U over k of any polynomial $f(X)$ in $k[X]$ which has amongst its roots the quantities $\alpha, \Omega_1, \cdots, \Omega_{p^u}$. Then we may assume $k \subset S \subset K \subset U$, and any relative isomorphism on K over k into any field containing K is already into U.

Now let σ be any relative isomorphism of S over k into U. The fact that $\Pi(X)$ is irreducible over $S[X]$ clearly implies that $\Pi^\sigma(X)$ is irreducible over $S^\sigma[X]$. We also assert that if $\sigma \neq \iota$, the identity isomorphism, then $\Pi(X)$ and and $\Pi^\sigma(X)$ are relatively prime in $U[X]$. To prove this, we first note that, since K is a pure inseparable extension of S, σ has a unique prolongation to an isomorphism (also denoted by σ) of K/k. Thus

$$\Pi(X) = \Xi^{p^e}, \ \Pi^\sigma(X) = (\Xi^\sigma)^{p^e}.$$

These can have a proper common factor if and only if

$$\lambda \Xi = \Xi^\sigma \text{ for } \lambda \text{ in } K.$$

If this is the case, then we compare the coefficients on either side of X_{01} and X_{11}, obtaining $\lambda = 1$ and $\alpha = \alpha^\sigma$, an impossibility if $\sigma \neq \iota$.

To complete the proof, we let $\sigma_1, \cdots, \sigma_s$ be all of the relative isomorphisms of S over k into U. We have

$$F(X) = N_{S/k}[\Pi(X)] = \prod_{h=1}^{s} [\Pi^{\sigma_h}(X)].$$

Let $G(X)$ be any irreducible factor of $F(X)$ in $k[X]$. It follows from the facts (a) each $\Pi^{\sigma_h}(X)$ is irreducible in $S^{\sigma_h}[X]$ and (b) the s polynomials $\Pi^{\sigma_h}(X)$ of $U[X]$ are pairwise relatively prime—an immediate consequence of the result of the last paragraph—that $G(X)$, after a trivial modification of leading coefficient, is necessarily of the form

$$G(X) = \prod_{h=1}^{r} [\Pi^{\sigma_h}(X)] \qquad (1 \leq r \leq s),$$

where, of course, we have rearranged the indices h as needed. Since $G(X) \in k[X]$, it follows that the polynomial

$$g(X) = \prod_{h=1}^{r} (X^{p^e} - \alpha^{\sigma_h}),$$

which results from the specialization

$$[X_{01} = X,\ X_{11} = -1,\ X_{ij} = 0 \text{ for all other } i, j],$$

is in $k[X]$. This implies $r = s$, $G(X) = F(X)$, as desired.

3. Characterization of the norm function.[1] In this section, let k, K be fields such that $[K : k] = n$. The norm function $N_{K/k}$ has the following properties:

(N_1) $\qquad N_{K/k}(AB) = (N_{K/k}A)\ (N_{K/k}B)$ for all $A, B \in K$,

(N_2) $\qquad N_{K/k}(a) = a^n$ for all $a \in k$.

These properties mean that $N_{K/k}0 = 0$ and that $N_{K/k}$ is a homomorphism on the multiplicative group K^* of nonzero elements of K into k^* such that

$$N_{K/k}a = a^n \text{ on } k^*.$$

[1] A somewhat different characterization is given in [1].

DEFINITION 1. A function f on K into k is a *norm-like function* if

(N_1) $\qquad f(AB) = f(A)\,f(B)$ for all $A, B \in K$,

(N_2) $\qquad f(a) = a^n$ for all $a \in k$.

It is evident from group-theoretic considerations that in general there are many norm-like functions. We wish here to impose further restrictions which will distinguish the norm function $N_{K/k}$ from amongst all norm-like functions. The considerations of §1 suggest a "continuity" condition which we proceed to formulate.

DEFINITION 2. Let L be an n-dimensional linear space over a field k. A function f on L into k will be called a *polynomial function* if there is a basis $x_1, \cdots, x_n$ of L and a polynomial

$$F(X_1, \cdots, X_n) \in k[X]$$

such that whenever

$$x = \sum a_i x_i \in L,$$

then

$$f(x) = F(a_1, \cdots, a_n).$$

It is clear that there is no real dependence on a particular basis in this definition. Similarly we may define a *homogeneous polynomial function of degree m on L to k* by insisting that $F(X)$ be homogeneous of degree m. The norm function $N_{K/k}$ is a homogeneous norm-like function of degree n on K into k.

