A RECIPROCITY LAW FOR MAXIMAL FIELDS

BY

LADNOR GEISSINGER

Introduction. Local class field theory at first was concerned with the abelian extensions of fields which are complete with respect to a non-Archimedean discrete rank one valuation and which have a finite residue class field. Moriya, Nakayama, Schilling [4] and Whaples [6], [9] generalized this theory, allowing the residue class field to be quasifinite, that is, perfect and having for each positive integer n a unique extension of degree n. The condition on the group of values was also relaxed somewhat to include infinite algebraic extensions of such generalized local fields, where the value group need not be infinite cyclic, though it is still of rank one. The purpose of this paper is to show that the reciprocity law holds for a certain class of complete fields with valuations of arbitrary rank.

The fields we consider are assumed to be maximal (maximally complete) [3, p. 80], [4, p. 36] with respect to a non-Archimedean valuation. The (multiplicative) value group V will be assumed to satisfy the condition $(V : V^n) = n$ and the residue class field will be essentially quasifinite. Under these conditions we show that there exists a norm residue symbol for abelian extensions which gives the reciprocity law, including the norm transfer and isomorphism transfer properties. The general approach is that of Whaples [1], [6], [9].

The norm index. For a valuation on a field k, $|c|$ will denote the value of an element c, $|k|$ will denote the (multiplicative) value group, and $O(c)$ and $o(c)$ will denote elements of k for which $|O(c)| \leq |c|$ and $|o(c)| < |c|$. If K is an extension field of finite degree $[K : k]$ over k, $N_{K/k}$ or N and $S_{K/k}$ or S will denote the norm and trace functions respectively from K to k. We want to compute the index $(k^* : NK^*)$ of the group of norms NK^* in the multiplicative group k^* of k. First we consider the case when the residue class field $\mathfrak{k}$ has characteristic $p > 0$ and K/k is cyclic ramified of degree p. The following theorem contains some facts about orthobases and distortion constants which will be used in this case. The relevant definitions, proofs, and further results are in a paper of MacKenzie and Whaples [2].

THEOREM 1. *Suppose K/k cyclic ramified of degree p and p is the characteristic of* $\mathfrak{k}$. *Let A be any element of K such that $|A| \notin |k|$, σ a generator of the Galois group $G(K/k)$, and $\Gamma = (\sigma A - A)A^{-1}$. Then:*

1. $|\Gamma| < 1$ *and* $|\sigma B - B| \leq |\Gamma B|$ *for all $B \in K$.*

2. *Every B in K^* can be expressed uniquely as $B = b\Gamma + C$ with $b \in k$, $SC = 0$, and* $|C\Gamma^{-1}| \notin |k|$.

3. $|SB| \leq |B\Gamma^{-1} S\Gamma|$ *for all $B \in K$, and equality holds iff* $|B\Gamma^{-1}| \in |k|$.

With the aid of this theorem we make some simple computations. Since

$$1+\Gamma = (\sigma A)A^{-1}, \qquad N(1+\Gamma) = 1.$$

But by expanding

$$N(1+\Gamma) = 1+S\Gamma+E_2(\Gamma)+\cdots+E_{p-1}(\Gamma)+N\Gamma$$

where the $E_n(\Gamma)$ are symmetric functions of Γ and its conjugates. Since the Galois group $G(K/k)$ is prime cyclic, each of the $E_n(\Gamma)$ is a sum of traces of elements of the form $\prod_{i=1}^{n}\tau_i\Gamma$ where $\tau_i \in G(K/k)$. But $|\tau_i\Gamma|=|\Gamma|$ and so by 3 above,

$$|E_n(\Gamma)| \leqq |\Gamma^n\Gamma^{-1}S\Gamma| < |S\Gamma|$$

for $1<n<p$. Hence

$$1 = N(1+\Gamma) = 1+S\Gamma+N\Gamma+o(S\Gamma)$$

from which $|S\Gamma|=|N\Gamma|=|\Gamma^p|$ and $S\Gamma = -N\Gamma+o(N\Gamma)$.

The inequality in 3 now becomes $|SB|\leqq|B\Gamma^{p-1}|$ with equality iff $|B\Gamma^{-1}| \in |k|$. For any $B \in K$,

$$N(1+B) = 1+SB+E_2(B)+\cdots+E_{p-1}(B)+NB$$

and as above, $|E_n(B)|\leqq|B^n\Gamma^{p-1}|$. We consider separately three possibilities for $|B|$.

