THE NORM FUNCTION OF AN ALGEBRAIC FIELD EXTENSION, II

HARLEY FLANDERS

1. Introduction. In our previous paper [3], we consider the general norm

$$N_{K/k}(\omega_1 X_1 + \cdots + \omega_n X_n)$$

of a finite extension K of an algebraic field k. We proved that this form is the (n/m)th power of an irreducible polynomial in $k[X]$, where m is the maximum of the degrees of the simple subfields $k(\theta)$ of K over k. The proof of this result used a considerable amount of the heavy machinery of the theory of algebraic extensions: the maximal separable subfield, conjugates, transitivity of the norm, etc. Using only the fact that the general norm is a power of an irreducible, we obtained a characterization of the norm function $N_{K/k}$ in terms of inner properties.

In the present paper we shall approach these matters from a different point of view. We shall give an entirely different proof that the general norm is a prime power—this one based on very little field theory and completely rational. From this, as noted above, the intrinsic characterization of the norm function follows. We shall then use this to derive certain theorems in field theory, such as the transitivity of the norm.

Section 2 contains some preliminary results on polynomials and their norms and the details of proof for certain results used in [3]. In § 3 we prove the main result and in § 4 we give some applications.

2. Tool theorems. We shall be dealing with polynomial rings $k[X]$ in indeterminates $X = (X_1, \cdots, X_r)$ and shall take for granted the fundamental fact that such rings are unique factorization domains [1, p. 39]. The following is well known, but we include it—as we do several of the results of this section—for completeness.

LEMMA 1. *Let $f(X)$, $g(X) \in k[X]$ and suppose f and g are relatively prime. Let $k \le K$ so that $k[X] \le K[X]$. Then f and g are still relatively prime when considered as elements of the extended ring $K[X]$.*

Received October 19, 1953.
Pacific J. Math. 5 (1955), 519-528

For the case $r = 1$ of one variable, this is so because of the Euclidean greatest common divisor algorithm.

In general, we suppose $H(X)$ is a common factor of f and g, $H(X) \in K[X]$. Without loss of generality, we may assume that H has positive degree in X_r. We form the fields of rational functions,

$$\overline{K} = K(x_1, \cdots, x_{r-1}), \quad \overline{k} = k(x_1, \cdots, x_{r-1}),$$

and the polynomials

$$\overline{f}(T) = f(x_1, \cdots, x_{r-1}, T), \quad \overline{g}(T) = g(x_1, \cdots, x_{r-1}, T)$$

of the ring $\overline{k}[T]$. These polynomials have a non-trivial factor $H(x, T)$ in $\overline{K}[T]$, hence by the case $r = 1$, they have a non-constant factor $h_1(x, T) \in \overline{k}[T]$:

$$\overline{f}(T) = h_1(x, T) f_1(T), \quad \overline{g}(T) = h_1(x, T) g_1(T).$$

Here h_1, f_1, g_1 are polynomials with coefficients rational functions over k in $x = (x_1, \cdots, x_{r-1})$. Multiplying by a suitable denominator $q(x)$, we obtain

$$q(x) f(x, T) = h(x, T) f_2(x, T), \quad q(x) g(x, T) = h(x, T) g_2(x, T),$$

where all terms are polynomials. This implies

$$q(X_1, \cdots, X_{r-1}) f(X) = h(X) f_2(X), \quad q(X_1, \cdots, X_{r-1}) g(X) = h(X) g_2(X).$$

Since $h(X)$ actually involves X_r, it follows from unique factorization that some irreducible factor of h must divide both f and g.

LEMMA 2. *Let k be a field, $\mathfrak{O}$ an integral domain such that $k \leq \mathfrak{O}$, and such that if $\mathfrak{O}$ is considered as a linear space over k, then $\mathfrak{O}$ is finite dimensional. Then $\mathfrak{O}$ is a field.*

Proof. Cf. [2, p. 75]. If $a \in \mathfrak{O}$ and $a \neq 0$, then the mapping $b \longrightarrow ab$ is a one-one linear transformation on $\mathfrak{O}$ into $\mathfrak{O}$. Since $\mathfrak{O}$ is finite dimensional and rank plus nullity equals dimension, it must map $\mathfrak{O}$ onto $\mathfrak{O}$. Thus $1 = ab$ for some b then a has an inverse.

