Therefore we may assume that $M'^2-3N' = \pm 3^v$. Using $\varepsilon = (-1)^k$ and (7), we see this can be written as

$$\pm 3^v + 2^{k+1} = (-1)^{k+1}.$$

The sign surely must be negative; and so by a theorem of LeVeque ([4], [2]), we have $(v, k) = (2, 2), (1, 1)$, or $(1, 0)$. We have already seen that $k \geqslant 2$. So $k = 2$ and the corresponding values of N' and M' are

$$N' = 5 \quad \text{and} \quad M' = \pm\sqrt{6}.$$

But then $V_6' = 236$ which is divisible by 59. If $\sqrt{59} \mid U_r'$, then $\sqrt{59} \mid (U_{12}', U_r') = |U_{(12,r)}'| = |M'|$. But then since $59 \mid V_6' = \{M'(M'^2-3N')\}^2 - 2N'^3$, we have $59 \mid N'$ contrary to $(M'^2, N') = 1$. So $59 \nmid Nd$, and Theorem 2 shows that $\{a_{12n}\}$ contains no more than two occurrences of d; therefore $m(d) \leqslant 4$.

The only remaining case is that in which $3 \mid N'$. By (7), we see then that $\varepsilon = (-1)^{k+1}$ and so

$$M'^2 = 2\big(2^{k-1}+(-1)^{k+1}\big) \quad \text{and} \quad N' = 2^k + (-1)^{k+1}.$$

If $k = 2$, then $m(d) \leqslant 4$ by Lemma 13. For $k \geqslant 3$, the result follows from Lemma 20, and so the proof of the theorem is complete.

References

[1] R. Alter and K. K. Kubota, *Multiplicities of second order linear recurrences*, Trans. Amer. Math. Soc. 178 (1973), pp. 271–284.

[2] J. W. S. Cassels, *On the diophantine equation $a^x - b^y = 1$*, Amer. J. Math. 75 (1953), pp. 159–162.

[3] K. K. Kubota, *On a conjecture of Morgan Ward, I*, Acta Arith., this volume, pp. 11–28.

[4] W. J. LeVeque, *On the equation $a^x - b^y = 1$*, Amer. J. Math. 74 (1952), pp. 325–331.

[5] W. Ljunggren, *Noen setninger om ubestemte likninger av formen $(x^n-1)/(x-1) = y^q$*, Norsk Mat. Tidsskr. 25 (1943), pp. 17–20.

[6] L. J. Mordell, *Diophantine Equations*, Academic Press, London 1969.

[7] — *The diophantine equation $y^2 = Dx^4+1$*, J. London Math. Soc. 39 (1964), pp. 161–164.

Received on 23. 4. 1975
and in revised form on 30. 12. 1975 (699)

ACTA ARITHMETICA
XXXIII (1977)

Proper solutions of the imbedding problem with restricted ramification

by

OLAF NEUMANN (Berlin)

Let k be a field, $\bar{k}$ its separable algebraic closure with the Galois group $\mathfrak{G} = \mathrm{Gal}(\bar{k}/k)$. An imbedding problem is defined by a diagram

$$\text{(1)} \qquad \begin{array}{ccccccccc} & & & & & & \mathfrak{G} & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ \{1\} & \longrightarrow & A & \longrightarrow & G & \xrightarrow{j} & F & \longrightarrow & \{1\} \end{array}$$

where A, G, F denote finite groups. All arrows are group homomorphisms and the horizontal sequence is exact. We assume φ surjective. Hence, the kernel of φ, $\mathfrak{G}_0 = \mathrm{Ker}\,\varphi$, determines a finite normal extension K/k with $\mathrm{Gal}(K/k) \simeq F$. A solution of the imbedding problem (1) is by definition a homomorphism $\psi\colon \mathfrak{G} \to G$ satisfying the condition $j \circ \psi = \varphi$. ψ is called a *proper solution* if and only if it is surjective.

Let k be a global field, i.e., a finite algebraic number field or an algebraic function field of one variable over a finite constant field. By k_S we denote the maximal normal extension of k unramified outside the given set of primes S. Let $\mathfrak{G}_S$ be the group $\mathrm{Gal}(k_S/k)$. If S contains all ramification points of the extension K/k occurring in the diagram (1), we can factorize φ through the group $\mathfrak{G}_S$:

$$\text{(1}_S\text{)} \qquad \begin{array}{ccccccccc} & & & & \mathfrak{G} & \xrightarrow{\pi_S} & \mathfrak{G}_S & & \\ & & & & & & \downarrow{\scriptstyle\varphi_S} & & \\ \{1\} & \longrightarrow & A & \longrightarrow & G & \xrightarrow{j} & F & \longrightarrow & \{1\}. \end{array}$$

We say (1) admits a solution ψ unramified outside S if and only if (1_S) admits a solution $\psi_S\colon \mathfrak{G}_S \to G$ with $j \circ \psi_S = \varphi_S$ and $\psi = \psi_S \circ \pi_S$ where π_S denotes the canonical epimorphism $\mathfrak{G} \to \mathfrak{G}_S$.

