ACTA ARITHMETICA
LII (1989)

On the distribution of norms of ideals in given ray-classes and the theory of central ray-class fields

by

R. W. K. ODONI (Exeter)

Introduction. Let K be an algebraic number field (thus a finite extension of the rational field $\boldsymbol{Q}$), and let $\mathfrak{f}$ be some conductor in K, containing as factors all the real infinite places of K (each to the first power). We write $\mathfrak{f} = \mathfrak{f}'\infty$, where $\mathfrak{f}'$, the "finite part" of $\mathfrak{f}$, can be regarded as an (integral) ideal in $\mathfrak{O}_K$, the ring of integers of K. We shall be concerned with various properties of the ray-class group (mod$^\times \mathfrak{f}$) of K, which we denote by $A(K, \mathfrak{f})$, or just by A when there is no danger of confusion. It is well known ([3], p. 112) that A is a finite abelian group. As is usual in group theory, when $X, Y \in 2^A$ (the power set of A), we define the product XY to be $\{xy;\ x \in X,\ y \in Y\}$, with the convention that $X\emptyset = \emptyset X = \emptyset$ (the empty set) for all $X \in 2^A$. It is clear that $X \subseteq Y$ implies $XZ \subseteq YZ$ for all $X, Y, Z \in 2^A$, and it is trivial to verify that multiplication and inclusion induce on 2^A the structure of a partially ordered finite commutative monoid, with identity element $\mathbf{1} := \{1_A\}$, where 1_A is the identity of A, i.e. the principal ray-class (mod$^\times \mathfrak{f}$).

Now let $1 \leqslant n \in \boldsymbol{Z}$ (the ordinary integers). We define the *range* $R(n)$ of n via

$$R(n) := \{[\mathfrak{a}];\ N\mathfrak{a} = n\}, \tag{0.1}$$

where $\mathfrak{a}$ runs over all (integral) ideals of $\mathfrak{O}_K$ (written $\mathfrak{a} \lhd \mathfrak{O}_K$) sa..sfying $\mathfrak{a} + \mathfrak{f}' = \mathfrak{O}_K$, while $N\mathfrak{a}$ is the absolute norm of $\mathfrak{a}$ (thus $\# \mathfrak{O}_K/\mathfrak{a}$) and $[\mathfrak{a}]$ is the ray-class of $\mathfrak{a}$ (mod$^\times \mathfrak{f}$). Thus $R(n) \in 2^A$, and $R(n) = \emptyset$ if and only if there is no $\mathfrak{a} \lhd \mathfrak{O}_K$ prime to $\mathfrak{f}'$ with norm n. Our first aim in this paper is to give a detailed analysis of the variation of $R(n)$ with n. We shall carry this out largely within the framework of the classical global theory of classfields, making extensive use of Dirichlet series and the Chebotarev density theorem. Eventually we shall derive as corollaries new, purely algebraic results, some of which can be translated easily into corresponding statements in the cohomological/idèle-theoretic version of classfield theory, while others seem more natural in the traditional setting.

In [5], [6] we considered the special case $\mathfrak{f}' = \mathfrak{O}_K$, so that $A = A(K, \mathfrak{f})$ reduces to the (narrow) ideal class group of K. For various special fields K we showed in [5] that there is a sort of "equidistribution" theorem for norms of ideals in given narrow classes, and also deduced that, in such cases, "almost all" norms have a *maximal range* (see Section 2 for definitions). We shall improve considerably on the results of [5], [6], eliminating the need for any special hypotheses about K and $\mathfrak{f}$. Instead we shall introduce new kinds of Dirichlet series, whose singularity structure and meromorphic continuations will be derived from the Chebotarev density theorem, together with standard results on tensor products of induced representations of finite groups. By applying the Mellin transformation and Perron's summation formula we are then able to obtain rather precise asymptotic expansions describing the distribution of those n with prescribed values of $R(n)$. In particular we shall obtain an equidistribution theorem, together with a proof that "almost all" norms have a maximal range, valid for arbitrary K and $\mathfrak{f}$. Since the precise results can only be made intelligible after some preliminary background material and definitions, we postpone the exact formulations of our main theorems until Section 3.

