THE INTERSECTION OF NORM GROUPS(1)

BY
JAMES AX

1. **Introduction.** Let Λ be a *global field* (either a finite extension of **Q** or a field of algebraic functions in one variable over a finite field) or a *local field* (a local completion of a global field). Let $C(\Lambda, n)$ (respectively: $A(\Lambda, n)$, $N(\Lambda, n)$ and $E(\Lambda, n)$) be the set of $\lambda \in \Lambda$ such that λ is the norm of every cyclic (respectively: abelian, normal and arbitrary) extension of Λ of degree n. We show that

$$(*) \qquad C(\Lambda, n) = A(\Lambda, n) = N(\Lambda, n) = E(\Lambda, n) = \Lambda^n$$

is "almost" true for any global or local field and any natural number n. For example, we prove (*) if Λ is a number field and $8 \nmid n$ or if Λ is a function field and n is arbitrary.

In the case when (*) is false we are still able to determine $C(\Lambda, n)$ precisely. It then turns out that there is a specified $\lambda_0 \in \Lambda$ such that

$$C(\Lambda,n) = \lambda_0^{n/2}\Lambda^n \cup \Lambda^n.$$

Since we always have

$$C(\Lambda,n) \supset A(\Lambda,n) \supset N(\Lambda,n) \supset E(\Lambda,n) \supset \Lambda^n,$$

there are thus two possibilities for each of the three middle sets. Determining which is true seems to be a delicate question; our results on this problem, which are incomplete, are presented in §5.

2. **Preliminaries.** We consider an algebraic number field Λ as a subfield of the field of all complex numbers. If p is a nonarchimedean prime of Λ then there is a natural injection $\Lambda \to \Lambda_p$ where Λ_p denotes the completion of Λ at p. We regard Λ as a subfield of Λ_p by means of this injection. For example, "$\sec(2\pi/256) \in \Lambda$" makes sense and if it is true then "$\sec(2\pi/256) \in \Lambda_p$" makes sense and is true.

If Ω is a field we also denote the multiplicative group of the field by Ω; the resulting danger of confusion is trivial. If Λ is a finite extension of Ω then $N_{\Lambda/\Omega}$ is the norm function $N_{\Lambda/\Omega} : \Lambda \to \Omega$, defined by setting $N_{\Lambda/\Omega}(\lambda) =$ determinant

Received by the editors November 25, 1961.

(1) This paper is, essentially, the author's dissertation written at the University of California at Berkeley under the helpful direction of Professor G. Hochschild.

of the endomorphism of Λ (regarded as a vector space over Ω) induced by multiplication by λ. If n is a natural number Ω^n is the set of ω^n with $\omega \in \Omega$.

$\mathbf{I}$ denotes the ring of all algebraic integers and so $\Omega \cap \mathbf{I}$ is the ring of integers of Ω. $\mathbf{Q}$ denotes the field of the rational numbers, and we set $\mathbf{Z} = \mathbf{Q} \cap \mathbf{I}$. $\mathbf{J}$ denotes the set of the natural numbers. If $a,b \in \mathbf{J}$ then "$a \mid b$" means that there exists $c \in \mathbf{J}$ such that $b = ac$; "$a \nmid b$" means that $a \mid b$ is false. If $a, b \in \mathbf{Z}$ then $\langle a,b \rangle$ denotes the set of $c \in \mathbf{Z}$ such that $a \leqq c \leqq b$.

If Λ is an algebraic number field then an even prime of Λ means a prime ideal of $\Lambda \cap \mathbf{I}$ containing 2.

Lemma 1. *Let Λ be a field. For each $n \in \mathbf{J}$, let X_n be a nonempty class of finite extensions of Λ such that if p is a prime in $\mathbf{J}$ and $p^r \mid n$ but $p^{r+1} \nmid n$ then, for every $\Omega \in X_{p^r}$, there exists $\Sigma \in X_n$ so that $\Omega \subset \Sigma$. Let B_n be the set of $\lambda \in \Lambda$ such that $\lambda \in N_{\Omega/\Lambda}(\Omega)$ for all $\Omega \in X_n$.*

Then if

$$B_n \subset \Lambda^n \tag{*}$$

when n is a power of a prime, (*) is true for all $n \in \mathbf{J}$.

Proof. We assume (*) is true for prime powers and decompose n into the product of powers of distinct primes

$$n = P_1 \cdots P_s.$$

Suppose $\omega \in B_n$. Let $i \in \langle 1,s \rangle$ and let $\Omega \in X_{P_i}$. Then there exists $\Sigma \in X_n$ so that $\Omega \subset \Sigma$. It follows that $\omega \in N_{\Sigma/\Lambda}(\Sigma) = N_{\Omega/\Lambda}(N_{\Sigma/\Omega}(\Sigma)) \subset N_{\Omega/\Lambda}(\Omega)$.

Thus $\omega \in B_{P_i} \subset \Lambda^{P_i}$. Hence, for each $i \in \langle 1,s \rangle$ there exists $\omega_i \in \Lambda$ so that $\omega = \omega_i^{P_i}$. Now for $i \in \langle 1,s \rangle$ there are $a_i \in \mathbf{Z}$ such that

$$a_1(n/P_1) + a_2(n/P_2) + \cdots + a_s(n/P_s) = 1,$$

and we have

$$\omega = (\omega_1^{a_1}\omega_2^{a_2}\cdots\omega_s^{a_s})^n \in \Lambda^n.$$

We have shown $B_n \subset \Lambda^n$ for all $n \in \mathbf{J}$, proving the lemma.

