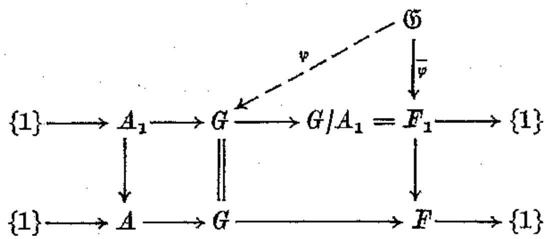
does not coincide with K. On the other hand, $\mathrm{Gal}(L/K)$ is a F-submodule of A/A_1, hence, in virtue of the F-irreducibility of A/A_1, it must be isomorphic to A/A_1. In this way, the solution $\bar{\psi}$ defines a third imbedding problem:

(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

THEOREM 3. *If K/Q is cubic, then the conclusions of Theorem 2 are still valid.*

The proof of Theorem 3 relies on a special argument, and there is no substantial evidence for the conjecture that Theorem 3 extends to arbitrary K.

The methods of proof in this paper are for the most part different from those of [4], and were inspired to some extent by a reading of the fine dissertation of Bernays [1] on the values of binary integral quadratic forms; I am indebted to Prof. A. Schinzel for drawing my attention to this sadly neglected work.

It is of some interest to note that Theorem 1 is still valid if the narrow ideal class group is replaced by any congruence divisor class group in K; Theorem 2 also carries over, provided that the corresponding identity class is invariant under the action of the Galois group of K/Q. Minor modifications of the latter extension of Theorems 1 and 2 yield all the results of Bernays [1] and also an interesting result on genera of forms, stated in § 5.

In § 1 we obtain some general results on the ranges of norms (cf. [4]), upon which we draw at various points in the paper; § 2 is devoted to the proof of Theorem 1. In § 3 we specialize to normal extensions and obtain Theorem 2. Theorem 3 is treated in § 4 by a special device which is unlikely to be fruitful if $[K:Q] > 3$.

1. Properties of ranges. In [4] we considered natural numbers n which were norms of integral ideals; for such n we defined the *range* $R(n)$ to be the set of all narrow classes $\mathscr{C}$ for which $n = N\mathfrak{a}$, $\mathfrak{a} \in \mathscr{C}$ is soluble. Here, as there, it is convenient to consider the collection $\mathscr{A}$ of all non-empty subsets of the narrow ideal class group I_K, defining the product AB of members of $\mathscr{A}$ to be $\{ab; a \in A, b \in B\}$. The fundamental property of ranges is (cf. [4], (1.2)):

LEMMA 1.1. $R(mn) \supseteq R(m)R(n)$, *with equality if* $(m, n) = 1$.

We shall occasionally need to use the following elementary result:

LEMMA 1.2. *Let $A \in \mathscr{A}$. There exists a natural number $n_0(A)$ and a subgroup $S = S(A)$ of I_K such that, for all $n \geqslant n_0(A)$, $A^n = a^n S$ for every $a \in A$; in fact, $S = \mathrm{gp}\{a_1 a_2^{-1}; a_i \in A\}$.*

Proof. Choose any $a \in A$. Then $A = aB$, where $1 \in B$. Consequently we have an ascending chain $B \subseteq B^2 \subseteq B^3 \subseteq \ldots$ of subsets of I_K, which must terminate, so that $B^{n_0} = B^{1+n_0} = \ldots$ If we put $C = B^{n_0}$, we must have $C = C^2$ and it is clear that C is a subgroup of I_K. For $n \geqslant n_0$ we have $A^n = a^n B^n = a^n C$ and we take $S = C$. If we had chosen a_1 instead of a, we would have $A^n = a^n S = a_1^n S_1$ for all large n. Thus S and S_1 are cosets of one another and so coincide. It is now seen that $(aa_1^{-1})^n \in S$ for all n, and the proof is complete.

