

Pacific Journal of Mathematics

MULTIPLICATIVITY OF THE LOCAL HILBERT SYMBOL

RONALD JACOBOWITZ

MULTIPLICATIVITY OF THE LOCAL HILBERT SYMBOL

RONALD JACOBOWITZ

1. Introduction. Let F be a commutative field of characteristic not 2, complete under a discrete, non-archimedean valuation $|\cdot|$, with finite residue class field—such a field is often called *local*—for example, the field of ordinary p -adic numbers. For nonzero elements α, β of F , the *Hilbert symbol* (α, β) is defined to be $+1$ or -1 according as the equation $\alpha x^2 + \beta y^2 = 1$ is or is not solvable in F . It has such obvious properties as $(\beta, \alpha) = (\alpha, \beta)$, $(\alpha, \beta\gamma^2) = (\alpha, \beta)$, $(\alpha, -\alpha\beta) = (\alpha, \beta)$; and if at least one of (α, β) , (α, γ) is $+1$, then

$$(1) \quad (\alpha, \beta)(\alpha, \gamma) = (\alpha, \beta\gamma),$$

as is easily seen by observing (whether or not $\alpha \in F^2$)

$$(2) \quad (\alpha, \beta) = +1 \text{ if and only if } \beta \in N_{E/F}E, \text{ where } E = F(\alpha^{1/2}).$$

These properties are true even without the assumption that F is local; under that assumption, however, the multiplicative property (1) is *always* true, i.e., $(\alpha, \beta) = (\alpha, \gamma) = -1 \Rightarrow (\alpha, \beta\gamma) = +1$. In [3], Example 63:12, O'Meara derives this result from the study of local quaternion algebras by applying Wedderburn structure theory to tensor products of such algebras. The point of the present paper is to give a direct proof, using only the most elementary facts about non-archimedean valuations (such as found in [3], Chap. I). Specifically, we shall prove the so-called "second inequality of local class field theory" for quadratic extensions, i.e., $(F^* : N_{E/F}E^*) \leq 2$, where E is an arbitrary quadratic extension of F , and F^* and E^* denote, respectively, the nonzero elements of F and E ; the required property (1) will then follow immediately, because of (2).

2. Proof of the second inequality. Since the ramification number of E/F is at most 2 ([3], Proposition 13:6), an obvious computation shows that it suffices to prove the

PROPOSITION.

$$\begin{cases} (u : N_{E/F}\mathfrak{U}) = 1 & \text{if } E/F \text{ is unramified} \\ (u : N_{E/F}\mathfrak{U}) \leq 2 & \text{if } E/F \text{ is ramified,} \end{cases}$$

where $\mathfrak{u} = \{\varepsilon \in F \mid |\varepsilon| = 1\}$ and $\mathfrak{U} = \{a \in E \mid |a| = 1\}$, the units of F and E , respectively.

The proof of the Proposition will be broken up into several steps. First, let π denote a generic prime element (to be specified later) for F , and for each positive rational integer n , define $u_n = \{\varepsilon \in u \mid \varepsilon \equiv 1 \pmod{\pi^n}\}$, a subgroup of u . Also define the nonnegative integer e by $|\pi|^e = |2|$; thus $e = 0$ in the non-dyadic case ($|2| = 1$), $e > 0$ in the dyadic case ($|2| < 1$). We obviously have $u \supseteq u_1 \supseteq u_2 \supseteq \dots \supseteq u_{2^e} \supseteq u_{2^{e+1}} \supseteq \dots$. Furthermore, by Hensel's lemma ([3], Theorem 63:1), $u_{2^{e+1}} \subseteq u^2 \subseteq N\mathcal{U}$ (notation: $N = N_{E/F}$), thus we can write $u \supseteq u_1 N\mathcal{U} \supseteq u_2 N\mathcal{U} \supseteq \dots \supseteq u_{2^e} N\mathcal{U} \supseteq u_{2^{e+1}} N\mathcal{U} = N\mathcal{U}$; since group-indices multiply, we therefore have