Remark. Retaining the hypothesis of the lemma, suppose further that Λ is a number field. Let B_n' be the set of $\lambda \in \Lambda \cap \mathbf{I}$ such that $\lambda \in N_{\Omega/\Lambda}(\Omega \cap \mathbf{I})$ for all $\Omega \in X_n$. Then if

$$B_n' \subset (\Lambda^n \cap \mathbf{I}) \tag{**}$$

when n is a power of a prime, (**) is true for all $n \in \mathbf{J}$. The proof is analogous to the proof of the lemma.

3. The local case.

Theorem 1. *If Λ is a local field and $n \in \mathbf{J}$ then*

$$A(\Lambda,n) = \Lambda\ ,$$

i.e.,

(*) $$\bigcap N_{\Omega/\Lambda}(\Omega) = \Lambda^n,$$

where the intersection is extended over all abelian extension Ω/Λ of degree n. Furthermore, (*) is true if the intersection is taken over all cyclic extensions Ω of degree dividing n.

Proof. Both results are evident when Λ is either the complex numbers or the real numbers. Thus we assume Λ is a nonarchimedean local field. Let P be a power of a rational prime. First, assume that the characteristic of Λ does not divide P.

As is proved in the introductory part of [2] we have

(1) $$(\Lambda:\Lambda^P) = \frac{P}{|P|} \cdot \int_P$$

where $\int_P$ is the number of Pth roots of unity of Λ and where $|\ \ |$ is the normed absolute value of Λ, determined by the condition that the reciprocal of the absolute value of a generator of the prime of Λ is equal to the order of its residue class field. Since we are assuming that P is not a multiple of the characteristic, $(\Lambda:\Lambda^P) < \infty$ and it follows from the existence theorem, as stated in Theorem 14 of [6], that there exists an abelian extension Ω of Λ such that

$$\Lambda^P = N_{\Omega/\Lambda}(\Omega).$$

By the local reciprocity law, the galois group B of Ω/Λ is isomorphic to

$$\Lambda/N_{\Omega/\Lambda}(\Omega) = \Lambda/\Lambda^P,$$

and hence the exponent P' of B divides P. Since B is abelian, there exist cyclic subgroups C_i of B for $i \in \langle 1,t \rangle$ so that

$$B = C_1 \cdots C_t \text{ (direct).}$$

Thus there exist cyclic extensions Γ_i of Λ such that Ω is the composite of the Γ_i and such that the galois group of Γ_i/Λ is canonically isomorphic with C_i for $i \in \langle 1,t \rangle$.

From the local class field theory, we know that the norm group of the composite of abelian extensions is the intersection of the norm groups:

(2) $$\bigcap_{i=1}^{t} N_{\Gamma_i/\Lambda}(\Gamma_i) = N_{\Omega/\Lambda}(\Omega) = \Lambda^P.$$

Since the order of C_i divides the exponent P' of B, it divides P. Thus the index of $C_1 \cdots C_{i-1} C_{i+1} \cdots C_t$ in B is a divisor of P. By (1), the order of B is a multiple of P. It follows from these two facts that there is a subgroup B_i of $C_1 \cdots C_{i-1} C_{i+1} \cdots C_t$ whose index in B is P. The fixed field Σ_i of B_i contains Γ_i and $[\Sigma:\Lambda] = P$. Thus

$$A(\Lambda,n) \subset \bigcap_{i=1}^{t} N_{\Sigma_{i/\Lambda}}(\Sigma_i) \subset \bigcap_{i=1}^{t} N_{\Gamma_{i/\Lambda}}(\Gamma_i) = \Lambda^P,$$

and so

$$A(\Lambda,n) = \bigcap_{i=1}^{t} N_{\Sigma_{i/\Lambda}}(\Sigma_i) = \bigcap_{i=1}^{t} N_{\Gamma_{i/\Lambda}}(\Gamma_i) = \Lambda^P. \tag{3}$$

Now suppose that P is a power of the characteristic p of Λ. For each $m \in \mathbf{J}$, we let W_m denote the set of $w \in \Lambda$ such that $w - 1 \in Y^m$, where Y denotes the prime ideal of the valuation ring R of Λ. Let y be a generator of the principal ideal Y and let T be the cyclic group of powers of y. Let U be the group of units of R. Then

$$\Lambda = TU \text{ (direct)}$$

and so

$$\Lambda^P = T^P U^P \text{ (direct)}.$$

Thus

$$\Lambda/\Lambda^P W_m = Z_P \cdot U/U^P W_m \text{ (direct)},$$

for all $m \in \mathbf{J}$, where Z_P is a cyclic group of order P.

Now $(U:U^P W_m) \leqq (U:W_m) = q^m - q^{m-1}$. We assert that $(U:U^P W_m)$ becomes arbitrarily large for sufficiently large m. We have $(U:U^P W_m) \geqq (W_1:W_1 \cap U^P W_m)$. But $W_1 \cap U^P W_m = W_1^P W_m$, so that $(U:U^P W_m) \geqq (W_1:W_1^P W_m)$. Now suppose that $(W_1:W_1^P W_{m+1}) = (W_1:W_1^P W_m)$. Then $W_m \subset W_1^P W_{m+1}$. Hence there exist $e \in \mathbf{J}$, $\gamma \in U$ and $\omega \in R$ such that $1 + y^m = (1 + \gamma y^e)^P (1 + \omega y^{m+1})$. This gives $y^m = \gamma^P y^{eP} + \omega y^{m+1} + \gamma^P \omega^{eP+m+1}$, whence $eP = m$. Thus if m is not divisible by P then $(W_1:W_1^P W_{m+1}) > (W_1:W_1^P W_m)$. This establishes our assertion.