An unexpected bonus coming out of our analysis is the opportunity to generalise the notion of central classfield, originally due (independently) to A. Scholz [9] and A. Fröhlich [1], [2], and defined only when K/Q is Galois. We show in Section 9 how to frame a suitable definition of central classfield (mod$^x \mathfrak{f}$) of K for arbitrary K and $\mathfrak{f}$.

The exposition of this paper is organised as follows. In Section 1 we study the structure of 2^A, and deduce the existence of d-maximal ranges; these are shown to be single cosets of certain subgroups of A. In Section 2 we consider "Frobenian properties" of ranges (and various associated numerical functions), and indicate how some preliminary, qualitative results on the distribution of $R(n)$ can be derived directly by means of the author's "method of Frobenian functions" [7], [8], developed some time after the publication of [5], [6]. Unfortunately these preliminary results only yield the existence of asymptotic expansions of a particular type, with little or no information about certain critical exponents and coefficients, and are insufficient even for a proof of our equidistribution theorem. To obtain the required extra information we must introduce more sophisticated methods, whose development and exploitation take up the major part of this paper. It is here that the systematic use of nonabelian representation theory shows to decisive advantage, compared with our earlier methods.

In Section 3 we formulate the precise statements of our main theorems, while in Section 4 we prove some (mostly elementary) lemmas on characters which will be used repeatedly in the remainder of the paper. Sections 5–8 are devoted to the proofs of our main results, Theorems I–IV. In Section 9 we formulate our generalised definition of central classfield and show that it includes the classical concept as a special case, while Section 10 consists of a survey of related literature, together with a discussion of prospects for further applications of our methods.

1. Maximal ranges. We recall the definition of $R(n)$ given in (0.1). From the uniqueness of factorisation of ideals and (total) multiplicativity of absolute norms it is a trivial exercise to prove that

$$R(mn) \supseteq R(m)R(n), \tag{1.1}$$

with equality if $(m, n) = 1$. Despite its simplicity (1.1) turns out to be fundamental in all that follows.

1A. Now let $1 \leqslant d \in \boldsymbol{Z}$ be fixed; we denote by N_d the set $\{n;\ 1 \leqslant n \in \boldsymbol{Z},\ (n, d) = 1\}$. We shall consider the ranges $R(n)$ for $n \in N_d$. The set $\mathcal{R}_d := \{R(n);\ n \in N_d\}$ is finite (since A is), and non-trivial, since $1 \in N_d$ and $R(1) = \{1_A\}$. Thus $\mathcal{R}_d$ possesses maximal elements with respect to inclusion in 2^A, which we call *d-maximal ranges.* (Ultimately it will be shown that these d-maximal ranges do not really depend on d at all, but this is a highly non-trivial fact which cannot be proved until Section 7.) It is clear that every member of $\mathcal{R}_d$ is contained in at least one d-maximal range. In fact we shall see shortly that every $(\emptyset \neq)\ X \in \mathcal{R}_d$ has a unique "d-maximal cover", which can be explicitly calculated.

First we note that $\mathbf{1} := \{1_A\} = R(1) \in \mathcal{R}_d$, so that certainly there must exist d-maximal ranges which contain $\mathbf{1}$. Let M_i $(i = 1, 2)$ be two such, $M_i = R(m_i)$ $(m_i \in N_d)$. Then $R(m_1 m_2) \in \mathcal{R}_d$, while $R(m_1 m_2) \supseteq R(m_1)R(m_2) = M_1 M_2 \supseteq M_1 \cup M_2$, since $1_A \in M_1 \cap M_2$. Since the M_i are d-maximal we deduce that $R(m_1 \cdot m_2) = M_1 M_2 = M_1 = M_2$. Hence there is precisely one d-maximal range containing $\mathbf{1}$; we denote it by H_d. The above argument also shows that $\emptyset \neq H_d = (H_d)^2$, and, since A is finite, we see that H_d is a subgroup of A.

Now let $N = R(n)$ be any d-maximal range, and let $H = H_d = R(h)$, with $n, h \in N_d$. Then $hn \in N_d$ and $R(hn) \in \mathcal{R}_d$, while $R(hn) \supseteq R(h)R(n) = HN \supseteq N$, since $\mathbf{1} \subseteq H$. Since N is d-maximal we deduce that $HN = N$, and this implies that N is a union of cosets of $H = H_d$. From the relation $HN = N$ in 2^A we see that $N^s H = N^s$ for all $s \geqslant 1$. Now we can choose s such that $1_A \in N^s$ (for example, $s = \# A$ would do). For such s we have $n^s h \in N_d$, $R(n^s h) \in \mathcal{R}_d$ and $R(n^s h) \supseteq R(n^s)R(h) \supseteq N^s H \supseteq H$. Since H is d-maximal we have $N^s H = H = N^s$. Let $x, y \in N$. Then x^s and $x^{s-1} y \in N^s = H$, so that $xH = yH$. But we showed above that N is a union of cosets of H, so we must have $N = xH = yH$, a single coset of $H = H_d$.

