PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 40, Number 1, September 1973

A LIFTING FORMULA FOR THE HILBERT SYMBOL

EDWARD A. BENDER

ABSTRACT. The Hilbert symbol in an extension field is expressed in terms of norms, traces and Hilbert symbols in the ground field.

1. **Introduction.** We use the terminology of O'Meara's book [2]. Let $(\cdot, \cdot)_L$ and $S_L(\cdot)$ denote the Hilbert and Hasse symbols over a local field L. The lifting formula is

THEOREM 1. *Let K be an extension of the local field k. For $\lambda \in K$ define the matrix $A(\lambda)$ by $a_{ij}(\lambda)=\mathrm{tr}_{K/k}\lambda\alpha_i\alpha_j$ where $\boldsymbol{\alpha}$ is a basis for K over k. Then*

$$(1) \qquad (\lambda, \mu)_K = S_k(A(1))S_k(A(\lambda))S_k(A(\mu))S_k(A(\lambda\mu))(N_{K/k}\lambda, N_{K/k}\mu)_k.$$

COROLLARY. *Suppose $b, c \in k$, then*

$$(\lambda, b)_K = (N_{K/k}\lambda, b)_k$$

and

$$(b, c)_K = (b, c)_k, \qquad [K:k] \text{ odd},$$
$$= +1, \qquad [K:k] \text{ even}.$$

When k is dyadic the theorem provides a method for computing Hilbert symbols over K such that the amount of work is bounded by a polynomial in $[K:k]$. The work involved in a direct approach grows exponentially.

2. **The proof.** Let X be a symmetric matrix with entries in K. The determinant of X is written $|X|$ and the dimension of X is written $\dim X$. Let $A(X)$ be the matrix obtained by replacing x_{ij} with $A(x_{ij})$.

We will deduce Theorem 1 from

THEOREM 2. *Suppose X and Y are nonsingular symmetric matrices with entries in K such that $\dim X = \dim Y$ and $|X|/|Y|$ is a square in K. Then*

$$(2) \qquad S_K(X)S_K(Y) = S_k(A(X))S_k(A(Y)).$$

Received by the editors November 9, 1972.
AMS (MOS) subject classifications (1970). Primary 10C05, 10C20.

We first prove Theorem 1. It is easily seen that

$$
\begin{aligned}
&\text{(a)} && (\lambda, \mu)_K = S_K(1 \oplus \lambda\mu) S_K(\lambda \oplus \mu), \\
(3)\quad &\text{(b)} && S_k(A(\beta \oplus \gamma)) = S_k(A(\beta)) S_k(A(\gamma))(|A(\beta)|, |A(\gamma)|), \\
&\text{(c)} && |A(\beta)| = |A(1)|\, N_{K/k}\beta.
\end{aligned}
$$

Using these observations it is easy to deduce Theorem 1 from Theorem 2. The corollary follows easily from (1), (3) (c) and $A(b\beta)=bA(\beta)$.

The rest of this paper is devoted to a proof of Theorem 2.

Suppose that V and W are symmetric matrices with entries in K and that V and W are "congruent" over K (i.e., $TVT^t=W$ for some matrix T with entries in K). We will show that $A(V)$ and $A(W)$ are congruent over k. Thus it will be possible to replace a matrix by a congruent one at any time. In particular the choice of the basis $\boldsymbol{\alpha}$ is irrelevant. By assumption $w_{ij}=\sum \tau_{im} v_{mn} \tau_{jn}$ for some $\tau_{ij} \in K$. (It is understood throughout that we sum over repeated indices.) Write $\tau_{ij}=\sum t_{ij}^m \alpha_m$ and $\alpha_i \alpha_j = \sum a_{ij}^m \alpha_m$ where $t_{ij}^m, a_{ij}^m \in k$. Since

$$
\mathrm{tr}_{K/k} \alpha_i w_{mn} \alpha_j = \sum d_{im}^{ps} (\mathrm{tr}_{K/k} \alpha_p v_{su} \alpha_q) d_{jn}^{qu}
$$

where $d_{im}^{ps}=\sum t_{ms}^j a_{ij}^p$, the claim follows.