Thus $(\Lambda:\Lambda^P W_m) = P \cdot (U:U^P W_m)$ is finite for each $m \in \mathbf{J}$, but becomes arbitrarily large for sufficiently large m. Since $\Lambda/\Lambda^P W_m$ has exponent dividing P, $(\Lambda:\Lambda^P W_m)$ is a power of p which is a multiple of P for m sufficiently large, say $m > M$.

The existence theorem of the local class field theory, in the case of a subgroup of Λ of index a power of the characteristic, as stated in Theorem 15 of Chapter 6 of [6], applies when the subgroup contains W_m for some $m \in \mathbf{J}$. Hence there exists an abelian extension Ω of Λ such that

$$N_{\Omega/\Lambda}(\Omega) = \Lambda^P W_{m_0},$$

where $m_0 > M$, and

$$P \mid [\Omega : \Lambda].$$

Let B be the galois group of Ω/Λ. As before, there exist cyclic extensions Γ_i of Λ with galois groups canonically isomorphic to C_i for $i \in \langle 1,t \rangle$ where

$$B = C_1 \cdots C_t \text{ (direct)}$$

and $(C_i : 1) \mid P$. Now we have

$$\bigcap_{i=1}^{t} N_{\Gamma_{i/\Lambda}}(\Gamma_i) = \Lambda^P W_{m_0}.$$

Since $[\Gamma_i:\Lambda] \mid P$ and $P \mid [\Omega:\Lambda]$ and Ω/Λ is abelian, there exist abelian extensions Σ_i/Λ such that $\Omega \supset \Sigma_i \supset \Gamma_i \supset \Lambda$ and $[\Sigma_i:\Lambda] = P$ for $i \in \langle 1,t \rangle$. We have

$$N_{\Omega/\Lambda}(\Omega) = \bigcap_{i=t}^{t} N_{\Sigma_{i/\Lambda}}(\Sigma_i) = \bigcap_{i=1}^{t} N_{\Gamma_{i/\Lambda}}(\Gamma_i) = \Lambda^P W_{m_0}.$$

By combining these facts for each $m > M$ and changing notation slightly we see that there exist cyclic extensions $\Gamma_{i/\Lambda}$ and abelian extensions $\Sigma_{i/\Lambda}$ with

$$\Omega \supset \Sigma_i \supset \Gamma_i \supset \Lambda \text{ and } [\Sigma_i:\Lambda] = P,$$

for all $i \in \mathbf{J}$, such that

$$(4) \qquad N_{\Omega/\Lambda}(\Omega) = \bigcap_{i=1}^{\infty} N_{\Sigma_{i/\Lambda}}(\Sigma_i) = \bigcap_{i=1}^{\infty} N_{\Gamma_{i/\Lambda}}(\Gamma_i) = \bigcap_{m>M} \Lambda^P W_m.$$

Let $\lambda \in \bigcap_{m>M} \Lambda^P W_m$.

There exists an $h \in \mathbf{Z}$ such that $\lambda y^{Ph} \in \bigcap_{m>M} U^P W_m$, because $\lambda y^{Ph} \in U$ for some $h \in \mathbf{Z}$. Thus, for each $m > M$, there exist $u_m \in U$ and $w_m \in W_m$ such that

$$\lambda y^{Ph} = u_m^P w_m.$$

From the definition of W_m, the sequence (w_m) converges to 1 with respect to the valuation of Λ. Hence the sequence (u_m^P) converges (to λy^{Ph}) and therefore is a Cauchy sequence. Since $u_m^P - u_n^P = (u_m - u_n)^P$, it follows that the sequence (u_m) is also a Cauchy sequence. Thus (u_m) converges to a limit $u \in \Lambda^P$. It follows that

$$\bigcap_{m>M} \Lambda^P W_m \subset \Lambda^P.$$

In view of (3), (4) and Lemma 1 of §2 we have established the theorem.

4. The global case.

4.1. *Some lemmas from the literature.* We collect some lemmas which will be used in proving Theorem 2. We either give the proof or give a specific reference (not necessarily the original source). Throughout this section, Λ denotes a fixed global field, and n will always denote a natural number.

We set $\mathbf{E}_n = \exp(2\pi i/2^n)$, $\mathbf{V}_n = 2 + \mathbf{E}_n + 1/\mathbf{E}_n$ and, if $n \geqq 2$,

$$\mathbf{W}_n = \left[\frac{2}{\mathbf{E}_{n+1} + 1/\mathbf{E}_{n+1}}\right]^2 = \frac{4}{\mathbf{V}_n} = \left[\frac{2}{\mathbf{V}_{n+1} - 2}\right]^2.$$

If Λ is a number field we set $s = s(\Lambda) =$ largest $a \in \mathbf{Z}$ such that $\mathbf{V}_a \in \Lambda$. We have $s \geqq 2$ and $\mathbf{V}_a \in \Lambda$ for $a \in \langle 0,s \rangle$ since $\mathbf{V}_a = [\mathbf{V}_{a+1} - 2]^2$. We set $S_0 = S_0(\Lambda)$ = the set of those even primes p of Λ for which -1, $\mathbf{V}_s$, $-\mathbf{V}_s \notin \Lambda_p^2$. We set $t(n) =$ largest $b \in \mathbf{Z}$ such that $2^b \mid n$.