In view of Lemma 1.2, it is reasonable to hope that norms sufficiently rich in prime factors of the various patterns $B \in \mathscr{B}$ would have ranges of a "stable" type (e.g. cosets of a fixed subgroup of I_K). The next result gives a partial confirmation of this:

LEMMA 1.3. *Let p be any prime. There is a subgroup H^p of I_K such that, for all large n with p^n an ideal norm, $R(p^n)$ is a coset of H^p.*

Proof. We remark that the result is not immediate since in general $R(p^n) \neq R(p)^n$; otherwise we could invoke Lemma 1.2 directly. Let us consider $\mathscr{T} = \{R(p^n); 1 \in R(p^n)\}$. Then $\mathscr{T} \subseteq \mathscr{A}$ is a finite set partially ordered by the relation of inclusion between its elements. Hence it has at least one maximal element M. Then $M = R(p^\mu)$, say, and $M \subseteq M^2 = R(p^\mu)^2 \subseteq R(p^{2\mu})$. Thus, as $1 \in R(p^{2\mu})$, we must have $M = M^2$, and so M is a subgroup of I_K. If $T \subseteq \mathscr{T}$ we have $T = R(p^\tau)$, $1 \in M \subseteq MT = R(p^\mu)R(p^\tau) \subseteq R(p^{\mu+\tau})$, and so $MT = M$, $T \subseteq M$. Thus $M \subseteq \bigcup_{T \in \mathscr{T}} T \subseteq M$, i.e., M is the unique maximal element of $\mathscr{T}$ and $M = \bigcup_{T \in \mathscr{T}} T$.

We now consider $\mathscr{S} = \{R(p^n)\} \supseteq \mathscr{T}$. If N is any maximal element of $\mathscr{S}$, we have $N = R(p^\nu)$, $N \subseteq MN = R(p^\mu)R(p^\nu) \subseteq R(p^{\mu+\nu})$, so, by the maximality of N, $MN = N$. Since $M = M^2 = M^3 = \ldots$, we have $MN^k = N^k$ for all $k \geqslant 1$. We can choose k so that N^k contains 1 and $N^v = n^v H$ for all $v \geqslant k$, where H is a subgroup of I_K and $n \in N$, using Lemma 1.2. Then $M \subseteq MH = H$, whence, by the maximality of M in $\mathscr{T}$, $M = H$. Since $1 \in N^k = H$, we have $N \subseteq MN = N^{k+1}$ and, as N is maximal in $\mathscr{S}$, we find $N = N^{k+1}$ and, since the latter equals $n^{k+1}H = n^{k+1}M$, this shows that N is a coset of M; we write $M = H^p$.

We observe here that the maximal cover of any $S \in \mathscr{S}$ is always SH^p. For, if N is a maximal cover for S, $S \subseteq N = nH^p$, say. Hence, if $s \in S$, $sH^p = nH^p$, i.e., $SH^p = nH^p = N$. Now let $D = \{n \geqslant 1; R(p^n) \neq \emptyset\} \cup \{0\}$; it is the monoid generated by the residual degrees $f_1, \ldots, f_r$ of the prime ideals of K lying above p. Suppose that $H^p = R(p^h)$. Then for any $d \in D$, $R(p^{h+d}) \subseteq R(p^d)H^p =$ maximal cover of $R(p^d)$, so that $R(p^{h+d}) = R(p^d)H^p$. We can write h as $\sum n_i f_i$; then we have shown that $R(p^v)$ is a coset of H^p when $v = \sum n_i' f_i$ and each $n_i' \geqslant n_i$. The set of all such v is an ideal in D and so contains all large elements of D, as required.

We note that H^p may be characterized as the set of all classes in I_K containing fractional ideals of norm unity and involving only the prime ideal factors of p. If H denotes the subgroup of I_K consisting of those classes containing fractional ideals whose norms are norms of narrow principal ideals, then H is also the group of all classes containing fractional ideals of norm unity (as in the statement of Theorem 2), and it is readily verified that H is the compositum of all the H^p, as p varies through all primes.