Case 1. Suppose $1>|B|>|\Gamma|$. Then $|B^n\Gamma^{p-1}|<|B^p|=|NB|$ for $0<n<p$. Hence

$$N(1+B) = 1+NB+o(NB).$$

Case 2. Suppose $|B|=|\Gamma|$. Again $|B^n\Gamma^{p-1}|<|B^p|=|NB|$ for $1<n<p$ so that

$$N(1+B) = 1+SB+NB+o(NB).$$

From 2 in Theorem 1, $B=b\Gamma+C$ with $b\in k$, $|b|=1$, $|C|<|B|$ and $SC=0$. Then $SB=bS\Gamma = -bN\Gamma+o(N\Gamma)$ and $B=b\Gamma(1+o(1))$ so $NB=b^pN\Gamma+o(N\Gamma)$. Hence

$$N(1+B) = N(1+b\Gamma+C) = 1+(b^p-b)N\Gamma+o(N\Gamma).$$

Case 3. Suppose $|B|<|\Gamma|$. $|B^n\Gamma^{p-1}|<|B\Gamma^{p-1}|$ for $1<n<p$, $|SB|\leqq|B\Gamma^{p-1}|$ and $|NB|=|B^p|<|B\Gamma^{p-1}|$. Thus

$$N(1+B) = 1+SB+o(B\Gamma^{p-1}).$$

If $|B\Gamma^{-1}| \in |k|$ then $|SB|=|B\Gamma^{p-1}|$ and so

$$N(1+B) = 1+SB+o(SB).$$

LEMMA 1. *Assume k is maximally complete and K/k and Γ are as in Theorem 1. Then $1+(N\Gamma)P_k=N(1+\Gamma P_K)$ where P_k, P_K are the maximal ideals of the valuation rings of k, K.*

Proof. By Case 3 $N(1 + \Gamma P_K) \subseteq 1 + (N\Gamma)P_k$. For the converse, let $a \in k$ such that $|a| < |N\Gamma|$, then $b = a(S\Gamma)^{-1} \in P_k$. By Case 3 $N(1 + b\Gamma) = 1 + bS\Gamma + o(bS\Gamma) = 1 + a + r_1$ with $|r_1| < |a|$. Again $c = -r_1(S\Gamma)^{-1} \in P_k$ so $N(1 + c\Gamma) = 1 - r_1 + o(r_1)$. Then $N(1 + b\Gamma)N(1 + c\Gamma) = (1 + a + r_1)(1 - r_1 + o(r_1)) = 1 + a + o(r_1)$. Set $B_1 = b$,

$$B_2 = b + c + bc\Gamma \quad \text{and} \quad N(1 + B_2\Gamma) = 1 + a + r_2.$$

Then $|B_1| > |a| > |r_1| > |r_2|$ and $|B_2 - B_1| = |c| = |r_1\Gamma^{-p}|$.

Now suppose $\{(B_i, r_i) : i < t\}$ is a sequence indexed by all ordinals less than some ordinal t, with $B_i \in K$, $r_i \in k$, $N(1 + B_i\Gamma) = 1 + a + r_i$, $|r_i| > |r_j|$ and $|B_j - B_i| = |r_i\Gamma^{-p}|$ if $i < j$, and (B_1, r_1) as given above. If t is not a limit ordinal and $r_{t-1} \neq 0$ set $d = -r_{t-1}(S\Gamma)^{-1}$, then $N(1 + d\Gamma) = 1 - r_{t-1} + o(r_{t-1})$. Let $B_t = B_{t-1} + d + dB_{t-1}\Gamma$, then as above $N(1 + B_t\Gamma) = 1 + a + r_t$ with $|r_t| < |r_{t-1}|$. Moreover

$$|B_t - B_{t-1}| = |d| = |r_{t-1}\Gamma^{-p}|$$

so $|B_t - B_i| = |r_i\Gamma^{-p}|$ for $i < t$ since $|r_{t-1}| < |r_i|$. So we can add (B_t, r_t) to the sequence and retain all the properties.