LEMMA 3. *If Λ is a number field, $p \in S_0$ and $t(n) > 0$ then $\mathbf{V}_s^{n/2} \notin \Lambda_p^n$.*

Proof. Suppose $\mathbf{V}_s^{n/2} = \lambda^n$, for some $\lambda \in \Lambda_p$. Setting $t = t(n)$, we have that $n = 2^t m$ where m is odd and

$$[\mathbf{V}_s^{2^{t-1}}]^m = [\lambda^m]^{2^t}.$$

This implies that

$$\mathbf{V}_s^{2^{t-1}} = \omega^{2^t} \text{ for some } \omega \in \Lambda_p;$$

in fact, for $\omega = \mathbf{V}_s^{K2^{t-1}} \lambda^{hm}$, where $hm + K2^t = 1$. Hence $\mathbf{V}_s = \zeta\omega^2$ where ζ is a 2^{t-1}th root of unity. But this relation implies $\zeta \in \Lambda_p$ and hence $\zeta = \pm 1$ since $-1 \notin \Lambda_p^2$ by the first requirement for p to be in S_0. But $\mathbf{V}_s = \pm\omega^2$ means $\pm\mathbf{V}_s \in \Lambda_p^2$, contradicting one of the remaining requirements for p to be in S_0. This completes the proof.

LEMMA 4. *Let S be a finite set of primes of Λ. Then $\Lambda \cap \bigcap_{p \notin S} \Lambda_p^n = \Lambda^n$ except in the special case when*

(1) *Λ is a number field,*
(2) *$t(n) > s$,*
(3) *$-1, \mathbf{V}_s, -\mathbf{V}_s, \notin \Lambda^2$,*
(4) *$S_0 \subset S$.*

In this special case

$$\Lambda \cap \bigcap_{p \notin S} \Lambda_p^n = \mathbf{W}_s^{n/2} \Lambda^n \cup \Lambda^n \neq \Lambda^n.$$

REMARK. Lemma 4 appears as Theorem 1 of Chapter 10 of [2]. We mention that the number $\mathbf{W}_s$ is an integer of Λ which is divisible only by even primes of Λ. First $\mathbf{W}_s = 4/\mathbf{V}_s \in \Lambda$. Second, $\mathbf{W}_s^{2^s} = [2/(1 + \mathbf{B}_s)]^{2^{s+1}}$; but we can show recursively that if ζ_s is any primitive 2^sth root of unity (e.g., $-\mathbf{E}_s$) then $[1 - \zeta_s]^{2^{s-1}} = 2u_s$ where u_s is a unit. In fact,

$$[1 - \zeta_{s+1}]^2 \; [1 + \zeta_{s+1}]^{2^s} = [1 - \zeta_s]^2 = [1 - \zeta_s]^{2^{s-1}} 2u_s,$$

whence

$$[1 - \zeta_{s+1}]^{2^s} = 2u_s \left[\frac{1 - \zeta_s}{[1 + \zeta_{s+1}]^2} \right]^{2^{s-1}} = 2u_s \left[\frac{1 - \zeta_{s+1}}{1 + \zeta_{s+1}} \right]^{2^{s-1}}.$$

Since $-\zeta_{s+1}$ and ζ_{s+1} are powers of each other $(1 - \zeta_{s+1})/(1 + \zeta_{s+1})$ is a unit; the fact we have mentioned follows from this.

We also need Theorem 5 of Chapter 10 of [2] which we state as

LEMMA 5 (GRUNWALD-WANG). *Let S be a finite set of primes of Λ, c_p a character of Λ_p of period n_p for each $p \in S$ and n the least common multiple of the n_p's.*

Then there exists a character c of the idèle class group of Λ whose local restrictions at $p \in S$ are the given c_p. The period of c can be made n provided that if Λ, n and S are as in the special case of Lemma 4 (or in other words, if $\Lambda \cap \bigcap_{p \notin S} \Lambda_p^n \neq \Lambda^n$) then

$$\prod_{p\in S_0} c_p(\mathbf{V}_s^{n/2})=1\,;$$

here, an empty product is understood to represent 1.

COROLLARY. *Under the same conditions, the period of c can be made any multiple m of n.*

Proof. We set $S' = S \cup \{q\}$, where q is any prime of Λ such that $q \notin S \cup S_0$. We further set c_q equal to the character of Λ_q defining the (cyclic) unramified extension of degree m. Applying the lemma to Λ, m and S' yields the corollary.

4.2. *The determination of* $C(\Lambda,n)$. As in the introduction, we denote by $C(\Lambda,n)$ the intersection of the norm groups of all cyclic extensions of degree n over Λ.

LEMMA 6. $C(\Lambda,n) \subset \Lambda \cap \bigcap_{p\notin S_0} \Lambda_p$.

Proof. Let $\lambda \in C(\Lambda,n)$. Let p be an arbitrary prime of Λ such that $p \notin S_0$ and let Σ be an arbitrary cyclic extension of Λ_p of degree dividing n. Let c_p be the character of Λ_p corresponding to the cyclic extension Σ/Λ_p. Then, by the Corollary to Lemma 5, there exists a global character c on the idèle class group of Λ whose local restriction at p is c_p and whose period is n. This c defines a cyclic extension Γ/Λ of degree n such that $\Gamma_{\bar p} = \Sigma$ where $\bar p$ is a prime of Γ above p. Now

$$\lambda \in C(\Lambda,n) \subset N_{\Gamma/\Lambda}(\Gamma) \subset N_{\Gamma_{\bar p}/\Lambda_p}(\Gamma_{\bar p} = N_{\Sigma/\Lambda_p}(\Sigma).$$

Since Σ is an arbitrary cyclic extension of Λ_p of degree dividing n, we have from Theorem 1 of §3 that $\lambda \in \Lambda_p^n$. Thus we have $\lambda \in \Lambda \cap \bigcap_{p\notin S_0} \Lambda_p^n$, and we have proved the lemma.