In H^p there is a subgroup W^p which is important in the sequel; we are concerned here only with primes p for which $R(p) \neq \emptyset$. Then W^p is defined as the subgroup of I_K such that $R(p)^n$ is a coset of W^p for all large n (its existence being guaranteed by Lemma 1.2). It is necessary later to know whether H is the compositum $W = \prod W^p$, taken over all unramified primes which are norms. In the normal case this must be so:

LEMMA 1.4. *If K/Q is normal then $H = W$.*

Proof. If p is any prime then all prime ideal factors of p have the same residual degree f, by normality, and it is clear that $R(p^{nf}) = R(p^f)^n$ for all $n \geqslant 1$. Now the Galois group G of K/Q acts transitively on the various $\mathfrak{p}$ lying over p in K, and it also acts on I_K (not necessarily transitively). It follows that $R(p^f)$ consists precisely of the single orbit $\{\mathscr{C}^\sigma\}_{\sigma\in G}$ for some $\mathscr{C} \in R(p^f)$. The subgroup H^p is thus $\mathrm{gp}\{\mathscr{C}^{\sigma-\tau}\}_{\sigma,\tau\in G}$. Now there exist infinitely many prime ideals of residual degree 1 in the class $\mathscr{C}$, since $\sum_{\mathfrak{p}\in\mathscr{C}} (N\mathfrak{p})^{-1}$ diverges. Hence we can find infinitely many unramified primes q with $\mathscr{C} \in R(q)$. By transitivity, $R(q) = R(p^f)$ with p as above, and then $H^p = H^q = W^q$, which proves the lemma. We shall show in § 4 that Lemma 1.3 also holds in any cubic field. It is not clear that it should hold for all K; if it does, then Theorem 2 is true for arbitrary K.

2. Analytic results. In order to obtain Theorems 1 and 2, we consider the following well-known decomposition of the set of natural numbers: each such n is uniquely expressible in the form $n = fm$, where $(m, f) = 1$, f is squarefree, and m is squarefull. By Lemma 1.1, we can say that every ideal norm is (uniquely) a product fm, where f is a squarefree norm involving only unramified prime factors, while m is a squarefull norm, multiplied possibly by a norm composed entirely of ramified primes, and $(m, f) = 1$. All our analytic results derive ultimately from

PROPOSITION 2.1. *Let m be a (squarefull norm-by-ramified norm), as above; if $\mathscr{C}$ is any narrow ideal class in K and μ is the Möbius function, then*

$$(2.1)\qquad \sum_{\substack{\text{unram. norms } f\leqslant y\\ (f,m)=1\\ \mathscr{C}\in R(mf)}} \mu^2(f)$$

$$= \frac{a\big(R(m)\big)}{\psi(m)}\, y(\log y)^{E(K)-1} + O_K\big(y(\log y)^{E(K)-1-\gamma}(\log\log y \log\log m)^\beta\big),$$

where $\gamma > 0$, β and γ depend only on K, $a\big(R(m)\big)$ depends only on the range of m, not on $\mathscr{C}$, and $\psi(m)$ is the sum of the reciprocal of the unramified squarefree norms dividing m; as usual, $E(K)$ is the Dirichlet density of the set of rational primes admitting in K at least one prime ideal factor of residual degree unity.

Proof. We remark that for f counted in (2.1) $R(mf) = R(m)R(f)$, so we are interested in the condition $\mathscr{C} \in R(m)R(f)$. Since $\mu^2(f) = 0$ unless f is squarefree, we know that the only relevant f have $R(f) = \prod_{p|f} R(p)$. If $\mathscr{B}^*$ is the set of patterns (cf. [4]) of unramified primes with non-empty $R(p)$, then for each $B \in \mathscr{B}^*$ we let $\omega_B(f)$ be the number of primes of pattern B dividing f, and we write R_B for $R(p)$, $p \leftrightarrow B$. Thus $R(f) = \prod_{B\in\mathscr{B}} R_B^{\omega_B(f)}$. If each $\omega_B(f) \geqslant \omega_B^0$, say, we have $R_B^{\omega_B(f)} = r_B^{\omega_B(f)} W^B$, where $W^B = W^p$ for $p \leftrightarrow B$, and so $R(f) = \prod_{B\in\mathscr{B}^*} r_B^{\omega_B(f)} W$, a coset of W. Thus, when f is sufficiently rich in prime divisors of each pattern $B^* \in \mathscr{B}$, we have