If t is a limit ordinal then $\{B_i \mid i < t\}$ is a pseudo-convergent sequence in K, for if $i < j < n < t$, $|B_j - B_i| = |r_i\Gamma^{-p}| > |r_j\Gamma^{-p}| = |B_n - B_j|$. Since k is maximally complete, K is also so there is a pseudo-limit of this sequence in K [4, Chapter 2]. That is, an element B_t in K such that $|B_t - B_i| = |B_j - B_i| = |r_i\Gamma^{-p}|$ for $i < j < t$. Let $C = (B_t - B_i)(1 + B_i\Gamma)^{-1}$, then $|C| = |r_i\Gamma^{-p}|$ so $N(1 + C\Gamma) = 1 + S(C\Gamma) + o(S(C\Gamma))$ and $|S(C\Gamma)| = |C\Gamma^p| = |r_i|$. Thus

$$N(1 + B_t\Gamma) = N(1 + B_i\Gamma)N(1 + C\Gamma) = (1 + a + r_i)(1 + S(C\Gamma) + o(r_i))$$

$$= 1 + a + r_i + S(C\Gamma) + o(r_i).$$

Let $N(1 + B_t\Gamma) = 1 + a + r_t$, then $|r_t - r_i| = |S(C\Gamma)| = |r_i|$ and since $|r_i| > |r_j|$ if $i < j$ then $|r_t| < |r_i|$ for all $i < t$. So again we could add (B_t, r_t) to the sequence and retain all the properties.

By Zorn's Lemma there is a maximal sequence among all such sequences. The preceding shows that for a maximal sequence $\{(B_i, r_i) : i < t\}$, t is not a limit ordinal and $r_{t-1} = 0$, which gives $N(1 + B_{t-1}\Gamma) = 1 + a$ and $|B_{t-1}| = |B_1| = |a(S\Gamma)^{-1}|$. Thus $1 + a \in N(1 + \Gamma P_k)$ and $1 + (N\Gamma)P_K \subseteq N(1 + \Gamma P_K)$ which completes the proof.

Let O_k, O_K be the valuation rings of k, K. By Cases 2 and 3 and Lemma 1,

$$1 + (N\Gamma)O_k \supseteq N(1 + \Gamma O_K) \supseteq 1 + (N\Gamma)P_k.$$

Also if $|B| = |\Gamma|$, then $B = b\Gamma + C$ with $b \in O_k$, $|b| = 1$, $SC = 0$ and

$$N(1 + B) = 1 + (b^p - b)N\Gamma + o(N\Gamma).$$

Let h be the homomorphism of the multiplicative group $1 + (N\Gamma)O_k$ onto the additive group $\mathfrak{k}$ given by $h(1 + (N\Gamma)u) = \mathfrak{u}$ where $\mathfrak{u}$ is the residue class of $u \in O_k$,

and let $\wp$ be the endomorphism of $\mathfrak{k}$ defined by $\wp(x) = x^p - x$. The kernel of h is $1 + (N\Gamma)P_k$ and the h-image of $N(1 + \Gamma O_K)$ is $\wp(\mathfrak{k})$, thus

$$(1 + (N\Gamma)O_k : N(1 + \Gamma O_K)) = (\mathfrak{k} : \wp(\mathfrak{k})).$$

LEMMA 2. *Assume k is maximally complete, characteristic $\mathfrak{k}$ is p, $(|k| : |k|^p) = p$, $\mathfrak{k}$ is perfect, and K/k, Γ are as in Theorem 1. Then $1 + P_k = (1 + (N\Gamma)O_k)N(1 + P_K)$.*

Proof. Let $a \in k$ with $1 > |a| > |N\Gamma|$. We must show that there exists a $B \in P_K$ and $c \in O_k$ such that $1 + a = (1 + cN\Gamma)N(1 + B)$. The condition $(|k| : |k|^p) = p$ is equivalent to $|K|^p = |k|$ so there is a $B \in P_K$ with $|a| = |B|^p = |NB|$. k being perfect means $\mathfrak{k}^p = \mathfrak{k}$ and since $a(NB)^{-1}$ is a unit of O_k there is a unit b of O_k such that b^p is in the residue class of $a(NB)^{-1}$. That is, $b^p = a(NB)^{-1} + o(1)$ or $a = b^p NB + o(NB)$. Since $1 > |bB| > |\Gamma|$, by Case 1

$$N(1 + bB) = 1 + b^p NB + o(NB) = 1 + a + o(a).$$

Thus we have an element $B_1 = bB$ for which $|B_1|^p = |a|$ and $N(1 + B_1) = 1 + a + r_1$ with $|r_1| < |a|$. If $|r_1| > |\Gamma|$ there exists as above a C such that $N(1 + C) = 1 - r_1 + o(r_1)$. Let $B_2 = B_1 + C + B_1 C$ and $N(1 + B_2) = 1 + a + r_2$, then $|r_2| < |r_1|$ and