LEMMA 1. $(u : N\mathcal{U}) =$
 $(u : u_1 N\mathcal{U})(u_1 N\mathcal{U} : u_2 N\mathcal{U}) \dots (u_{2^{e-1}} N\mathcal{U} : u_{2^e} N\mathcal{U})(u_{2^e} N\mathcal{U} : u_{2^{e+1}} N\mathcal{U}) .$

We next refer to [2], § 5, for a classification of the several types of extensions E/F , namely:

Non-dyadic: *Unramified* if $E = F(\theta^{1/2})$ with $|\theta| = 1$
 Ramified if $E = F(\pi^{1/2})$

Dyadic: *Unramified* if $E = F((1 + 4\delta)^{1/2})$ with $|\delta| = 1$
 Ramified ("R-P") if $E = F(\pi^{1/2})$
 Ramified ("R-U") if $E = F((1 + \pi^{2k+1}\delta)^{1/2})$ with
 $|\delta| = 1$ and $0 \leq k \leq e - 1$.

Here π , of course, denotes some *particular* prime element for F . In the case we are calling "R-U", recall from [2], p. 454, that $p = [1 + (1 + \pi^{2k+1}\delta)^{1/2}]/\pi^k$ satisfies $Np = -\pi\delta$ and hence can (and shall) serve as prime element for E ; and in "R-P", we shall take $p = \pi^{1/2}$ as prime element for E . Let us also write $\mathfrak{o} = \{\alpha \in F \mid |\alpha| \leq 1\}$, the "integers" of F .

LEMMA 2.

$$\begin{cases} (u : u_1 N\mathcal{U}) = 1 & \text{in the unramified non-dyadic, and} \\ & \text{the three dyadic cases;} \\ (u : u_1 N\mathcal{U}) \leq 2 & \text{in the ramified non-dyadic case.} \end{cases}$$

Proof. The composite map $u \xrightarrow{\text{CAN}} \mathfrak{F}^* \xrightarrow{\text{CAN}} \mathfrak{F}^*/\mathfrak{F}^{*2}$, \mathfrak{F} denoting the residue class field of F , is a multiplicative epimorphism with kernel $u_1 u^2$, so $(u : u_1 N\mathcal{U}) \leq (u : u_1 u^2) =$ order of $\mathfrak{F}^*/\mathfrak{F}^{*2}$; since \mathfrak{F} is finite, this order is 1 in the dyadic case, 2 in the non-dyadic. This proves the Lemma except in the unramified non-dyadic case, where we need a sharper estimate; however, in that case, we can apply Proposition

62:1 of [3] (which shows that for any unit ε of F , the congruence $\varepsilon x^2 + \theta y^2 \equiv 1 \pmod{\pi}$ can be solved in \mathfrak{o}) and Hensel's lemma to conclude that the Hilbert symbol (ε, θ) is equal to $+1$ for all ε in \mathfrak{u} , hence $\mathfrak{u} = N\mathfrak{u}$.

LEMMA 3. *Suppose E/F is dyadic. Then $(\mathfrak{u}_n N\mathfrak{u} : \mathfrak{u}_{n+1} N\mathfrak{u}) = 1$ in the following cases: Unramified: $1 \leq n \leq 2e$*

R-P: $1 \leq n \leq 2e - 1$

R-U: $1 \leq n \leq 2(e - k) - 2$ and $2(e - k) \leq n \leq 2e$.

Proof. Our procedure will be, given $\varepsilon = 1 + \pi^n \alpha$ in \mathfrak{u}_n (thus with $\alpha \in \mathfrak{o}$), to construct a in \mathfrak{u} with $\varepsilon \equiv Na \pmod{\pi^{n+1}}$, thus $\varepsilon/Na \in \mathfrak{u}_{n+1}$, thus $\varepsilon \in \mathfrak{u}_{n+1} N\mathfrak{u}$; this will show $\mathfrak{u}_n \subseteq \mathfrak{u}_{n+1} N\mathfrak{u}$, hence $\mathfrak{u}_n N\mathfrak{u} = \mathfrak{u}_{n+1} N\mathfrak{u}$. We consider five cases (note that II and V overlap, which simply means that either construction will work).

(I) Unramified. Take $a = 1 + \pi^n \alpha(1 + (1 + 4\delta)^{1/2})/2$.