If $S_K(X)=S_K(Y)$, then X and Y are congruent over K. By the previous paragraph (2) holds.

Suppose $|X|=\lambda$ and X and Y are not congruent over K. Define

$$
\begin{aligned}
M_1 &= I_2 \oplus -I_2 = I_2 \otimes (-1 \oplus 1), \\
M_2 &= M_2(K) = (-\Delta \oplus 1) \otimes (-\Pi \oplus 1)
\end{aligned}
$$

where I_2 is the 2 dimensional identity matrix, Π is any prime of K, and Δ is any unit of quadratic defect $4\mathfrak{o}$ in K. By [2, 63:11a], $S_K(M_1)S_K(M_2)=-1$. Hence $X \oplus I_5$ and $Y \oplus I_5$ are congruent over K to $\lambda \oplus I_n \oplus M_1$ and $\lambda \oplus I_n \oplus M_2$ in some order where $n=\dim X$. Since $|X|/|Y|$ is a square in K, it follows easily from (3) (c) that $|A(X)|/|A(Y)|$ is a square in k. By some simple calculations

$$
\begin{aligned}
S_k(A(X)) S_k(A(Y)) &= S_k(A(X \oplus I_5)) S_k(A(Y \oplus I_5)) \\
&= S_k(A(M_1)) S_k(A(M_2)).
\end{aligned}
$$

Therefore (2) holds in general if it holds for $X=M_1$, $Y=M_2$.

We may regard the theorem as a statement about K/k. Suppose Theorem 2 holds for K/L and for L/k. We will show that it holds for K/k. To distinguish the fields involved, write $A(\lambda; K/k)$ for the $A(\lambda)$ defined in

Theorem 1. We must show that

$$(4)\qquad \begin{aligned} &\text{(a)}\quad S_L(A(M_1; K/L)) \neq S_L(A(M_2(K); K/L)),\\ &\text{(b)}\quad S_k(A(M_1; L/k)) \neq S_k(A(M_2(L); L/k)) \end{aligned}$$

together imply

$$(5)\qquad S_k(A(A(M_1; K/L); L/k)) \neq S_k(A(A(M_2(K); K/L); L/k)).$$

Note that $|A(M_i; K/L)|$ is a square. By (4) (a), $A(M_1; K/L)$ and $A(M_2(K); K/L)$ are congruent over L to $I \oplus M_1$ and $I \oplus M_2(L)$ in some order. Equation (5) follows from (4) (b).

By the previous paragraph we need only prove the theorem for pure ramified and pure inertial extensions. In this case we may take one of Δ and Π to be in k. Call it γ and call the other Γ. Then

$$A(M_1) = A(-1 \oplus 1) \otimes I_2, \qquad A(M_2) = A(-\Gamma \oplus 1) \otimes (-\gamma \oplus 1).$$

After a little computation

$$S_k(A(M_1)) = (-1, (-1)^m)_k, \qquad S_k(A(M_2)) = (-1, (-1)^m)_k(\gamma, N_{K/k}\Gamma)_k$$

where $m = [K:k]$. It suffices to show that $(\gamma, N_{K/k}\Gamma)_k = -1$.

We will show that γ and $N_{K/k}\Gamma$ equal δ and π in some order where δ is a unit of quadratic defect $4\mathfrak{o}$ in k and π is a prime of k. By [2, 63:11a] this completes the proof. If K/k is pure ramified, $\Gamma = \Pi$ and $N_{K/k}\Pi$ is a prime of k. If K/k is pure inertial, we can choose $\delta \in k$ and $\Delta \in K$ such that $\delta \equiv \Delta \equiv 1 \pmod 4$, δ has quadratic defect $4\mathfrak{o}$ in k, and $N_{K/k}\Delta = \delta$ (see [1, p. 129]). Since δ is not a square, neither is Δ. Hence Δ has quadratic defect $4\mathfrak{o}$ in K.

References

1. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967. MR **38** #5742.

2. O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der math. Wissenschaften, Band 117, Academic Press, New York; Springer-Verlag, Berlin, 1963. MR **27** #2485.

Institute for Defense Analyses, Princeton, New Jersey 08540