$$R(mf) = R(m)\prod r_B^{\omega_B(f)} W = \prod r_B^{\omega_B(f)} \cdot R(m)W.$$

Now $R(m)W$ is a complete union of cosets of W, $R(m)W = \bigcup \varrho_j W$, an irredundant decomposition. Consequently,

$$(2.1\text{A})\qquad R(mf) = \bigcup_j \varrho_j \prod_B r_B^{\omega_B(f)} W,$$

if f is "rich enough in each pattern $B \in \mathscr{B}^*$". It follows that $\mathscr{C} \in R(mf)$ if and only if $\prod_B r_B^{\omega_B(f)}$ belongs to (precisely) one of the cosets $\mathscr{C}\varrho_j^{-1}W$, again assuming that f is rich enough in each pattern $B \in \mathscr{B}^*$. Our first task now is to show that those $f \leqslant y$ not rich enough in each pattern $B \in \mathscr{B}^*$ contribute only a negligible part to (2.1). In fact, for each $B \in \mathscr{B}^*$, the number of integers counted in (2.1) and involving only $< \omega_B^0$ factors of pattern B is

$$O_K\big(y(\log\log y)^{\beta(B)}(\log y)^{E(K)-1-\gamma(B)}\big),$$

where $\beta(B) \leqslant \omega_B^0$ and $\gamma(B)$ is the Dirichlet density of rational primes $p \leftrightarrow B$, $E(K)$ being the Dirichlet density of primes which are norms of prime ideals. This result follows from a weak version of a Tauberian theorem of H. Delange [3], once the existence of $\gamma(B)$ and $E(K)$ is established; for the latter, see [4], § 4. From the above we see that there exist positive constants β and γ such that the f counted in (2.1) which are deficient in at least one pattern $B \in \mathscr{B}^*$ contribute only

$$O_K\big(y(\log\log y)^{\beta}(\log y)^{E(K)-\gamma-1}\big)$$

to (2.1).

To obtain Proposition 2.1, we now concentrate on those f in (2.1) rich enough in each pattern $B \in \mathscr{B}^*$. Then the condition for $R(mf)$ to contain $\mathscr{C}$ is that $\prod_B r_B^{\omega_B(f)}$ belong to one of a particular family of cosets of W, the *number of these cosets being independent of the choice of* $\mathscr{C}$. This is because the union of all R_B, $B\in\mathscr{B}^*$ is I_K, since there exist infinitely many prime ideals of residual degree unity in each class of I_K. We are therefore led to the problem of counting $\mu^2(f)$ for those unramified norms f prime to m having $\prod r_B^{\omega_B(f)}W$ equal to a given coset aW. Consider all ordered $\mathscr{B}^*$-tuples (n_B) of integers such that $\prod r_B^{n_B}\cdot W = W$. These form a lattice $\mathscr{L}$ of maximal rank in $\boldsymbol{R}^{\mathscr{B}^*}$, and those (n_B) for which $\prod r_B^{n_B}\in aW$ form a coset of $\mathscr{L}$; there is a natural isomorphism $\boldsymbol{Z}^{\mathscr{B}^*}/\mathscr{L}\cong I_K/W$, induced by the mapping $(n_B)\to\prod r_B^{n_B}W$. The condition $(n_B)\in\mathscr{L}+\boldsymbol{c}$ is thus expressible in terms of the group characters of I_K/W, a finite abelian group. It is now clear that the condition $\mathscr{C}\in R(mf)$ for rich enough f is equivalent to the pair of conditions:

$$\text{(2.2)}\qquad \begin{array}{ll}\text{(i)} & \omega_B(f)\geqslant\omega_B^0;\\ \text{(ii)} & \big(\omega_B(f)\big)_{B\in\mathscr{B}^*}\in\bigcup_{j\in J}\boldsymbol{c}_j+\mathscr{L}.\end{array}$$