The main result of the present paper is the following

THEOREM. *Suppose k is a global field, K/k is a given finite normal extension with $F = \mathrm{Gal}(K/k)$, A a finite F-module with* $\mathrm{char}\,k \nmid \mathrm{card}\,A$. *Then every imbedding problem* (1) *with at least one solution admits a proper solution unramified outside a suitable finite set of primes $S \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. Here S depends only on n = exponent of A and on the extension $K(\zeta_n)/k$ (ζ_n denotes a primitive n-th root of unity). The set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ is disjoint to S and consists of m different primes totally decomposed in the extension $k(A, \zeta_n)/k$, m being the length of a F-composition series of A. (By $k(A, \zeta_n)/k$ we denote the field $k(A)(\zeta_n)$ where $k(A)$ is the field corresponding to the fix group of A.)*

The theorem constitutes a strengthened version of results of Ikeda [3] and Iškhanov [4].

For the proof of the theorem, we introduce the following notations: $k_\mathfrak{p}$ – the $\mathfrak{p}$-adic closure of k; $\bar{k}_\mathfrak{p}$ — a separable algebraic closure of $k_\mathfrak{p}$; $k_\mathfrak{p}^{nr}$ — the maximal unramified extension of $k_\mathfrak{p}$ contained in $\bar{k}_\mathfrak{p}$; $T_\mathfrak{p} = \mathrm{Gal}(\bar{k}_\mathfrak{p}/k_\mathfrak{p}^{nr})$; $H^1_{nr}(k_\mathfrak{p}, A) = \mathrm{Im}[\mathrm{inf}\colon H^1(k_\mathfrak{p}^{nr}/k_\mathfrak{p}, A^{T_\mathfrak{p}}) \to H^1(\bar{k}_\mathfrak{p}/k_\mathfrak{p}, A)]$.

The following key proposition is derived from Tate's global duality theorem ([9], [2]).

PROPOSITION (see [6], Behauptung). *Under the assumptions of our theorem there exists a finite set of primes S containing all ramification points of K/k and depending only on n = exponent of A and on the extension $K(\zeta_n)/k$ such that for any finite set T of primes disjoint to S and any finite F-module A with* $\mathrm{char}\,k \nmid \mathrm{card}\,A$ *the canonical map*

$$H^1(k_{S\cup T}/k, A) \to \sum_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A)/H^1_{nr}(k_\mathfrak{p}, A)$$

is surjective.

In the paper [6] the author described a class of sets S satisfying the conditions of this proposition.

Proof of the theorem. We fix a diagram (1) with at least one solution. Suppose that the corresponding group extension is given by the cohomology class $\varepsilon \in H^2(F, A)$. Let be $\mathfrak{G}_0 = \mathrm{Ker}\,\varphi = \mathrm{Gal}(\bar{k}/K)$. It is well-known that the existence of a solution of (1) amounts to the existence of a certain element $\chi \in H^1(\mathfrak{G}_0, A)^F$ going over *via* the transgression map $H^1(\mathfrak{G}_0, A)^F \to H^2(F, A)$ into the given class $\varepsilon \in H^2(F, A)$. The whole set of all solutions of (1) is described by the sums $\chi + \omega \in H^1(\mathfrak{G}_0, A)^F$ where $\omega = \mathrm{Res}\,\alpha$, $\alpha \in H^1(\mathfrak{G}, A)$, Res: $H^1(\mathfrak{G}, A) \to H^1(\mathfrak{G}_0, A)^F$ (cf. Neukirch [5], § 1). The analogous facts hold for the solutions of (1_S).