(II) *R-P* or *R-U*, $n = 2r$ even, $1 \leq r \leq e - 1$. Recalling that \mathfrak{F} is finite of characteristic 2, find $\beta \in \mathfrak{o}$ with $\beta^2 \equiv \alpha \pmod{\pi}$, and take $a = 1 + \pi^r \beta$.

(III) *R-P*, $n = 2r + 1$ odd, $0 \leq r \leq e - 1$. Find $\beta \in \mathfrak{o}$ with $\beta^2 \equiv -\alpha \pmod{\pi}$, and take $a = 1 + p\pi^r \beta$.

(IV) *R-U*, $n = 2r + 1$ odd, $0 \leq r \leq e - k - 2$. Find $\beta \in \mathfrak{o}$ with $\beta^2 \equiv -\alpha/\delta \pmod{\pi}$, and take $a = 1 + p\pi^r \beta$.

(V) *R-U*, $n \geq 2(e - k)$. Take $a = 1 + p\pi^{n+k} \alpha/2$. We check in each case that a belongs to \mathfrak{u} and $\varepsilon \equiv Na \pmod{\pi^{n+1}}$.

For the remaining two indices, we have

LEMMA 4. *In R-P, $(\mathfrak{u}_{2e} N\mathfrak{u} : \mathfrak{u}_{2e+1} N\mathfrak{u}) \leq 2$; in R-U, $(\mathfrak{u}_{2(e-k)-1} N\mathfrak{u} : \mathfrak{u}_{2(e-k)} N\mathfrak{u}) \leq 2$.*

Proof. The first of the two inequalities is easily disposed of by Proposition 63:4 of [3], which essentially states that $(\mathfrak{u}_{2e} : \mathfrak{u}_{2e+1}) = 2$, so we turn to the second. Note that (for β in \mathfrak{o}) $N(1 + p\pi^{e-k-1} \beta) = 1 + \pi^{2(e-k)-1} (2\pi^{-e} \beta - \delta \beta^2)$, and set $\mathfrak{N} = \{N(1 + p\pi^{e-k-1} \beta) \mid \beta \in \mathfrak{o}\}$. Now we may assume $\mathfrak{u}_{2(e-k)-1}$ is not a subset of $\mathfrak{u}_{2(e-k)} N\mathfrak{u}$, and so can fix $\varepsilon_0 = 1 + \pi^{2(e-k)-1} \alpha_0$ in $\mathfrak{u}_{2(e-k)-1}$ but not in $\mathfrak{u}_{2(e-k)} N\mathfrak{u}$, hence with $\varepsilon_0 \notin \mathfrak{N}$, hence with α_0 not of the form $2\pi^{-e} \beta - \delta \beta^2$; then for any $\varepsilon = 1 + \pi^{2(e-k)-1} \alpha$ in $\mathfrak{u}_{2(e-k)-1}$ but not in $\mathfrak{u}_{2(e-k)} N\mathfrak{u}$, we also have α not of

the form $2\pi^{-e}\beta - \delta\beta^2$, and since, reading modulo π , elements of the form $2\pi^{-e}\beta - \delta\beta^2$ determine an additive subgroup of \mathfrak{o} of index 2, we can find β_1 in \mathfrak{o} with $\alpha + \alpha_0 \equiv 2\pi^{-e}\beta_1 - \delta\beta_1^2 \pmod{\pi}$, so that $\varepsilon\varepsilon_0 \equiv N(1 + p\pi^{e-k-1}\beta_1) \pmod{\pi^{2(e-k)}}$, i.e., $\varepsilon \in \varepsilon_0 u_{2(e-k)} N\mathfrak{U}$; thus the index $(u_{2(e-k)-1} N\mathfrak{U} : u_{2(e-k)} N\mathfrak{U})$ is at most 2. q.e.d.

The proof of the Proposition, and thus the multiplicative property (1), now follows by combining the four Lemmas.

3. Concluding remarks. The “first inequality of local class field theory” states $(F^* : NE^*) \geq 2$, and can also be proven directly—cf. [3], Propositions 63:13 and 63:13a. Its significance for us is that each of our index-inequalities in the Proposition and Lemmas 2 and 4 is now seen to be an equality.