$$|B_2 - B_1|^p = |C|^p = |r_1|.$$

Now suppose $\{(B_i, r_i) : i < t\}$ is a sequence with $B_i \in P_K$, $N(1 + B_i) = 1 + a + r_i$, and $|r_i| > |r_j|$, and $|B_i - B_j|^p = |r_i|$ if $i < j$. As in Lemma 1 one can show that if all $|r_i| > |N\Gamma|$ the sequence can be extended. Thus for a maximal sequence some $|r_i| \leq |N\Gamma|$, which means $N(1 + B_i) = 1 + a + r_i = (1 + a)(1 + cN\Gamma)$ with $c \in O_k$.

THEOREM 2. *Assume k is maximally complete, $(|k| : |k|^p) = p$, $\mathfrak{k}^p = \mathfrak{k}$, and K/k cyclic ramified of degree p where p is the characteristic of $\mathfrak{k}$. Then*

$$(k^* : NK^*) = (\mathfrak{k} : \wp(\mathfrak{k})).$$

Proof. Let a be any element of k^*. In the proof of Lemma 2 we showed that $a = (1 + o(1))NB = (1 + c)N(1 + D)NB$ with $c \in k$ and $|c| \leq |N\Gamma|$. Thus

$$k^* = (1 + (N\Gamma)O_k)NK^*.$$

From Case 1 and the fact that $\mathfrak{k}$ has no primitive pth root of 1 it follows that if $NB = 1 + O(N\Gamma)$ then $B = 1 + O(\Gamma)$. Thus $(1 + (N\Gamma)O_k) \cap NK^* = N(1 + \Gamma O_K)$. This and the computation following Lemma 1 gives

$$(k^* : NK^*) = (1 + (N\Gamma)O_k : N(1 + \Gamma O_K)) = (\mathfrak{k} : \wp(\mathfrak{k})).$$

Essentially the same method works for unramified extensions.

THEOREM 3. *Assume k is maximally complete, K/k unramified of degree n, and $\mathfrak{K}/\mathfrak{k}$ separable. Then $1 + P_k = N(1 + P_K)$ and $(k^* : NK^*) = (|k| : |k|^n)(\mathfrak{k}^* : N\mathfrak{K}^*)$. If $\mathfrak{k}^* = N\mathfrak{K}^*$ then $NK^* = k^{*n}k_0^*$ where k_0^* is the group of units of O_k.*

Proof. It is easy to see that the norm and trace on O_K/O_k induce the norm and trace on $\mathfrak{K}/\mathfrak{k}$. Since $\mathfrak{K}/\mathfrak{k}$ is separable there is an $\mathfrak{A} \in \mathfrak{K}$ such that $S\mathfrak{A} \neq 0$. Thus there is a unit A in K with $|SA| = 1$.

Now for any $a \in P_k$ if we let $b_1 = a(SA)^{-1}$ then $|b_1| = |a|$ and

$$N(1 + b_1 A) = 1 + b_1 SA + E_2(b_1 A) + \cdots + N(b_1 A).$$

Each of the $E_i(b_1 A)$ is a sum of products of i conjugates of $b_1 A$ so $|E_i(b_1 A)| \leq |b_1 A|^i$ and hence $N(1 + b_1 A) = 1 + b_1 SA + o(b_1) = 1 + a + r_1$ with $|r_1| < |a|$. Let $c = -r_1 (SA)^{-1}$ then $N(1 + cA) = 1 - r_1 + o(r_1)$. Now $1 + (b_1 + c)A = (1 + b_1 A)(1 + cA)(1 + O(b_1 c))$ from which

$$N(1 + (b_1 + c)A) = (1 + a + r_1)(1 - r_1 + o(r_1))(1 + O(b_1 c)).$$

Thus $N(1 + (b_1 + c)A) = 1 + a + o(r_1)$ and if we set $b_2 = b_1 + c$ and

$$N(1 + b_2 A) = 1 + a + r_2$$

then $|b_2 - b_1| = |r_1|$ and $|r_1| > |r_2|$. This is the beginning of an approximating sequence which yields as in Lemma 1 an element b such that $N(1 + bA) = 1 + a$.