REMARK. Lemmas 4 and 6 together give an estimate of $C(\Lambda,n)$. Namely,

$$\Lambda^n \subset C(\Lambda,n) \subset \mathbf{W}_s^{n/2}\Lambda^n \cup \Lambda^n$$

always, and $C(\Lambda,n) = \Lambda^n$ except, perhaps, when Λ and n satisfy 1, 2 and 3 of Lemma 4. We sharpen this estimate to determine $C(\Lambda,n)$ exactly.

THEOREM 2. $C(\Lambda,n) = \Lambda^n$ *except in the special case when*

(1) Λ *is a number field,*

(2) $t(n) > s$,

(3) S_0 *has precisely one member or* S_0 *is empty but* -1, $\mathbf{V}(s)$, $-\mathbf{V}(s) \notin \Lambda^2$.

In this special case,

$$C(\Lambda,n) = \mathbf{W}_s^{n/2}\,\Lambda^n \cup \Lambda^n \neq \Lambda^n.$$

Proof. The last inequality follows from the last inequality of Lemma 4, since, if $S_0 = \{p\}$, -1, $\mathbf{V}_s$, $-\mathbf{V}_s \notin \Lambda_p^2$ and so, a fortiori, -1, $\mathbf{V}_s$, $-\mathbf{V}_s \in \Lambda^2$.

For the proof of the rest of the result, it suffices, by the remark preceding the theorem, to assume Λ is a number field, $t(n) > s$ and then to prove that

$$\mathbf{W}^{n/2} \in C(\Lambda,n)$$

if, and only if, S_0 has at most one member.

Suppose that S_0 has at least 2 members, say

$$S_0 = \{p_1, p_2, \cdots, p_k\}, \text{ where } k \geqq 2.$$

For $i \in \langle 1,k \rangle$ let Λ_i denote the completion of Λ at p_i. For $i \in \langle 1,2 \rangle$ (in particular) we have $\mathbf{V}_s^{n/2} \notin \Lambda_i^n$ by Lemma 3. By Theorem 1 of §3 there exists a cyclic extension Γ_i of Λ_i of degree dividing n such that $\mathbf{V}_s^{n/2} \notin N_{\Gamma_i/\Lambda_i}(\Gamma_i)$, for $i \in \langle 1,2 \rangle$. Let $\Gamma_i = \Lambda_i$ for $i \in \langle 3,k \rangle$. Letting c_i be the character of Λ_i defining Γ_i, for each $i \in \langle 1,k \rangle$, we may apply the Corollary to Lemma 5 and obtain a global character c whose local restriction at p_i is c_i. The period of c can be taken to be any multiple of all the periods of the c_i, provided that

$$\prod_{i=1}^{k} c_i(\mathbf{V}_s^{n/2}) = 1.$$

This proviso is satisfied, because, for $i \in \langle 3,k \rangle$, c_i is identically 1, while, for $i \in \langle 1,2 \rangle$, we have $c_i(\mathbf{V}_s^{n/2}) = -1$, since $\mathbf{V}_s^{n/2} \notin N_{\Gamma_i/\Lambda_i}(\Gamma_i)$, by the choice of Γ_i, while

$$[\mathbf{V}_s^{n/2}]^2 = \mathbf{V}_s^n \in \Lambda_i^n \subset N_{\Gamma_i/\Lambda_i}(\Gamma_i).$$

Since $[\Gamma_i : \Lambda_i] \mid n$, for $i \in \langle 1,k \rangle$, we may take the period of c to be n. Thus c defines a cyclic extension Γ/Λ of degree n such that (in particular) the completion of Γ at a prime above p_1 is Γ_1. Now

$$\mathbf{W}_s^{n/2} = \frac{2^n}{\mathbf{V}_s^{n/2}} \notin N_{\Gamma_1/\Lambda}(\Gamma_1);$$

a fortiori,

$$\mathbf{W}_s^{n/2} \notin M_{\Gamma/\Lambda}(\Gamma).$$

We have shown that if $\mathbf{W}_s^{n/2} \in C(\Lambda,n)$ then S_0 has at most one member.

Conversely, assume S_0 has at most one member and let Γ/Λ be a cyclic extension of degree n with galois group C. We must show $\mathbf{W}_s^{n/2} \in N_{\Gamma/\Lambda}(\Gamma)$. Using the formulation of Artin's reciprocity theorem as given in [5],

$$\psi_{\Gamma/\Lambda} : J_\Lambda \to C$$

be the reciprocity map, where J_Λ is the idèle group of Λ, and we let $\psi_{\Gamma/\Lambda,q}$ be the local reciprocity map for each prime q of Λ. Identifying Λ with a subgroup of J_Λ in the natural way, we have

$$(*) \qquad 1 = \psi_{\Gamma/\Lambda}(\mathbf{W}_s^{n/2}) = \prod_q \psi_{\Gamma/\Lambda,q}(\mathbf{W}_s^{n/2}),$$

where the product is extended over all primes q of Λ. Since

$$\ker(\psi_{\Gamma/\Lambda,q}) = N_{\Gamma_{\bar{q}}/\Lambda_q}(\Gamma_q) \supset \Lambda_q^n$$

where $\bar{q}$ is a prime of Γ above q, we have (using Lemma 4)

$$(**) \qquad \psi_{\Gamma/\Lambda,q}(\mathbf{W}_s^{n/2}) = 1,$$

except for at most one q. But then (*) shows (**) must hold for this q also. It follows that $\mathbf{W}_s^{n/2}$ is a norm of every local completion of Γ. Since Γ/Λ is cyclic $\mathbf{W}_s^{n/2}$ must be a norm of Γ by the Hasse Norm Theorem. This completes the proof.