Let us consider for a fixed $\boldsymbol{c}\in\boldsymbol{Z}^{\mathscr{B}^*}$ the condition $\big(\omega_B(f)\big)\in\mathscr{L}+\boldsymbol{c}$, which we write as $\boldsymbol{\omega}\in\mathscr{L}+\boldsymbol{c}$. Since $\mathscr{L}$ is finitely-generated and contained in $\boldsymbol{Z}^{\mathscr{B}^*}$, the condition under consideration is equivalent to a finite system of simultaneous linear congruences modulo various integers, to be satisfied by the components of $\boldsymbol{\omega}-\boldsymbol{c}$. Suppose that the system in question is

$$\sum_B a_{iB}\big(\omega_B(f)-c_B\big)\equiv 0 \pmod{k_i},\qquad i=1,\ldots,N.$$

Then the required sifting function for the $\boldsymbol{\omega}\in\mathscr{L}+\boldsymbol{c}$ is

$$\text{(2.3)}\qquad \prod_{i=1,\ldots,N} k_i^{-1}\sum_{l_i\,(\mathrm{mod}\,k_i)} e\Big(l_i k_i^{-1}\Big(\sum_B a_{iB}\big(\omega_B(f)-c_B\big)\Big)\Big),$$

where $e(x)=e^{2\pi ix}$.

From this we are led to consider the Dirichlet series

$$\text{(2.4)}\qquad \sum_{\boldsymbol{\theta}} a(\boldsymbol{\theta};\boldsymbol{c})\prod_{B\in\mathscr{B}^*}\prod_{p_B\nmid m}(1+\theta_B p_B^{-s})\qquad(\sigma=\operatorname{Re}s>1),$$

where $\boldsymbol{\theta}=(\theta_B)_{B\in\mathscr{B}^*}$ runs through certain vectors of roots of unity, of the various orders k_i introduced above. By choosing the $\boldsymbol{\theta}$ in an appropriate way, the series (2.4) becomes precisely $\sum\mu^2(n)n^{-s}$ taken over all those n composed entirely of primes from the various $B\in\mathscr{B}^*$ not dividing m, and such that $\big(\omega_B(n)\big)_{B\in\mathscr{B}^*}$ lies in $\mathscr{L}+\boldsymbol{c}$. In (2.4), the dominant contribution will be shown to arise from the term with each $\theta_B=1$, and we note that $a(1,\ldots,1)$ is the same for all choices of $\boldsymbol{c}$. More precisely, the individual products in (2.4) may be analysed using Čebotarëv's density theorem, as in [4]. We have

$$\text{(2.5)}\qquad \sum_{p_B} p_B^{-s}=a(B)\log\frac{1}{s-1}+A_B(s)\qquad(\sigma>1),$$

where $A_B(s)$ is regular and satisfies

$$\text{(2.6)}\qquad |A_B(s)|=O_{K,B}\big(\log\log(2+t^2)\big)$$

in a region

$$\text{(2.7)}\qquad s=\sigma+it,\qquad \sigma>1-c(K)/\log(2+t^2),$$

while $a(B)$ is the Dirichlet density of the set of rational primes p_B of pattern B. Consequently, for $\sigma>1$,

$$\text{(2.8)}\qquad \prod_{p_B}(1+\theta_B p_B^{-s})=H_B(s,\theta_B)\exp\Big\{a(B)\,\theta_B\log\frac{1}{s-1}\Big\},$$

where $H_B(s,\theta_B)$ is regular and $O\big((\log 2+t^2)^{c(K)}\big)$ in the region (2.7). If we write $H(s,\boldsymbol{\theta})$ for $\prod_{B\in\mathscr{B}^*}H_B(s,\theta_B)$, we have

$$\text{(2.9)}\qquad \prod_{B\in\mathscr{B}^*}\prod_{p_B\nmid m}(1+\theta_B p_B^{-s})=\frac{H(s,\boldsymbol{\theta})}{\psi(s,m,\boldsymbol{\theta})}\exp\Big(\sum_{B\in\mathscr{B}^*}a(B)\,\theta_B\log\frac{1}{s-1}\Big)$$

in the same region where $\psi(s,m,\boldsymbol{\theta})=\prod_{B\in\mathscr{B}^*}\prod_{p_B|m}(1+p_B^{-s}\theta_B)$. Following [4], § 0 we find that