As Durfee has shown in [1], the local isometry invariants for quadratic forms can easily be derived once our multiplicative property is known. Similarly, in the more modern, “geometric” treatment given in [3], § 58, § 63, it is not difficult to reinterpret O’Meara’s quaternion algebra (α, β) as a Hilbert symbol, tensor product \otimes as ordinary multiplication, and algebra-similarity \sim as equality; most of the arithmetic results of [3] then follow readily from the multiplicative property (1) and the Hasse theorem that any form in five variables is locally isotropic.

REFERENCES

1. W. H. Durfee, *Quadratic forms over fields with a valuation*, Bull. Amer. Math. Soc., **54** (1948), 338–351.
2. R. Jacobowitz, *Hermitian forms over local fields*, Amer. Jour. Math., **84** (1962), 441–465.
3. O. T. O’Meara, *Introduction to Quadratic Forms*, Berlin, 1963.

THE UNIVERSITY OF ARIZONA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

ROBERT OSSERMAN
Stanford University
Stanford, California

M. G. ARSOVE
University of Washington
Seattle 5, Washington

J. DUGUNDJI
University of Southern California
Los Angeles 7, California

LOWELL J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Richard Arens, <i>Normal form for a Pfaffian</i>	1
Charles Vernon Coffman, <i>Non-linear differential equations on cones in Banach spaces</i>	9
Ralph DeMarr, <i>Order convergence in linear topological spaces</i>	17
Peter Larkin Duren, <i>On the spectrum of a Toeplitz operator</i>	21
Robert E. Edwards, <i>Endomorphisms of function-spaces which leave stable all translation-invariant manifolds</i>	31
Erik Maurice Ellentuck, <i>Infinite products of isolos</i>	49
William James Firey, <i>Some applications of means of convex bodies</i>	53
Haim Gaifman, <i>Concerning measures on Boolean algebras</i>	61
Richard Carl Gilbert, <i>Extremal spectral functions of a symmetric operator</i>	75
Ronald Lewis Graham, <i>On finite sums of reciprocals of distinct nth powers</i>	85
Hwa Suk Hahn, <i>On the relative growth of differences of partition functions</i>	93
Isidore Isaac Hirschman, Jr., <i>Extreme eigen values of Toeplitz forms associated with Jacobi polynomials</i>	107
Chen-jung Hsu, <i>Remarks on certain almost product spaces</i>	163
George Seth Innis, Jr., <i>Some reproducing kernels for the unit disk</i>	177
Ronald Jacobowitz, <i>Multiplicativity of the local Hilbert symbol</i>	187
Paul Joseph Kelly, <i>On some mappings related to graphs</i>	191
William A. Kirk, <i>On curvature of a metric space at a point</i>	195
G. J. Kurowski, <i>On the convergence of semi-discrete analytic functions</i>	199
Richard George Laatsch, <i>Extensions of subadditive functions</i>	209
V. Marić, <i>On some properties of solutions of $\Delta\psi + A(r^2)X\nabla\psi + C(r^2)\psi = 0$</i> ...	217
William H. Mills, <i>Polynomials with minimal value sets</i>	225
George James Minty, Jr., <i>On the monotonicity of the gradient of a convex function</i>	243
George James Minty, Jr., <i>On the solvability of nonlinear functional equations of 'monotonic' type</i>	249
J. B. Muskat, <i>On the solvability of $x^e \equiv e \pmod{p}$</i>	257
Zeev Nehari, <i>On an inequality of P. R. Bessack</i>	261
Raymond Moos Redheffer and Ernst Gabor Straus, <i>Degenerate elliptic equations</i>	265
Abraham Robinson, <i>On generalized limits and linear functionals</i>	269
Bernard W. Roos, <i>On a class of singular second order differential equations with a non linear parameter</i>	285
Tôru Saitô, <i>Ordered completely regular semigroups</i>	295
Edward Silverman, <i>A problem of least area</i>	309
Robert C. Sine, <i>Spectral decomposition of a class of operators</i>	333
Jonathan Dean Swift, <i>Chains and graphs of Ostrom planes</i>	353
John Griggs Thompson, <i>2-signalizers of finite groups</i>	363
Harold Widom, <i>On the spectrum of a Toeplitz operator</i>	365