EXAMPLES. 1. $S_0(\mathbf{Q})$ has one member, (2). This follows from the fact that (2) is the unique even prime of $\mathbf{Q}$, while $\Gamma(\sqrt{-1})$, $\mathbf{Q}(\sqrt{\mathbf{V}_2}) = \mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{-\mathbf{V}_2}) = \mathbf{Q}(\sqrt{-2})$ are ramified of degree 2 at (2), so that $-1, \mathbf{V}_2, -\mathbf{V}_2 \notin \mathbf{Q}_{(2)}^2$. Since $\mathbf{V}_3 = 2/\sqrt{2} + 2 \notin \mathbf{Q}$, $s(\mathbf{Q}) = 2$. Thus $\Lambda = \mathbf{Q}$ and $n = 8$ provide an example where the special conditions of Theorem 2 are satisfied with S_0 having precisely one member.

2. $S_0(\mathbf{Q}(\sqrt{7}))$ is empty. Since $7 \equiv 3 \mod 4$, $\mathbf{Q}(\sqrt{7})$ is ramified of degree 2 above (2), and so $\mathbf{Q}(\sqrt{7})$ has a unique even prime, say p. But since $-7 \equiv 1 \mod 8$, $-7 \in \mathbf{Q}_{(2)}^2 \subset \mathbf{Q}_p(\sqrt{7})^2$. Since $7 \in \mathbf{Q}_p(\sqrt{7})^2$, we have $-1 \in \mathbf{Q}_p(\sqrt{7})^2$, proving the assertion. Thus $\Lambda = \mathbf{Q}(\sqrt{7})$, $n = 8$ is an example where the special conditions of Theorem 2 are satisfied with $S_0(\mathbf{Q}(\sqrt{7}))$ empty but -1, $\mathbf{V}_2 = 2$, $-\mathbf{V}_2 = -2 \notin \mathbf{Q}(\sqrt{7})^2$.

3. For $\Lambda = \mathbf{Q}(\sqrt{-1})$ and n arbitrary, the special conditions of Theorem 2 are not satisfied; yet $S_0(\mathbf{Q}(\sqrt{-1}))$ is empty.

4. For Λ arbitrary and $8 \nmid n$, the special conditions of Theorem 2 are not satisfied, and yet $S_0(k)$ may have precisely one member; for example, if $\Lambda = \mathbf{Q}$.

5. $S_0(\mathbf{Q}(\sqrt{-7}))$ has 2 members. In fact, $-7 \in \mathbf{Q}_{(2)}$, and so (2) splits into 2 distinct primes, say p_1 and p_2. Since $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-2})$ are ramified of degree 2 over (2), we have $-1, 2, -2 \notin \mathbf{Q}_{(2)}^2 = \mathbf{Q}_{p_i}(\sqrt{-7})^2$, for $i \in \langle 1,2 \rangle$. Thus $\Lambda = \mathbf{Q}(\sqrt{-7})$ and n arbitrary is an example where the special conditions of Theorem 2 are not satisfied, because $S_0(\mathbf{Q}\sqrt{-7})$ has more than one member.

REMARK. By these examples, it follows that, for number fields, the conditions 2 and 3 of Theorem 2 are independent and irredundant.

5. **Further results and unsolved problems in the number field case.** Throughout this section, Λ denotes a fixed number field. We define $s = s(\Lambda)$, $S_0 = S_0(\Lambda)$, $C(\Lambda,n)$ and $t(n)$ as in Chapter 4. We let $E(\Lambda,n)$ be the intersection of the norm groups of all extensions of Λ of degree n. We always have

$$\Lambda^n \subset E(\Lambda,n) \subset C(\Lambda,n);$$

we can strengthen this, but we need a well-known auxiliary result.

LEMMA 7. *If L is an algebraic number field, π a prime of L and G/L_π an extension of degree n, there exists an extension S/L of degree n and a prime $\bar{\pi}$ of S above π so that $S_{\bar{\pi}} = G$.*

Proof. Let $G = L_\pi(\alpha)$ and let f be the monic irreducible polynomial for α over L_π. Then it follows from Theorems 9 and 10 of Chapter 2 of [1] that if g

is a monic polynomial of degree n in $L_\pi[X]$ such that the coefficients of equal powers of X in f and g are sufficiently near in the valuation of L_π, then $L_\pi(\alpha) = L_\pi(\beta)$ for some root β of g. We may find such a g in $L[X] \subset L_\pi[X]$. For this g we have, for some prime $\bar{\pi}$ of $L(\beta)$ above π, $(L(\beta))_{\bar{\pi}} = L_\pi(\beta) = G$ and so $S = L(\beta)$ satisfies the requirements of the lemma.

THEOREM 3. *$E(\Lambda,n) = \Lambda^n$, unless*

(1) $t(n) > s$,

(2) S_0 is empty.

Proof. By Theorem 2 of §4, all we must show is that

$$\mathbf{W}_s^{n/2} \notin N_{\Gamma/\Lambda}(\Omega),$$

for some extensions Ω/Λ of degree n, assuming that $t(n) > s$ and S_0 has precisely one member p.