$$\text{(2.10)}\qquad \sum_{\substack{\text{unram. norms } f\\ (f,m)=1\\ \omega(f)\in\boldsymbol{c}+\mathscr{L}}}\mu^2(f)=\frac{k}{\psi(m)}y(\log y)^{E-1}+O_K\big(y(\log y)^{E-1-\varrho}\log\log m\big),$$

where $E=E(K)$ of Proposition 2.1, ϱ is positive,

$$\text{(2.11)}\qquad \psi(m)=\prod_{B\in\mathscr{B}^*}\prod_{p_B|m}(1+p_B^{-1}),$$

and k is the same for all $\boldsymbol{c}$ and all relevant m with the same range. If we sum (2.10) over all cosets $\boldsymbol{c}_j+\mathscr{L}$ occurring in (2.2), then we obtain Proposition 2.1, except that we have possibly violated (2.2) (i); however, to remove the f insufficiently rich in some pattern B will add only an error $O_K\big(y(\log\log y)^{B}(\log y)^{E-1-\gamma}\big)$, by an argument already encountered, and Proposition 2.1 is proved.

We now observe that two squarefull-by-ramified norms m with the same range $R(m)$ give the same number of cosets $\boldsymbol{c}_j+\mathscr{L}$ in (2.2). Thus (2.1) gives

$$\text{(2.12)}\qquad \sum_{\substack{\text{unram. norms } f\\ (f,m)=1,\, fm\leqslant x\\ \mathscr{C}\in R(fm)}}\mu^2(f)$$

$$=\frac{a\big(R(m)\big)}{m\psi(m)}x\Big(\log\frac{x}{m}\Big)^{E-1}+O_K\Big(\frac{x}{m}\Big(\log\frac{x}{m}\Big)^{E-1-\lambda}\Big(\log\log\frac{x}{m}\Big)^{\beta}\log\log m\Big),$$

where $\lambda > 0$, and $a(R(m))$ depends only on $R(m)$, not on $\mathscr{C}$. The estimate (2.12) is not very efficient for $m > x^{1-\varepsilon}$ if ε is small, but in that event the left side of (2.12) is trivially $O(x^\varepsilon)$.

In order to obtain Theorem 1 it remains to vary m in (2.12). We first consider a fixed range $R = R(m)$, and sum (2.12) over all squarefull-by-ramified norms $m \leqslant x$ of range R. From the $m \leqslant x^{1-\varepsilon}$ we get the contribution

$$(2.13)\quad a(R)\sum_{m\leqslant x^{1-\varepsilon}}^{*}(m\psi(m))^{-1}x(\log x-\log m)^{E-1}+ \\ + O_K\Big(x(\log x)^{\varepsilon-1-\lambda}(\log\log x)^{\beta'}\sum_{m\leqslant x^{1-\varepsilon}}^{*}m^{-1}\Big),$$

where the * indicates that only the squarefull-by-ramified norms of range R are to be included in the summation, and β' is a constant. Now $(1-\log m/\log x)^{E-1} = 1+\theta\log m/\log x$ if $m \leqslant x^{1-\varepsilon}$, where θ is bounded by a function of ε. Consequently, (2.13) yields

$$(2.14)\quad a(R)x(\log x)^{E-1}\sum_{m\leqslant x^{1-\varepsilon}}^{*}(m\psi(m))^{-1}+ \\ +\theta^* a(R)x(\log x)^{E-2}\sum_{m\leqslant x^{1-\varepsilon}}^{*}\log m(m\psi(m))^{-1}+ \\ + O_K\Big(x(\log x)^{E-1-\lambda}(\log\log x)^{\beta'}\sum_{m\leqslant x^{1-\varepsilon}}^{*}m^{-1}\Big),$$

where θ^* is bounded by a function of ε. We show next that each of the infinite series

$$\sum\nolimits^{*}(m\psi(m))^{-1},\quad \sum\nolimits^{*}\log m(m\psi(m))^{-1},\quad \sum\nolimits^{*}m^{-1}$$