For each $B \in K^*$ there is a $b \in k^*$ such that $|B| = |b|$ since K/k is unramified. $|NB| = |B|^n = |b|^n$ so $|NK^*| = |k|^n$ and $NK^* \cap k_0^* = NK_0^*$. Let h be the natural homomorphism of k_0^* onto $\mathfrak{k}^*$. The kernel of h is $1 + P_k$ which is contained in NK_0^* by the first half of this proof, and $h(NK_0^*) = N\mathfrak{K}^*$. We get the last result and the norm index

$$(k^* : NK^*) = (|k^*| : |k^*|^n)(k_0^* : NK_0^*)$$

$$= (|k^*| : |k^*|^n)(\mathfrak{k}^* : N\mathfrak{K}^*)$$

by two applications of the following proposition.

PROPOSITION 1. *Assume A is a group, B is a subgroup of A, and ϕ is a homomorphism of A. Then*

$$(A : B) = (\phi(A) : \phi(B))(\ker \phi : \ker \phi \cap B).$$

We shall also use Proposition 1 in the following form.

COROLLARY. *For any tower of fields $R \subset S \subset T$ with $[T : R]$ finite, $(R^* : N(T/R))$ divides $(R^* : N(S/R))(S^* : N(T/S))$.*

For $(R^* : N(T/R)) = (R^* : N(S/R))(N(S/R) : N(T/R))$, so applying Proposition 1 to $N_{S/R}$, $(N(S/R) : N(T/R))$ divides $(S^* : N(T/S))$ and the corollary follows.

For tamely ramified extensions the norms are easy to compute, even for more general kinds of fields [4, pp. 60–66]. We state here for reference the relevant results.

THEOREM 4. *Assume k is relatively complete (Henselian) and n is relatively prime* to the characteristic exponent of $\mathfrak{k}$. Then $(1 + P_k)^n = 1 + P_k$. If K/k has degree n and is totally ramified, it is a radical extension and*

$$(k^* : NK^*) = (1/n)(|k| : |k|^n)(\mathfrak{k}^* : \mathfrak{k}^{*n}).$$

Finally, suppose k is maximally complete and K/k is a finite Galois extension. By the Hilbert ramification theory [4, Chapter 3] there is a tower

$$k \subset U \subset T_1 \subset T_2 \subset \cdots \subset T_m = K$$

where U is the maximal unramified extension in K/k, T_1 is the maximal tamely ramified extension in K/U, and each T_{i+1}/T_i is cyclic ramified of degree the characteristic exponent of $\mathfrak{k}$. In the next section we will discuss conditions on $|k|$ and $\mathfrak{k}$ which guarantee that when Theorems 3, 4, 2 are applied to U/k, T_1/U, and T_{i+1}/T_i respectively, in each case the norm index equals the degree. By the corollary of Proposition 1 we may then conclude that $(k^* : NK^*)$ divides $[K : k]$.

The conditions on $|k|$ and $\mathfrak{k}$. Henceforth k will be a fixed maximally complete base field and all extensions of it are assumed to be in a fixed algebraic closure with its unique extension of the valuation on k. The remaining conditions on k can be stated most easily, without unduly restricting $|k|$, in terms of a collection of prime numbers. Let P be any set of primes and let D be the formal product of the p^∞ for all $p \in P$ with the natural definition of when an integer divides D. For each prime p in P we assume that $(|k| : |k|^p) = p$. Also, for each $p \in P$ we assume that if $\mathfrak{L}/\mathfrak{k}$ is finite then $\mathfrak{L}$ has a unique cyclic extension of degree p, if $p = 2$ then $\mathfrak{k}$ is not an ordered field in which every sum of squares is a square, and if p is the characteristic of $\mathfrak{k}$ then $\mathfrak{k}$ is perfect.

We list some of the consequences of the latter assumption [5], [7], [8], [9].

1. For each finite $\mathfrak{L}/\mathfrak{k}$ and each $n > 0$ there is a unique extension of $\mathfrak{L}$ of degree p^n, and it is cyclic.

2. If $[\mathfrak{M} : \mathfrak{L}] = p^n b$ with $(p, b) = 1$ then $\mathfrak{M}$ contains the p^n extension of $\mathfrak{L}$.