LEMMA 3. *Let $[K:k] = n$ and $\omega_1, \cdots, \omega_n$ be a basis of K over k. Then $[K(X):k(X)] = n$ and (ω) is a basis of $K(X)$ over $k(X)$.*

Proof. Let

$$\mathfrak{D} = k(X)\omega_1 + \cdots + k(X)\omega_n.$$

Then $\mathfrak{D}$ is a finite dimensional integral domain over $k(X)$ and

$$k(X) \leq \mathfrak{D} \leq K(X).$$

By Lemma 2, $\mathfrak{D}$ is a field; since

$$K = k\omega_1 + \cdots + k\omega_n \leq \mathfrak{D},$$

we have

$$K(X) = K \cdot k(X) \leq \mathfrak{D},$$

hence $\mathfrak{D} = K(X)$. It follows that (ω) spans $K(X)$ over $k(X)$. But it is clear (by equating coefficients) that (ω) is linearly independent over the rational function field $k(X)$.

We introduce the *norm* in this way. If $[K:k] = n$ and $A \in K$, then $N_{K/k}A$ is the determinant of the linear transformation $B \longrightarrow AB$ on K over k. Specifically, if $\omega_1, \cdots, \omega_n$ is any basis of K over k, and

$$A\omega_i = \sum a_{ij}\omega_j$$

then

$$N_{K/k}A = |a_{ij}|.$$

We similarly define the *trace*

$$S_{K/k}A = \sum a_{ii}$$

for later purposes. The rules

$$N_{K/k}(AB) = (N_{K/k}A)(N_{K/k}B), \quad S_{K/k}(A+B) = S_{K/k}A + S_{K/k}B,$$

$$N_{K/k}(a) = a^n, \qquad S_{K/k}(a) = n \cdot a,$$

follow immediately.

We form the fields $K(X)$, $k(X)$ so that also $[K(X):k(X)] = n$ and we may discuss

$$N_{K(X)/k(X)}[R(X)]$$

for $R(X) \in K(X)$. We shall use the abbreviation

$$N_{K/k} = N_{K(X)/k(X)}$$

as we did in [3] since this can hardly lead to confusion.

LEMMA 4. *Let*

$$F(X) \in K[X] \text{ and } f(X) = N_{K/k} F(X).$$

Then

$$f(X) \in k[X]$$

and $F(X)$ *divides* $f(X)$ *in the ring* $K[X]$.

Proof. We write

$$F(X) = \sum A^{(\alpha)} X_{(\alpha)}$$

where $A^{(\alpha)} \in K$ and $X_{(\alpha)}$ is a monomial in $X = (X_1, \cdots, X_r)$. We have

$$A^{(\alpha)} \omega_i = \sum a_{ij}^{(\alpha)} \omega_j, \qquad a_{ij}^{(\alpha)} \in k,$$

hence

$$F(X) \omega_i = \sum a_{ij}^{(\alpha)} X_{(\alpha)} \omega_j = \sum f_{ij}(X) \omega_j,$$

where $f_{ij} \in k[X]$. Thus

$$f(X) = N_{K/k} F = |f_{ij}| \in k[X],$$

which settles the first point. We may also write

$$\sum (F(X) \delta_{ij} - f_{ij}) \omega_j = 0,$$

which implies

$$|F(X) \delta_{ij} - f_{ij}| = 0.$$

On expanding the determinant we soon see that $F(X)$ does indeed divide $f(X)$.

LEMMA 5. *If*

$$F(X),\ G(X) \in K[X],\ \ h(X) \in k[X],$$

and

$$F(X) \equiv G(X) \pmod{h(X)},$$

then

$$N_{K/k}F(X) \equiv N_{K/k}G(X) \qquad \pmod{h(X)}.$$

Proof. We may write

$$F(X) = G(X) + h(X)Q(X)$$

with $Q(X) \in K[X]$. As above, we have

$$F(X)\,\omega_i = \sum f_{ij}(X)\,\omega_j, \quad G(X)\,\omega_i = \sum g_{ij}(X)\,\omega_j,$$
$$Q(X)\,\omega_i = \sum q_{ij}(X)\,\omega_j,$$

with $f_{ij}, g_{ij}, q_{ij} \in k[X]$. Thus

$$f_{ij} = g_{ij} + hq_{ij}.$$

and therefore

$$N(F) = |f_{ij}| = |g_{ij} + hq_{ij}| \equiv |g_{ij}| = N(G) \qquad \pmod{h(X)}.$$

LEMMA 6. *Let $F(X)$ be an irreducible polynomial in $K[X]$. Let $f(X) = N_{K/k}F(X)$ and suppose that $g(X)$ is any non-constant divisor of $f(X)$ in $k[X]$. Then $F(X)$ divides $g(X)$.*

The case $r = 1$ is given in [**4**, p. 19].