is convergent. Indeed, let $S(n)$ be the number of relevant $m \leqslant n$; then $S(n)$ is trivially $O(n^{1/2+\delta})$ for any $\delta > 0$. Then it suffices to show that $\sum^*\log m/m$ converges (since $\psi(m)\geqslant 1$), and we obtain convergence from the estimate for $S(n)$, *via* summation by parts. In fact, we find

$$\sum_{m\leqslant x^{1-\varepsilon}}^{*}(m\psi(m))^{-1} = \sum\nolimits^{*}(m\psi(m))^{-1}+O(x^{(1-\varepsilon)(\delta-1/2)}),$$

$$\sum_{m\leqslant x^{1-\varepsilon}}^{*}\log m(m\psi(m))^{-1} = \sum\nolimits^{*}\log m(m\psi(m))^{-1}+O(\log x\cdot x^{(1-\varepsilon)(\delta-1/2)}),$$

$$\sum_{m\leqslant x^{1-\varepsilon}}m^{-1} = \sum\nolimits^{*}m^{-1}+O(x^{(1-\varepsilon)(\delta-1/2)}).$$

For those m with $x^{1-\varepsilon} < m \leqslant x$ we use the trivial bound $O(x^\varepsilon)$ for (2.12), with the observation that the number of m involved is at most $O(x^{1/2+\delta})$, so the net contribution is $O(x^{1/2+\delta+\varepsilon})$. We can take e.g. $\varepsilon = 1/4$, $\delta = 10^{-2}$, and then we obtain Theorem 1 by summing over all available ranges $R = R(m)$, noting that in each case (2.14) and its refinements are independent of the choice of $\mathscr{C}$.

Finally, by comparing our results with Theorem 1 of [4], we see that the powers of $\log\log x$ appearing in our error terms here are unduly pessimistic and may be discarded.

3. Proof of Theorem 2. A crucial point in the proof of Theorem 1 was the remark that only the squarefree unramified norms sufficiently rich in each pattern $B\in\mathscr{B}^*$ matter in producing the dominant part of the asymptotic expansion. But any norm involving these and any squarefull-by-ramified norm necessarily has range containing a coset of W (in the notation of §§ 1 and 2). In the case where K/Q is normal, Lemma 1.4 gives $W = H$. Thus these ranges are precisely full cosets of H. If the range of a norm is not such a coset, the norm must be deficient in primes of some pattern $B\in\mathscr{B}^*$, and so, by the argument of § 2, it must be one of only $O_K(x(\log\log x)^{\beta'}(\log x)^{E-\gamma-1})$ norms in $[1, x]$. These comments suffice to prove Theorem 2.

4. Proof of Theorem 3. We now assume that K/Q is cubic; if it were normal, we could invoke Theorem 2. Thus we may assume that $K = Q(a)$, where a satisfies a cubic irreducible equation over Q with Galois group S_3, the symmetric group on 3 symbols, and the Galois hull $\bar{K}/Q$ of K/Q is a sextic extension with $\mathrm{Gal}\bar{K}/Q \cong S_3$. In view of the argument of § 3, it will suffice to show that $W = H$ for the field K.

Let us consider a rational prime p. Assume first that it is ramified in K. Then *either* $(p) = \mathfrak{p}^3$, $N\mathfrak{p} = p$ and $W^p = H^p = 1$, a trivial case, *or* $(p) = \mathfrak{p}^2\mathfrak{q}$, where $N\mathfrak{p} = N\mathfrak{q} = p$. If $\mathfrak{p}$ belongs to the narrow class X, then $\mathfrak{q}$ belongs to X^{-2}, and we readily see that $W^p = H^p = \mathrm{gp}\,X^3$. To deal with such ramified p, it will suffice to show that there exists an unramified prime q with $\mathrm{gp}\,X^3 \subseteq W^q$. This will emerge later.