3. If $[\mathfrak{M} : \mathfrak{L}] = p$, then $N(\mathfrak{M}/\mathfrak{L}) = \mathfrak{L}^*$ and if p is not the characteristic then $(\mathfrak{L}^* : \mathfrak{L}^{*p}) = p$ whereas if p is the characteristic then $(\mathfrak{L} : \wp(\mathfrak{L})) = p$.

By taking composites over the primes in P one gets the following extensions of 1, 2, and 3.

4. For each finite $\mathfrak{L}/\mathfrak{k}$ and each $n | D$ there is a unique extension of $\mathfrak{L}$ of degree n, and it is cyclic.

5. If $[\mathfrak{M} : \mathfrak{L}] = nb$ with $n | D$ and $(D, b) = 1$, then $\mathfrak{M}$ contains the n extension of $\mathfrak{L}$.

6. If $[\mathfrak{M} : \mathfrak{L}] = n$ with $n | D$ then $N(\mathfrak{M}/\mathfrak{L}) = \mathfrak{L}^*$ and if n is relatively prime to the characteristic exponent then $(\mathfrak{L}^* : \mathfrak{L}^{*n}) = n$.

Now every finite K/k has a unique maximal unramified subextension, and the unramified extensions of K correspond uniquely to the extensions of $\mathfrak{K}$ [4]. Thus for each finite K/k and each $n | D$ there is a unique unramified extension $U_{K,n}$ of degree n over K, and it is cyclic. Let $U_{K,D}$ be the union of the $U_{K,n}$ for all $n | D$. From 5 above it is easy to see that these unramified extensions have the following important property.

7. If K/k is finite and $[\mathfrak{K} : \mathfrak{k}] = nb$ with $n | D$ and $(D, b) = 1$, then $K \cap U_{k,D} = U_{k,n}$ and for each $r | D$, $U_{K,r} = K U_{k,nr}$.

The next lemma provides us with the analogue of the classical Frobenius automorphism.

LEMMA 3. *There exists a family of automorphisms* $\{F_K\}$ *indexed by all finite* K/k *such that*:

A. $F_K \in G(U_{K,D}/K)$ *and* F_K *restricted to* $U_{K,n}$ *generates* $G(U_{K,n}/K)$ *for each* $n\,|\,D$.

B. *If* $K \subset L$ *and* $[\mathfrak{L} : \mathfrak{K}] = f$ *then* F_L *restricted to* $U_{K,D}$ *is* F_K^f.

C. *If* σ *is any automorphism of the algebraic closure which is identity on* k, *then* $F_{\sigma K} = \sigma F_K \sigma^{-1}$ *for each finite* K/k.

Proof. It is well known that in this situation each $G(U_{K,D}/K)$ is isomorphic to the topological product of the p-adic integers for all $p \in P$. So there is an automorphism F_k of $U_{k,D}/k$ which generates an infinite cyclic subgroup which is dense in $G(U_{k,D}/k)$; that is, A holds for F_k. Keeping this F_k fixed all the other F_K can be defined in a unique way such that A, B, and C hold. Namely, if $[\mathfrak{K} : \mathfrak{k}] = nb$ with $n\,|\,D$ and $(D, b) = 1$, then F_k^{nb} is identity on $K \cap U_{k,D} = U_{k,n}$ so there is a unique extension of it to an automorphism F_K of $U_{K,D} = KU_{k,D}$ which is identity on K. For each $r\,|\,D$, F_k^{nb} restricted to $U_{k,nr}$ generates $G(U_{k,nr}/U_{k,n})$ since $(nr, b) = 1$ and so F_K restricted to $U_{K,r} = KU_{k,nr}$ generates $G(U_{K,r}/K)$. It is easy to check that B and C also hold for these F_K.

We turn now to the value groups. Since the value group W of the algebraic closure is torsion-free and divisible, the condition $(|k| : |k|^p) = p$ is equivalent to saying that there is a unique subgroup S of W such that $(S : |k|) = p$, that is, $|k|$ has a unique p extension in W. This generalizes immediately to powers of p and then to products of the primes p in P. The result is that for each $n\,|\,D$, $|k|/|k|^n$ is cyclic of order n and the set of all nth roots of the elements of $|k|$ is the unique n extension of $|k|$ in W. It follows easily that for each finite K/k and each $r\,|\,D$, $(|K| : |K|^r) = r$ so that $|K|$ has the same properties as $|k|$. Moreover, if $(|K| : |k|) = nb$ with $n\,|\,D$ and $(D, b) = 1$, then $|K|$ contains the n extension of $|k|$ so that the r extension of $|K|$ is the composite of $|K|$ with the nr extension of $|k|$, and $|k| \cap |K|^{nr} = |k|^r$. Thus the system of Galois groups $G(U_{K,n}/K)$ with restriction maps is mirrored exactly in the system of value groups $|K|$ and subgroups $|K|^n$ with inclusion maps.