By results of Iškhanov [4] and the author [6], there exists a finite set of primes S with all properties required in our proposition such that our soluble imbedding problem (1) has a solution, ψ (say), unramified outside S. Starting from this solution we proceed by induction on m (= length of the F-module A). Choose the F-submodule A_1 of A such

that A/A_1 is an irreducible F-module $\neq \{0\}$. Obviously, A_1 is a normal subgroup in G, and the canonical epimorphism $G \to G/A_1$ yields a new imbedding problem:

(2)
$$\begin{array}{ccccccccc} & & & & G & \xleftarrow{\ \psi\ } & \mathfrak{G} & & \\ & & & & \downarrow & \swarrow_{\bar{\psi}} & \downarrow{\scriptstyle\varphi} & & \\ \{1\} & \longrightarrow & A/A_1 & \longrightarrow & G/A_1 & \longrightarrow & F & \longrightarrow & \{1\}. \end{array}$$

Every solution ψ of (1) gives us a solution $\bar{\psi}$ of (2).

Let $\mathfrak{q}_1 = \mathfrak{q}$ be a prime of the ground field k totally decomposed in the extension $k(A, \zeta_n)/k$ and different from all primes lying in S. By the well-known facts (see an elementary proof by Dress [1]), such a prime ideal always exists. Set $L_\mathfrak{q} = k_\mathfrak{q}(\sqrt[n]{\pi_\mathfrak{q}})$ where $\pi_\mathfrak{q}$ denotes a prime element for $\mathfrak{q}$. $L_\mathfrak{q}/k_\mathfrak{q}$ is a totally ramified cyclic extension of degree n. Let $a \in A$ be an arbitrary element of A with $a \notin A_1$. If we map a generator of $\mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{q})$ onto the element a, we get a non-trivial homomorphism

$$\eta_\mathfrak{q}\colon \mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{q}) \to A$$

whereas the composition with the canonical map $A \to A/A_1$ is still a non-trivial homomorphism

$$\bar{\eta}_\mathfrak{q}\colon \mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{q}) \to A/A_1.$$

By the choice of $\mathfrak{q}$ the group $\mathrm{Gal}(\bar{k}_\mathfrak{q}/k_\mathfrak{q})$ acts trivially on A, and we get elements

$$\eta_\mathfrak{q} \in H^1(k_\mathfrak{q}, A), \qquad \eta_\mathfrak{q} \notin H^1_{nr}(k_\mathfrak{q}, A),$$
$$\bar{\eta}_\mathfrak{q} \in H^1(k_\mathfrak{q}, A/A_1) \qquad \bar{\eta}_\mathfrak{q} \notin H^1_{nr}(k_\mathfrak{q}, A/A_1).$$

By the proposition stated above, there is an element α' from $H^1(\mathfrak{G}_{S\cup\{\mathfrak{q}\}}, A)$ which localizes at $\mathfrak{q}$ just to the given class

$$\eta'_\mathfrak{q} = \eta_\mathfrak{q} \bmod H^1_{nr}(k_\mathfrak{q}, A) = \alpha'.$$

Set $\mathfrak{G}' = \mathfrak{G}_{S\cup\{\mathfrak{q}\}}$, $\mathfrak{G}'_0 = \mathrm{Gal}(k_{S\cup\{\mathfrak{q}\}}/K)$. To the solution ψ of (1) unramified outside S corresponds a solution ψ_S of (1_S) and we can associate to ψ_S an element $\chi_S \in H^1(k_S/K, A)^F$. Then

$$\omega' = \mathrm{Res}(\mathfrak{G}' \to \mathfrak{G}'_0)\,\alpha' \in H^1(k_{S\cup\{\mathfrak{q}\}}/K, A)^F$$

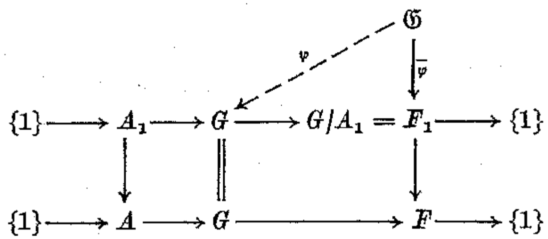
and

$$\chi'_S = \mathrm{inf}\big(H^1(k_S/K, A)^F \to H^1(k_{S\cup\{\mathfrak{q}\}}/K, A)^F\big)\chi_S$$

give a new solution ψ' of (1) corresponding to $\chi'_S + \omega' \in H^1(k_{S\cup\{\mathfrak{q}\}}/K, A)^F$ and a solution $\bar{\psi}'$ of (2) corresponding to $(\chi'_S + \omega') \in H^1(k_{S\cup\{\mathfrak{q}\}}/K, A/A_1)^F$. Thus we have solutions ψ' resp. $\bar{\psi}'$ unramified outside $S \cup \{\mathfrak{q}_1\}$. This last solution induces a proper solution of (2) because localization at $\mathfrak{q}$ and the map $A \to A/A_1$ show that the fixed field, L (say), of the kernel of $\overline{(\chi'_S + \omega')}$

does not coincide with K. On the other hand, $\mathrm{Gal}(L/K)$ is a F-submodule of A/A_1, hence, in virtue of the F-irreducibility of A/A_1, it must be isomorphic to A/A_1. In this way, the solution $\bar{\psi}$ defines a third imbedding problem:

(3)



F_1 acts *via* the canonical epimorphism $F_1 \to F$ on the F-module A_1. The F_1-length of the F_1-module A_1 is not greater than $(m-1)$. Now by induction the proof is complete because for the new module A_1 the field $k(A_1, \zeta_n)$ is contained in the field $k(A, \zeta_n)$.

I would like to thank H.-J. Fitzner (Berlin) who critically read a preliminary version of this paper.

References

[1] A. Dress, *Zu einem Satz aus der Theorie der algebraischen Zahlen*, J. Reine Angew. Math. 216 (1964), pp. 218–219.

[2] K. Haberland, *Der Tatesche Dualitätssatz aus der Galois-Kohomologie über Zahlkörpern*, Dissertation, Berlin 1975.

[3] M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem*, Abh. Math. Sem. Univ. Hamburg 24 (1960), pp. 126–131.

[4] В. В. Ишханов, *Задача погружения с ограниченным ветвлением*, Известия АН СССР, серия матем. 36: 4 (1972), pp. 742–748.

[5] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. 21 (1973), pp. 59–116.

[6] O. Neumann, *Über das Einbettungsproblem für globale Körper bei beschränkter Verzweigung*, Math. Nachr. 71 (1976), pp. 147–152.

[7] G. Poitou, *Cohomologie Galoisienne des modules finis*, Paris 1967.

[8] J.-P. Serre, *Cohomologie Galoisienne*, Lecture notes in mathematics 5, Berlin–Göttingen–Heidelberg 1964.

[9] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proceed. Intern. Congr. Math. Stockholm, 1962, pp. 288–292.

AKADEMIE DER WISSENSCHAFTEN DER DDR
ZENTRALINSTITUT FÜR MATHEMATIK UND MECHANIK
Berlin, DDR

Received on 28. 7. 1975 (747)

ACTA ARITHMETICA
XXXIII (1977)

A new equidistribution property of norms of ideals in given classes

by

R. W. K. Odoni (Exeter)

0. Introduction. In [4] the author obtained the following theorem:

Let K be a finite extension of Q, the rational field. If $\{\mathscr{C}_j\}_{j\in J}$ is any non-empty collection of narrow ideal classes of K, then the number of natural numbers $\leqslant x$ which are norms of integral ideals in $\bigcup_{j\in J} \mathscr{C}_j$ is asymptotically

$$D(K, J)x(\log x)^{E(K)-1}\{1 + O_{K,J}(\log x)^{-C(K,J)}\}, \tag{0.1}$$

where $D(K, J)$ and $C(K, J)$ are positive and $E(K)$ is the Dirichlet density of the set of rational primes admitting in K at least one prime ideal factor of residual degree unity.

Owing to the great complexity of the proof of (0.1) it was not feasible in [4] to attempt a discussion of the relations between the $D(K, J)$, as J varies. It is natural to expect that $D(K, J_1)$ equals $D(K, J_2)$ if J_1 and J_2 are singletons, since the weighted sums

$$\sum_{\mathfrak{a}\in\mathscr{C}, N\mathfrak{a}\leqslant x} 1 \tag{0.2}$$

are well-known to be asymptotically the same for all classes $\mathscr{C}$. However, the unweighted sums in (0.1) are much more difficult to handle. In this paper, we shall prove the following results:

THEOREM 1. *For singletons J_i, $D(K, J_1) = D(K, J_2)$.*

THEOREM 2. *If K/Q is normal, then all but a proportion*

$$O_K\big((\log\log x)^{A(K)}/(\log x)^{B(K)}\big)$$

of the integers $\leqslant x$ which are norms of integral ideals in a given class $\mathscr{C}$ are norms of integral ideals of each class in the coset $\mathscr{C}H$, where H is the group of narrow classes containing fractional ideals of norm unity. (The constant $B(K)$ is positive.)

We remark that if $n = N\mathfrak{a} = N\mathfrak{b}$, where $\mathfrak{a}\in\mathscr{C}$ and $\mathfrak{b}\in\mathscr{D}$, then $\mathscr{C}\mathscr{D}^{-1}\in H$, so $\mathscr{C}H = \mathscr{D}H$, and this indicates the strength of Theorem 2. We also prove