Now consider an unramified prime p, $(p) = \mathfrak{p}\mathfrak{q}$, with $\mathfrak{p}$ of residual degree 1 and $\mathfrak{q}$ of residual degree 2, $\mathfrak{p}$ in class Y. Then $W^p = 1$ and $H^p = \mathrm{gp}\,Y^3$. We shall show that there exists a rational prime q splitting completely in K (and hence in $\bar{K}$) with $H^p \subseteq W^q$. Consider the decomposition of p in $\bar{K}$. By simple counting arguments, (p) breaks into 3 unramified factors in $\bar{K}$, each of residual degree 2 over Q. Hence $\mathfrak{q}$ is the $(\bar{K}/K)$-norm of a prime ideal of $\bar{K}$. We deduce that the class Y contains norms of fractional ideals of $\bar{K}$. There will be infinitely many prime ideals of residual degree unity over Q whose $(\bar{K}/K)$-norms lie in Y; these prime ideals lie over rational primes q which split in $\bar{K}$ (and thus in K). Suppose such a $(q) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ in K, where $\mathfrak{q}_1$ belongs to Y and $\mathfrak{q}_2$ belongs to Z, say. (We neither know nor care which class Z is !). Then

$$H^q = W^q = \mathrm{gp}\{YZ^{-1}, Y^3\} \supseteq H^p,$$

as required.

Finally, we return to the ramified p with $H^p = \mathrm{gp}\, X^3$. Then, in $\bar{K}$, there are 3 prime ideal factors of (p), each of residual degree 1 and ramification index 2 over Q. Thus $\mathfrak{p}$ is the $\bar{K}/K$-norm of an ideal of $\bar{K}$, that is, the class X contains $(\bar{K}/K)$-norms of ideals. We can now proceed as above to find a rational prime q, completely split in $\bar{K}$, with $H^q = W^q \supseteq H^p$. We have now shown that $H = W$ for any cubic field.

5. Concluding remarks. The method of § 2 can be adapted (cf. [5]) to prove the following result on the representation of integers by binary integral quadratic forms:

THEOREM 4. *Let $D \equiv 0$ or $1 \pmod 4$ be a discriminant b^2-4ac of primitive binary integral quadratic forms. With "probability one" a randomly chosen positive integer prime to $2D$, and with specified values for the genus characters of D, will be integrally represented by every form in the appropriate genus. That is, only a proportion $O\big((\log\log x)^A(\log x)^{-B}\big)$ of the integers in question in the interval $[1, x]$ will fail to be represented by all the forms of the genus, where $B > 0$.*

An approach to this result is implicit in Bernays [1], although he does not give the result an explicit formulation; the key observation is that if $D = df^2$, where d is a field discriminant, then one needs to consider ideal classes $(\mathrm{mod}^X f)$, i.e. $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a} = (a)\mathfrak{b}$, where $Na > 0$ and $a \equiv 1$ $(\mathrm{mod}^X f)$, in the field $K = Q(\sqrt{d})$. Since the principal class $(\mathrm{mod}^X f)$ is invariant under the action of $\mathrm{Gal}(K/Q)$, the remarks of § 0 suffice to indicate the lines of the proof, which resembles that of Theorem 2 quite closely.

We remark in closing that the restriction (in Theorem 4) to integers prime to $2D$ may be dropped; this is achieved by replacing the ideal classes $(\mathrm{mod}^X f)$ by strict equivalence classes of binary quadratic forms of discriminant D, in accordance with the well-known correspondence principle, and by the use of some elementary results on the classes of forms reprenting a given prime. This more general result appears to have been first proved by Bredihin and Linnik [2], by another method.

References

[1] P. Bernays, *Über die Darstellung... durch primitiven binaren quadratischen Formen* (Dissertation), Gottingen 1912.

[2] Б. М. Бредихин, Ю. В. Линник, *Асимптотика и эргодические свойства решений обобщенного уравнения Гарди-Литтльвуда*, Мат. сб. 71 (1966), pp. 145–161.

[3] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Ann. Sci. de l'Ecole Norm. Sup. 73 (1956), pp. 15–74.

[4] R. Odoni, *On the norms of algebraic integers*, Mathematika 22 (1975), pp. 71–80.

[5] — *Norms of integers in a full module ... binary integral quadratic forms*, ibid. 22 (1975), pp. 108–111.

Received on 18. 8. 1975
and in revised form on 13. 2. 1976 (751)