Let V_K be the inverse limit of the system of cyclic groups $|K|/|K|^n$ for all $n\,|\,D$ with the natural projection maps. The limit homomorphism maps $|K|$ onto a dense subgroup of V_K, for V_K is the Hausdorff completion of $|K|$ relative to the topology defined by the subgroups $|K|^n$ for all $n\,|\,D$, and the kernel of the homomorphism is the intersection of these subgroups. Since $|k| \cap |K|^{nr} = |k|^r$ when $(|K| : |k|) = nb$ with $n\,|\,D$, $(D, b) = 1$, and $r\,|\,D$, the inclusion $|k| \subset |K|$ yields a monomorphism of $|k|/|k|^r$ into $|K|/|K|^{nr}$. These maps for all $r\,|\,D$ induce a monomorphism of V_k into V_K and we shall identify V_k with its image in V_K. On the other hand, the map $x \to x^{nb}$ takes $|K|/|K|^r$ isomorphically onto $|k|/|k|^r$ for each $r\,|\,D$, so this map is also an isomorphism of V_K onto its subgroup V_k.

LEMMA 4. *There is a family $\{T_K\}$ indexed by all finite K/k such that*:

A. T_K *generates a subgroup which is dense in* V_K.

B. *If $K \subset L$ and $(|L| : |K|) = e$ then $T_L^e = T_K$.*

C. *If σ is any automorphism of the algebraic closure which is identity on k, then* $T_{\sigma K} = T_K$ *for each finite K/k.*

Proof. Let T_k be any element of V_k for which A holds. If K/k is finite with $(|K| : |k|) = d$ we have seen above that $V_K^d = V_k$ so there is a unique element T_K in V_K such that $T_K^d = T_k$. The T_K determined like this clearly satisfy A and B. For any σ as in C, by the uniqueness of the valuation on K and σK it follows that $|K| = |\sigma K|$ and so $V_K = V_{\sigma K}$ and $T_K = T_{\sigma K}$ by construction.

The norm residue symbol. Having chosen a family of automorphisms $\{F_K\}$ as in Lemma 3 and a family $\{T_K\}$ as in Lemma 4, the assignment $T_K \to F_K$ extends uniquely to an isomorphism of V_K onto $G(U_{K,D}/K)$ for each finite K/k by property A. Composing this isomorphism with the natural map of $|K|$ into V_K and the homomorphism $|\ |$ of K^* onto $|K|$ gives a homomorphism ϕ_K of K^* into $G(U_{K,D}/K)$. These ϕ_K give a norm residue symbol for the $U_{K,n}$.

THEOREM 5. *The homomorphisms ϕ_K of K^* into $G(U_{K,D}/K)$ have the following properties*:

1. (*Reciprocity*) *For each finite K/k and each $n|D$, ϕ_K followed by restriction induces the exact sequence*

$$1 \to N(U_{K,n}/K) \to K^* \to G(U_{K,n}/K) \to 1.$$

2. (*Norm Transfer*) *If $k \subset K \subset L$ with L/k finite, for each $E \in L^*$,*

$$\phi_K(N_{L/K}E) = \phi_L(E)$$

restricted to $U_{K,D}$.

3. (*Isomorphism Transfer*) *If σ is any automorphism of the algebraic closure which is identity on k, then $\phi_{\sigma K}(\sigma E) = \sigma \phi_K(E) \sigma^{-1}$ for each $E \in K^*$ and each finite K/k.*

Proof. $|K|$ maps onto a dense subgroup of V_K so ϕ_K maps K^* onto a dense subgroup of $G(U_{K,D}/K)$ which implies that ϕ_K followed by restriction to $U_{K,n}$ maps K^* onto the cyclic group $G(U_{K,n}/K)$. The kernel of this homomorphism is the subgroup of K^* which $|\ |$ takes onto $|K|^n$, that is, $K^{*n}K_0^*$. But by Theorem 3 and property 6 of the residue class fields, $K^{*n}K_0^*$ is $N(U_{K,n}/K)$ and so part 1 is proved. Part 2 results from the following commutative diagram.