THEOREM 3. *Let k be an infinite field, $[K : k] = n$, and let f be a polynomial norm-like function on K into k. Then $f = N_{K/k}$.*

Proof. Let $\omega_1 = 1, \omega_2, \cdots, \omega_n$ be a basis of K/k. $F(X_1, \cdots, X_n)$ a polynomial such that

$$f(\sum a_i \omega_i) = F(a_1, \cdots, a_n).$$

Since k is infinite, F is necessarily unique. It is known that there exist polynomials $g_1(X), \cdots, g_n(X) \in k[X]$ such that if

$$A = \sum a_i \omega_i \in K$$

and we set

$$B = \sum g_i(a_1, \cdots, a_n)\omega_i,$$

then $AB = N_{K/k}A$. Thus

$$f(AB) = f(A)\,f(B) = (N_{K/k}A)^n,$$

and so we have

$$F(a_1, \cdots, a_n)\,F(g_1(a_1, \cdots, a_n), \cdots) = [N(a_1, \cdots, a_n)]^n,$$

where $N(X)$ is the general norm of K/k. Since k is infinite, this is an identity; that is,

$$F(X)\,F(g_1(X), \cdots, g_n(X)) = N(X)^n.$$

By Theorem 2, we have

$$N(X) = M(X)^h,$$

where $M(X)$ is irreducible in $k[X]$. It follows that

$$F(X) = cM(X)^r$$

for some power r and $c \in k$. We specialize:

$$X \longrightarrow (a, 0, \cdots, 0),$$

obtaining

$$a^n = F(a, 0, \cdots, 0) = cM(a, 0, \cdots, 0)^r.$$

We raise to the h-power, noting that

$$N(a, 0, \cdots, 0) = a^n; \quad a^{nh} = c^h a^{nr}.$$

This is true for all $a \in k$; hence

$$nh = nr,\ h = r,\ c^h = 1,\ F(X) = cM(X)^h = cN(X).$$

It is immediate that $c = 1$, and hence $f = N_{K/k}$.

In the case that k is a finite field we get a somewhat different result unless we strengthen the hypotheses. We first have the following result.

THEOREM 4. *Let k be a finite field of q elements and let $[K : k] = n$. Suppose that f is a norm-like function on K into k. Then either $f = (N_{K/k})^r$, where $0 < r < q - 1$ and $nr \equiv n \pmod{q-1}$, or $n \equiv 0 \pmod{q-1}$ and f is given by $f(0) = 0$ and $f(A) = 1$ for all $A \neq 0$. Conversely, each such function is norm-like.*

Proof. Let A be a generator of the (cyclic) group K^*. Then

$$a = N_{K/k}A = A^u$$

is a generator of k^*. Here we have set $u = (q^n - 1)/(q - 1)$ for convenience. The norm-like function f, being a homomorphism on K^*, is completely determined by its effect on A. Thus we have $f(A) = a^r$ for some rational integer r. Since $a^{q-1} = 1$, we may assume that $0 \leq r < q - 1$. If $B \in K^*$, then $B = A^c$ and so

$$f(B) = f(A)^c = (N_{K/k}A)^{rc} = (N_{K/k}A^c)^r = (N_{K/k}B)^r.$$

Thus our function f is given by

$$f(B) = (N_{K/k}B)^r \text{ for } B \neq 0, \ f(0) = 0.$$

So far we have used only the property (N_1). Property (N_2) asserts that $f(a) = a^n$. But in our case we have

$$f(a) = (N_{K/k}a)^r = a^{nr};$$

hence $a^n = a^{nr}$ is a necessary and sufficient condition that f be norm-like. This is equivalent to

$$nr \equiv n \pmod{q-1},$$

since $k^* = \langle a \rangle$ is a cyclic group of $q - 1$ elements.

In our next proof we shall use the following results of Chevalley [3]. Let k be a finite field of q elements, and let L denote the linear space of all *n-tuples* $\mathbf{a} = (a_1, \cdots, a_n)$ of elements of k. Let I denote the ideal in $k[X_1, \cdots, X_n]$ of all polynomials $F(X)$ such that $F(\mathbf{a}) = 0$ identically on L. Then

$$I = (X_1^q - X_1, \cdots, X_n^q - X_n).$$

If $F(X) \in k[X]$, then there is a unique polynomial $F^*(X)$ such that (a) $F \equiv F^* \pmod{I}$ and (b) $\deg_{X_i} F^* \leq q-1$ for each $i = 1, \cdots, n$. The polynomial F^* is called the *reduced form* of F, and has degree at most that of F. Finally, if $F(\mathbf{a}) = 1$ for all $\mathbf{a} \neq 0$ and $F(0) = 0$, then

$$F^* = (-1)^{n-1} (X_1^{q-1} - 1) \cdots (X_n^{q-1} - 1) + 1.$$

THEOREM 5. *Let k be a finite field and let $[K : k] = n$. Suppose that f is a norm-like function on K into k, and that f is also a polynomial function of degree at most n. Then $f = N_{K/k}$.*