Proof. If $r = 1$ and $F(X)$ does not divide $g(X)$, then we can find polynomials $U(X), V(X) \in K[X]$ such that

$$U(X)F(X) + V(X)g(X) = 1.$$

Thus

$$U(X)F(X) \equiv 1 \qquad \pmod{g(X)}.$$

By Lemma 5 we obtain

$$u(X)\,f(X) \equiv 1 \pmod{g(X)}$$

which is clearly impossible.

In the general case we may suppose that the degree of F in X_r is positive and pass to the rational function fields $\overline{k} = k(x)$, $\overline{K} = K(x)$, where $x = (x_1, \cdots, x_{r-1})$. The usual unique factorization argument shows that $\overline{F}(T) = F(x_1, \cdots, x_{r-1}, T)$ is irreducible in $\overline{K}[T]$. For the norm we have

$$N_{\overline{K}/\overline{k}}\,\overline{F}(T) = \overline{f}(T) = f(x_1, \cdots, x_{r-1}, T).$$

The polynomial $\overline{g}(T) = g(x_1, \cdots, x_{r-1}, T)$ divides $\overline{f}(T)$ in $\overline{k}[T]$; it follows from the case $r = 1$ that $\overline{F}(T)$ divides $\overline{g}(T)$:

$$\overline{g}(T) = \overline{F}(T)\overline{H}(T).$$

We multiply by the denominator of $\overline{H}$ to arrive at a relation of the form

$$q(X_1, \cdots, X_{r-1})\,g(X) = F(X)H(X).$$

Since $F(X)$ is irreducible, this implies that $F(X)$ divides $g(X)$.

THEOREM 1. *Let $F(X)$ be irreducible in $K[X]$. Then $f(X) = N_{K/k}\,F(X)$ is a power of an irreducible polynomial in $k[X]$.*

Proof. If $p(X)$ and $q(X)$ are irreducible factors of $f(X)$ in $k[X]$, then by Lemma 6, $F(X)$ divides both $p(X)$ and $q(X)$. This implies, by Lemma 1, that $p(X) = q(X)$. Hence $f(X)$ has only one distinct irreducible factor.

NOTE 1. In the proofs of both Lemma 1 and Lemma 6, the reduction of the case of general r to the case $r = 1$ could have been effected by the Kronecker device of substituting suitable powers of a new variable T for the X_i, since in these statements we dealt with only a finite number of fixed polynomials and their divisors, all of bounded degree.

NOTE 2. Lemma 1, for the case in which $[K:k] = n$, is an immediate consequence of Lemma 4. For if $H(X) \in K(X)$ and $H(X)$ is a non-constant common divisor of f and g, then we have $f = HF_1$, $g = HG_1$, and thus

$$f^n = N(f) = N(H)N(F_1), \; g^n = N(H)N(G_1).$$

But H divides $N_{K/k}H$, hence $N(H)$ is non-constant. This is clearly impossible when f and g are relatively prime.

Once Lemma 1 is proved for finite extensions, it can be proved for arbitrary extensions by the use of a transcendence basis.

3. The general norm. Let $[K:k]=n$ and let $\omega_1, \cdots, \omega_n$ be a basis of K over k. As in [3], we form the *general element*

$$\Xi = \omega_1 X_1 + \cdots + \omega_n X_n \in K[X]$$

and the *general norm*

$$N_{N/k}(\Xi) \in k[X]$$

which is a form of degree n.

THEOREM 2. *The general norm is a power of an irreducible polynomial in* $k[X]$.

Proof. The general element Ξ is a linear form in $K[X]$, hence irreducible; Theorem 1 now applies.

From this now follow the results of §3 of [3]; we state the following instance.

THEOREM 3. *Let* $[K:k]=n$ *and let* ϕ *be a function on* K *into* k *with the following properties:*

(1) $\phi(AB)=\phi(A)\phi(B)$.

(2) $\phi(a)=a^n$.

(3) $\phi(\sum a_i \omega_i)=f(a_1, \cdots, a_n)$,

where f *is a polynomial of degree at most* n. *Then* $\phi(A)=N_{K/k}A$ *for all* A *in* K.