By Lemma 3 of §4,

$$\mathbf{W}_s^{n/2} = 2^n/\mathbf{V}_s^{n/2} \notin \Lambda_p^n.$$

By Theorem 1 of §3, there is a cyclic extension Γ/Λ_p of degree m such that $m \mid n$ and

$$(*) \qquad \mathbf{W}_s^{n/2} \notin N_{\Gamma/\Lambda_p}(\Gamma).$$

By Lemma 7, there exists an extension Σ'/Λ of degree m and a prime p' of Σ' above p so that $\Sigma'_{p'} = \Gamma$. By the Corollary to Lemma 5 of §4, there exists an (cyclic) extension Σ/Σ' of degree n/m and a prime $\bar{p}$ of Σ above p' so that $\Sigma_{\bar{p}} = \Gamma$. Using (*) and the fact that

$$N_{\Sigma/\Lambda}(\Sigma) \subset N_{\Sigma_{\bar{p}}/\Lambda_p}(\Sigma_{\bar{p}}) = N_{\Gamma/\Lambda_p}(\Gamma),$$

we have

$$\mathbf{W}_s^{n/2} \notin N_{\Sigma/\Lambda}(\Sigma).$$

Since

$$[\Sigma : \Lambda] = [\Sigma : \Sigma'] \, [\Sigma' : \Lambda] = n/m \cdot m = n,$$

the theorem is established.

REMARK. Theorem 3 gives new information in the case when $S_0(\Lambda)$ has precisely one member, e.g., if $\Lambda = \mathbf{Q}$. Thus we *now* know that while 16 is the norm of every cyclic extension of $\mathbf{Q}$ of degree 8, there is some extension of $\mathbf{Q}$ of degree 8 for which 16 is not a norm.

After Theorems 2 and 3 it is natural to attempt to determine $A(\Lambda,n)$, the intersection of the norm groups of all abelian extensions of degree n over Λ. By Theorem 2, we may restrict our attention to fields Λ and numbers n which satisfy the conditions 1, 2 and 3 of that theorem. The question hinges on whether or not $\mathbf{W}_s^{n/2}$ is the norm of every abelian extension of degree n over Λ. For example, is 16 a norm of every abelian extension of degree 8 over $\mathbf{Q}$? We do not know the answer to this question. However, we can show that 16 is not the norm of an *integer* of every abelian extension of degree 8 over $\mathbf{Q}$. More generally, we have the following result.

THEOREM 4. *Let* Λ *be a number field such that the principal* (*integral*) *ideal* $(\mathbf{W}_s)$ *is not the square of a principal* (*integral*) *ideal of* Λ. *Then we have, for all* $n \in \mathbf{J}$,

$$(*) \qquad \bigcap N_{\Omega/\Lambda}(\mathbf{I} \cap \Omega) = (\mathbf{I} \cap \Lambda)^n = \mathbf{I} \cap \Lambda^n,$$

where the intersection is over all abelian extensions Ω/Λ *of degree* n.

Proof. By the remark following Lemma 2 of §2, we may assume n is a power of a prime and thence, by Theorem 2 of §4, we may assume n is a power of 2, $n = 2^t$. For the purpose of proving the result by induction, we must use a stronger induction hypothesis than the statement of the theorem requires; let H_t be the proposition: There exists an abelian extension Γ of degree 2^t over Λ such that the principal ideal $(\mathbf{W}_s^{2^t})$ of Λ is not the norm of the square of a principal integral ideal of Γ.

If H_t is true for all $t \in \mathbf{J}$ then $(\mathbf{W}_s)^{2^{t-1}}$ is not the norm of a principal integral ideal of Γ, where Γ satisfies H_t. Hence $\mathbf{W}^{2^{t-1}}$ is not the norm of an integer of Γ. As we know, this imples that (*) is true for $n = 2^t$.

Now H_0 is true by our assumption about Λ. We assume $t \in \mathbf{J}$ and Γ satisfies H_{t-1}.

Let $\gamma_1, \cdots, \gamma_N$ be integers of Γ such that $(\gamma_1), \cdots, (\gamma_N)$ are all the distinct principal integral ideals having norm $(\mathbf{W}_s^{2^{t-1}})$ over Λ. That there exists such an $N \in \mathbf{J}$ and γ_i for $i \in \langle 1,N \rangle$ follows from the fact that there are only a finite number of integral ideals with a given norm and from $N_{\Gamma/\Lambda}((\mathbf{W}_s)) = (\mathbf{W}^{2^{t-1}})$, which shows $N \geqq 1$.

Let U be the group of units of Γ. Since U is finitely generated, U/U^2 is finite with exponent 2 and so has a basis $u_1, \cdots, u_M$. This means that, for all $u \in U$, there exist $m_j \in \mathbf{Z}$ and $v \in U$ such that

$$u = v^2 \prod_{j=1}^{M} u_j^{m_j},$$

and if

$$u = v'^2 \prod_{j=1}^{M} u_j^{m'_j},$$

with $v' \in U$ and $m'_j \in \mathbf{Z}$, then $m_j \equiv m'_j \bmod 2$, for each j.