$$
\begin{array}{ccccccc}
L^* & \longrightarrow & |L| & \longrightarrow & V_L & \longrightarrow & G(U_{L,D}/L) \\
{\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle ef} & & \downarrow{\scriptstyle ef} & & \downarrow \\
K^* & \longrightarrow & |K| & \longrightarrow & V_K & \longrightarrow & G(U_{K,D}/K)
\end{array}
\qquad \text{restriction}
$$

where $e = (|L| : |K|)$ and $f = [\mathfrak{L} : \mathfrak{K}]$. It is clear that the first square commutes and

we have previously shown that the second does also. The third commutes because $T_L^{ef} = T_K^f$ by B of Lemma 4 and F_L restricted to $U_{K,D}$ is F_K^f by B of Lemma 3. Part 3 comes from the fact that $|E| = |\sigma E|$ for all $E \in K^*$, $T_{\sigma K} = T_K$ by C of Lemma 4, and $F_{\sigma K} = \sigma F_K \sigma^{-1}$ by C of Lemma 3.

For each finite K/k let A_K be the composite of all the finite abelian extensions of K with degree dividing D. A_K is abelian over K and contains $U_{K,D}$. The ϕ_K can now be extended to give a norm residue symbol for all the fields in A_K.

THEOREM 6. *The ϕ_K extend uniquely to homomorphisms ψ_K of K^* into $G(A_K/K)$ with the following properties*:

1. (*Reciprocity*) *For all finite K/k and M/K with $M \subset A_K$, ψ_K followed by restriction induces the exact sequence*

$$1 \to N(M/K) \to K^* \to G(M/K) \to 1.$$

2. (*Norm Transfer*) *If $k \subset K \subset L$ with L/k finite, for each $E \in L^*$, $\psi_K(N_{L/K}E) = \psi_L(E)$ restricted to A_K.*

3. (*Isomorphism Transfer*) *If σ is any automorphism of the algebraic closure which is identity on k, then $\psi_{\sigma K}(\sigma E) = \sigma \psi_K(E)\sigma^{-1}$ for each $E \in K^*$ and each finite K/k.*

Proof. This result follows directly from Theorem 5 by means of a general theorem on extending a norm residue symbol [1]. We need only check that the following two sufficient conditions for the extension theorem are satisfied.

1. For all $k \subset K \subset L$ with L/k finite and each cyclic C/K with $C \subset A_K$, if $[CL : L] = r$ there is a cyclic Z/K with $Z \subset U_{K,D}$ such that $[ZL : L] = r$.

This condition is clearly satisfied, since if $L \cap U_{K,D} = U_{K,n}$ we may take $U_{K,nr}$ for Z.

2. For all $k \subset K \subset M$ with M/k finite and $M \subset A_K$, $(K^* : N(M/K)) \leqq [M : K]$.

The conditions we have imposed on $|k|$ and $\mathfrak{k}$ are sufficient to guarantee that for extensions of degree dividing D and of onè of the types in Theorems 2, 3, 4 the norm index equals the degree. So by the remarks following Theorem 4, condition 2 is satified. Thus Theorem 6 is proved.

We remark in conclusion that the most interesting situation is when $\mathfrak{k}$ has characteristic $p > 0$ and $p \in P$ because the structure of the abelian p^n extensions, the norm maps, and the norm groups are quite complicated in this case.

REFERENCES

1. K. Glass, R. Moore, and G. Whaples, *On extending a norm residue symbol*, Mimeographed notes.

2. R. MacKenzie and G. Whaples, *Artin-Schreier equations in characteristic zero*, Amer. J. Math. **78** (1956), 473–485.

3. P. Ribenboim, *Théorie des valuations*, Université de Montreal, Montreal, 1964.

4. O. F. G. Schilling, *The theory of valuations*, Math. Surveys No. 4, Amer. Math. Soc., Providence, R. I., 1950.

5. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

6. G. Whaples, *Generalized local class field theory*. I, II, Duke Math. J. **19** (1952), 505–517; ibid. **21** (1954), 247–255.

7. ———, *Galois cohomology of additive polynomial and nth power mappings of fields*, Duke Math. J. **24** (1957), 143–150.

8. ———, *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201–204.

9. ———, *Class field theory*, Mimeographed notes.

PURDUE UNIVERSITY,
    LAFAYETTE, INDIANA