4. Applications. Let $k \leq L \leq K$, where K is a finite extension of k, and consider the function

$$A \longrightarrow N_{L/k}[N_{K/L}A]$$

on K into k. Evidently this satisfies the properties (1, 2, 3) of the theorem above, so we obtain

$$N_{K/k} = N_{L/k} \circ N_{K/L}.$$

Next, let $[K:k]=n$ and let $A \in K$. The *field polynomial* of A is

$$f_A(T) = f_{A,K/k}(T) = N_{K/k}(T-A).$$

It is clear that $f_A(A)=0$ and that $f_A(T)$ is the minimum polynomial of A in case $K = k(A)$—since $1, A, \cdots, A^{n-1}$ is a basis in that case. If $K \geq L \geq k$, then

$$f_{A,K/k}(T) = N_{K/k}(T-A) = N_{L/k}[N_{K/L}(T-A)]$$

$$= N_{L/k}[f_{A,K/L}(T)].$$

Especially if $A \in L$, then

$$f_{A,K/k}(T) = [f_{A,L/k}(T)]^{[K:L]}.$$

Here is another consequence; if $K \geq L \geq k$ and $A \in K$, we have

$$S_{K/k}(A) = S_{L/k}[S_{K/L}(A)].$$

For if $[K:k]=r$, then

$$f_{A,K/k}(T) = T^r - S_{K/k}(A)T^{r-1} + \cdots.$$

Our statement follows at once from this and the following lemma.

LEMMA 7. *Let* $[K:k]=n$ *and*

$$f(T) = T^r + A_1 T^{r-1} + \cdots + A_r \in K[T].$$

Then

$$N_{K/k} f(T) = T^{nr} + S_{K/k}(A_1) T^{nr-1} + \cdots + N_{K/k}(A_n).$$

This is proved by slightly modifying the proof of Lemma 4.

Finally we derive the familiar expressions for the norm and trace in terms of conjugates. Let $[K:k]=n$ and let $K \leq U$. Suppose $\sigma_1, \cdots, \sigma_n$ are n not necessarily distinct isomorphisms over k on K into U with the property that whenever $h(X_1, \cdots, X_n)$ is a symmetric polynomial in $k[X]$ then $h(\sigma_1(A), \cdots, \sigma_n(A)) \in k$ for all $A \in K$. We consider the mapping

$$A \longrightarrow \sigma_1(A) \cdots \sigma_n(A)$$

on K into k. This satisfies properties (1) and (2) of the last theorem. To show that it also satisfies the third property, we let $\omega_1, \cdots, \omega_n$ be a basis of K over k and let $A = \sum a_i \omega_i$ be an element of K, $a_i \in k$. Then

$$\sigma_1(A) \cdots \sigma_n(A) = \prod_{j=1}^{n} \left\{ \sum_{i=1}^{n} a_i \, \sigma_j(\omega_i) \right\} = f(a_1, \cdots, a_n)$$

where f is a form of degree n in $a_1, \cdots, a_n$ whose coefficients are, until we say more, in U. If k is infinite, one finds that these coefficients are in k from the fact that $f(a_1, \cdots, a_n) \in k$ for all vectors $(a_1, \cdots, a_n)$; when k is finite, then $K = k(B)$ is simple over k, and we may use $1, B, \cdots, B^{n-1}$ for a basis. Then the coefficients of f are symmetric in $\sigma_1(B), \cdots, \sigma_n(B)$, and hence are in k. At any rate we obtain

$$N_{K/k}(A) = \sigma_1(A) \cdots \sigma_n(A).$$

If $F(T) = \sum A_i T^i$, we set

$$F^{\sigma}(T) = \sum \sigma(A_i) T^i$$

and make the obvious extension to rational functions. A similar argument to that above implies that

$$h(R^{\sigma_1}(T), \cdots, R^{\sigma_n}(T)) \in k(T)$$

when $h(X)$ is symmetric in $X = (X_1, \cdots, X_n)$, $h(X) \in k[X]$, and $R(T) \in K(T)$. It follows that the formula for the norm as a product (of conjugates) is also valid in $K(T)$ over $k(T)$, hence in particular

$$f_{A,K/k}(T) = (T - \sigma_1(A)) \cdots (T - \sigma_n(A)),$$

and by comparing the second coefficients,

$$S_{K/k} = \sigma_1(A) + \cdots + \sigma_n(A).$$

References

1. A. A. Albert, *Modern higher algebra*, Chicago (1937).

2. N. Bourbaki, *Algèbre*, Chapitre V, Corps commutatifs, Paris (1950).

3. H. Flanders, *Norm function of an algebraic field extension*, Pacific J. Math. **3** (1953), 103-113.

4. H. Weyl, *Algebraic theory of numbers*, Princeton (1940).

THE UNIVERSITY OF CALIFORNIA, BERKELEY