If $w \in U$ then $\gamma_i w \notin \Gamma^2$, for otherwise $(\gamma_i) = (\gamma_i w)$ would be the square of a principal integral ideal of Γ, so that $(\mathbf{W}_s^{2^{t-1}})$ would be the norm of the square of a principal integral ideal of Γ, contradicting our inductive hypothesis. Given an $i \in \langle 1,N \rangle$, it follows from these considerations that if

$$\gamma_i^{m_0} \prod_{j=1}^{M} u_j^{m_j} \in \Gamma^2$$

then $m_k \equiv 0 \bmod 2$, for $k \in \langle 0,M \rangle$. By Satz 169 of [4], it follows that there exists an infinite set S_i of primes of Γ such that

$$\left(\frac{\gamma_i}{P}\right) = -1$$

and

$$\left(\frac{u_j}{P}\right) = 1$$

for all $j \in \langle 1,M \rangle$ and for all $P \in S_i$ where, for $x \in \Gamma$ such that x is integral at P

$$\left(\frac{x}{P}\right) = \begin{cases} 1 \text{ if } x \equiv y^2 \bmod P \text{ for some } y \in \Gamma \cap \mathbf{I}, \\ -1 \text{ otherwise.} \end{cases}$$

For each prime P of Γ, we set $\bar{P}$ equal to the positive generator of the prime ideal of $\mathbf{Z}$ below P. Since the S_i are infinite we can recursively determine a $P \in S$ for each $i \in \langle 1,N \rangle$ such that

(i) no $(\bar{P}_i)$ ramifies in $\Gamma/\mathbf{Q}$,

(ii) $P_i \neq P_j$ if $i \neq j$.

Setting

$$d = \prod_{i=1}^{N} \bar{P}_i$$

we claim that $\Gamma(\sqrt{d})$ satisfies H_t.

$\sqrt{d} \notin \Gamma$ since $\bar{P}_i$ ramifies in $\mathbf{Q}(\sqrt{d})$. Thus $\Gamma(\sqrt{d})$ is an abelian extension of degree 2^t over Λ. Now suppose that contrary to our claim

$$(\mathbf{W}_s^{2^t}) = N_{\Gamma(\sqrt{d})/\Gamma}((\int)^2)$$

for some integral

$$\int \in \Gamma(\sqrt{d}).$$

Then

$$(\mathbf{W}^{2^{t-1}}) = N_{\Gamma(\sqrt{d})/\Lambda}((\int)) = N_{\Gamma/\Lambda}(N_{\Gamma(\sqrt{d})\Gamma}((\int))) .$$

Since $N_{\Gamma(\sqrt{d})/\Gamma}((\int))$ is a principal integral ideal, there exists an $i \in \langle 1,N \rangle$ so that

$$(\gamma_i) = N_{\Gamma(\sqrt{d})/\Gamma}((\int)) = (N_{\Gamma(\sqrt{d})/\Gamma}(\int)).$$

Setting $\int = \gamma + \sqrt{d}\,\omega$ with $\lambda,\ \omega \in \Gamma$, we have

$$(\gamma_i) = (\lambda^2 - d\omega^2).$$

Thus there exists $u \in U$ such that

$$\gamma_i u = \lambda^2 - d\omega^2.$$

Hence there exist $m_j \in \mathbf{Z}$ and $w \in U$ such that

$$\gamma_i w^2 \prod_{j=1}^{M} u_j^{m_j} = \lambda^2 - d\omega^2.$$

For $\eta \in \Gamma$, let $v(\eta)$ be the order of η at P_i. Then $v(\lambda^2)$ is even and from (i) and (ii) $v(d) = 1$. Hence $v(-d\omega^2)$ is odd. Hence

$$v(\lambda^2) \neq v(-d\omega^2)$$

which implies

$$v(\lambda^2 - d\omega^2) = \min(v(\lambda^2), v(d\omega^2)).$$

Since

$$v\left(\gamma_i w^2 \prod_{j=1}^{M} u_j^{m_j}\right) \geqq 0,$$

it follows that

$$v(\lambda^2),\ v(d\omega^2) \geqq 0.$$

Thus $v(\omega^2) \geqq 0$. Hence we have

$$1 = \left[\frac{\gamma_i w^2 \prod_{j=1}^{M} u_j^{m_j}}{P_i}\right] = \left(\frac{\gamma_i}{P_i}\right)\left(\frac{w}{P_i}\right)^2 \prod_{j=1}^{M} \left(\frac{u_j}{P_i}\right)^{m_j} = \left(\frac{\gamma_i}{P_i}\right) = -1,$$

a contradiction.

Thus $\Gamma(\sqrt{d})$ does satisfy H_t, and Theorem 4 is proved.

REMARK. For the field $\mathbf{Q}(\sqrt{7})$, for example, the indeterminateness of $A(\mathbf{Q}(\sqrt{7}), n)$ and $E(\mathbf{Q}(\sqrt{7}), n)$ when $8 \mid n$ persists. For we have seen (Example 2 of Chapter 4) that $S_0(\mathbf{Q}(\sqrt{7}))$ is empty, so that Theorem 3 does not apply. Also we have noted that $\mathbf{Q}(\sqrt{7})$ ramifies above (2), so that $(2) = p^2$. Since $\mathbf{Q}(\sqrt{7}) \cap \mathbf{I}$ is a unique factorization domain, p is principal, and so Theorem 4 does not apply.

REFERENCES

1. E. Artin, *Algebraic numbers and algebraic functions*. I, Institute for Mathematics and Mechanics, New York University, New York, 1951.

2. E. Artin and J. Tate, *Class field theory*, Harvard Notes, 1961.

3. C. Chevalley, *Class field theory*, Nagoya University, 1954.

4. E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, Leipzig, 1923.

5. G. Hochschild, *Note on Artin's reciprocity law*, Ann. of Math. **51** (1950), 694–701.

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

7. S. Wang, *On Grunwald's theorem*, Ann. of Math. **51** (1950), 471–484.

STANFORD UNIVERSITY,
STANFORD, CALIFORNIA