Proof. As before, we let q be the number of elements of k, and we may apply Theorem 4. If $q = 2$, we clearly have $f = N_{K/k}$ since

$$f(0) = 0 = N_{K/k} 0;$$

whilst if $A \neq 0$, then $f(A) \neq 0$, and hence

$$f(A) = 1 = N_{K/k} A.$$

We may henceforth assume that $q > 2$.

Next, let $\omega_1, \cdots, \omega_n$ be a basis of K/k, and let $N(X)$ be the general norm of K/k with respect to this basis. By hypothesis, there exists a polynomial $F(X)$ of degree at most n such that

$$f(A) = F(a_1, \cdots, a_n) \text{ for all } A = \sum a_i \omega_i .$$

Suppose that the second alternative of Theorem 4 is the case. Then

$$f(0) = 0 \text{ and } f(A) = 1 \text{ for all } A \neq 0.$$

This implies that

$$F^* = (-1)^{n-1} (X_1^{q-1} - 1) \cdots (X_n^{q-1} - 1) + 1,$$

and so

$$(q-1)n = \deg F^* \leq \deg F = n.$$

Hence $q - 1 \leq 1$, $q = 2$. We have already ruled out this possibility.

Finally suppose that $f = (N_{K/k})^r$, where $1 \leq r < q - 1$. We set

$$G(X) = F(X)[N(X)]^{q-1-r},$$

and have $G(0) = 0$. If $\mathbf{a} \neq 0$, then

$$A = \sum a_i \omega_i \neq 0,$$

and

$$G(\mathbf{a}) = f(A)(N_{K/k}A)^{q-1-r} = (N_{K/k}A)^{q-1} = 1.$$

This implies that

$$G^* = (-1)^{n-1}(X_1^{q-1} - 1)\cdots(X_n^{q-1} - 1) + 1;$$

hence

$$(q-1)n = \deg G^* \leq \deg G \leq n + (q-1-r)n = (q-r)n,$$

so that

$$q - 1 \leq q - r,\ r \leq 1,\ r = 1.$$

We are left with the single possibility $f = N_{K/k}$, as desired.

It is worth noting that the proof can still be pushed through under the weaker assumption that f is a polynomial function of degree at most $2n - 1$. However, the most interesting case is that in which f is a homogeneous polynomial function of degree n.

4. Conjecture. It would be interesting to prove Theorem 3 under weakened conditions. We make the following definition.

DEFINITION 3. Let L be an n-dimensional linear space over a field k. A function f on L to k will be called an *algebraic function* if there is a basis $x_1, \cdots, x_n$ of L and a polynomial

$$F(X_0, X_1, \cdots, X_n) \in k[X],$$

such that $F(X) \neq 0$, and such that whenever $x = \sum a_i x_i$ then

$$F(f(x), a_1, \cdots, a_n) = 0.$$

Our conjecture is the following.

If k is an infinite field, $[K : k] = n$, and f is an algebraic norm-like function on K into k, then $f = N_{K/k}$.

REFERENCES

1. E. Artin, *Remarques concernant la théorie de Galois*, Collogues Internationaux C.N.R.S., XXIV, 1950, pp. 161-162.

2. N. Bourbaki, *Algèbra*, Hermann, Paris, Chapter 5.

3. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg, **11** (1935), 73-75.

4. B. van der Waerden, *Moderne Algebra* I, Ungar, New York, 1948.

5. H. Weyl, *Algebraic theory of numbers*, Princeton, 1940.

UNIVERSITY OF CALIFORNIA, BERKELEY

PACIFIC JOURNAL OF MATHEMATICS

Vari-Type Composition by
Elaine Barth
Delores Wierman

With the cooperation of
E. F. Beckenbach
E. G. Straus

Printed in the United States of America by
Edwards Brothers, Inc., Ann Arbor, Michigan

UNIVERSITY OF CALIFORNIA PRESS * BERKELEY AND LOS ANGELES

Pacific Journal of Mathematics
Vol. 3, No. 1 March, 1953