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 $|\ |$, 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

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

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., $(\alpha, \beta) = (\alpha, \gamma) = -1 \Rightarrow (a, \beta\gamma) = +1$. 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., $(F^* : N_{E/F}E^*) \leqq 2$, 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.

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

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.*

Received February 27, 1963.

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 $\mathfrak{u}_n = \{\varepsilon \in \mathfrak{u} \mid \varepsilon \equiv 1 \pmod{\pi^n}\}$, a subgroup of $\mathfrak{u}$. 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 $\mathfrak{u} \supseteqq \mathfrak{u}_1 \supseteqq \mathfrak{u}_2 \supseteqq \cdots \supseteqq \mathfrak{u}_{2e} \supseteqq \mathfrak{u}_{2e+1} \supseteqq \cdots$ Furthermore, by Hensel's lemma ([3], Theorem 63:1), $\mathfrak{u}_{2e+1} \subseteqq \mathfrak{u}^2 \subseteqq N\mathfrak{U}$ (notation: $N = N_{E/F}$), thus we can write $\mathfrak{u} \supseteqq \mathfrak{u}_1 N\mathfrak{U} \supseteqq \mathfrak{u}_2 N\mathfrak{U} \supseteqq \cdots \supseteqq \mathfrak{u}_{2e} N\mathfrak{U} \supseteqq \mathfrak{u}_{2e+1} N\mathfrak{U} = N\mathfrak{U}$; since group-indices multiply, we therefore have

LEMMA 1. $(\mathfrak{u} : N\mathfrak{U}) =$
$$(\mathfrak{u} : \mathfrak{u}_1 N\mathfrak{U})(\mathfrak{u}_1 N\mathfrak{U} : \mathfrak{u}_2 N\mathfrak{U}) \cdots (\mathfrak{u}_{2e-1} N\mathfrak{U} : \mathfrak{u}_{2e} N\mathfrak{U})(\mathfrak{u}_{2e} N\mathfrak{U} : \mathfrak{u}_{2e+1} N\mathfrak{U}) .$$

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 $0 \leqq k \leqq e - 1$.

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 $\mathfrak{o} = \{\alpha \in F \mid |\alpha| \leqq 1\}$, the "integers" of F.

LEMMA 2.
$$\begin{cases} (\mathfrak{u} : \mathfrak{u}_1 N\mathfrak{U}) = 1 & \textit{in the unramified non-dyadic, and the three dyadic cases;} \\ (\mathfrak{u} : \mathfrak{u}_1 N\mathfrak{U}) \leqq 2 & \textit{in the ramified non-dyadic case .} \end{cases}$$

Proof. The composite map $\mathfrak{u} \xrightarrow[\text{CAN}]{} \mathfrak{F}^* \xrightarrow[\text{CAN}]{} \mathfrak{F}^*/\mathfrak{F}^{*2}$, $\mathfrak{F}$ denoting the residue class field of F, is a multiplicative epimorphism with kernel $\mathfrak{u}_1\mathfrak{u}^2$, so $(\mathfrak{u} : \mathfrak{u}_1 N\mathfrak{U}) \leqq (\mathfrak{u} : \mathfrak{u}_1\mathfrak{u}^2) =$ 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: $1 \leqq n \leqq 2e$*

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

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

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 $\mathfrak{u}_n \subseteqq \mathfrak{u}_{n+1} N\mathfrak{U}$, 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, $1 \leqq r \leqq e - 1$. 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, $0 \leqq r \leqq e - 1$. 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, $0 \leqq r \leqq e - k - 2$. Find $\beta \in \mathfrak{o}$ with $\beta^2 \equiv -\alpha/\delta \pmod{\pi}$, and take $a = 1 + p\pi^r \beta$.

(V) *R-U*, $n \geqq 2(e - k)$. 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, $(\mathfrak{u}_{2e} N\mathfrak{U} : \mathfrak{u}_{2e+1} N\mathfrak{U}) \leqq 2$; in R-U, $(\mathfrak{u}_{2(e-k)-1} N\mathfrak{U} : \mathfrak{u}_{2(e-k)} N\mathfrak{U}) \leqq 2$.*

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 $\alpha + \alpha_0 \equiv 2\pi^{-e}\beta_1 - \delta\beta_1^2 (\operatorname{mod} \pi)$, so that $\varepsilon\varepsilon_0 \equiv N(1 + p\pi^{e-k-1}\beta_1)(\operatorname{mod} \pi^{2(e-k)})$, i.e., $\varepsilon \in \varepsilon_0\mathfrak{u}_{2(e-k)}N\mathfrak{U}$; thus the index $(\mathfrak{u}_{2(e-k)-1}N\mathfrak{U} : \mathfrak{u}_{2(e-k)}N\mathfrak{U})$ 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 $(F^* : NE^*) \geqq 2$, 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