Now let $R(t) \in \mathcal{R}_d$, $x \in R(t)$, $t \in N_d$, and let $R(t) \subseteq N$, with N d-maximal. Then $x \in N$ and so $N = xH = R(t)H$. This shows that $R(t)H_d$ is the unique d-maximal cover of $R(t)$ (provided that the latter is non-empty). We recall

([3], p. 112) that every ray-class $(\bmod^{\times} \mathfrak{f})$ contains integral ideals prime to any preassigned ideal. Hence every $a \in A$ belongs to some $R(t)$ with $t \in N_d$, so that $R(t)\,H_d = aH_d$. It follows that the d-maximal ranges are precisely the cosets of H_d in A.

1B. We now seek characterisations of H_d as a subroup of A. First, if $h \in N_d$, $R(h) = H_d$, then, given $\eta \in H_d$, we can find integral $\mathfrak{a}$, $\mathfrak{b}$ prime to $\mathfrak{f}'$ such that $N\mathfrak{a} = N\mathfrak{b} = h$ and $[\mathfrak{a}] = \eta$, $[\mathfrak{b}] = 1_A$. (Here $[\cdot]$ denotes ray-class $(\bmod^{\times} \mathfrak{f})$.) Then $[\mathfrak{a}\mathfrak{b}^{-1}] = \eta$, while $N(\mathfrak{a}\mathfrak{b}^{-1}) = 1$ and $\mathfrak{a}\mathfrak{b}^{-1}$ is prime both to $\mathfrak{f}'$ and to d. Hence $H_d \subseteq H_d^*$, the subgroup of A consisting of those $[\mathfrak{c}]$, where $\mathfrak{c}$ is a fractional ideal prime to $d\mathfrak{f}'$ and of norm 1. Conversely, if $\mathfrak{c}$ is any such fractional ideal, and $[\mathfrak{c}] = \eta$, we can write $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b} \lhd \mathfrak{D}_K$, $\mathfrak{a} + d\mathfrak{f}' = \mathfrak{b} + d\mathfrak{f}' = \mathfrak{D}_K$ and $N\mathfrak{a} = N\mathfrak{b} = n \in N_d$. Then $[\mathfrak{a}], [\mathfrak{b}] \in R(n) \subseteq R(n)\,H_d$, a single coset of H_d, and thus $[\mathfrak{c}] = [\mathfrak{a}\mathfrak{b}^{-1}] \in H_d$. This implies that $H_d^* \subseteq H_d$, and, in view of the previous inclusion, we deduce that $H_d = H_d^*$.

An alternative characterisation of H_d is now easily obtained; for H_d^* is (trivially) identical with the set of ray-classes $(\bmod^{\times} \mathfrak{f})$ which contain fractional ideals $\mathfrak{c}$, prime to $d\mathfrak{f}'$, such that $N\mathfrak{c} = N_{K/Q}(\alpha)$ for some $\alpha \equiv 1 (\bmod^{\times} \mathfrak{f})$ in K^*. (The latter means that α is totally positive, and expressible as β/γ, where β and γ are both in $\mathfrak{D}_K$ and congruent to $1 (\bmod\ \mathfrak{f}')$.)

We now consider the effect of changing d. Clearly, if $1 \leqslant e \equiv 0 (\bmod\ d)$, then $N_e \subseteq N_d$ and $\mathscr{R}_e \subseteq \mathscr{R}_d$. Hence, for some $n \in N_e$, we have $R(n) = H_e \ni 1_A$, and so the d-maximal cover of $R(n)$ is H_d, i.e. H_e is a subgroup of H_d. We shall see in Section 2 that there is a subgroup $\tilde{H}$ of A with $\tilde{H} = \bigcap\limits_{d \geqslant 1} H_d$, which plays an important role in the sequel. $\tilde{H}$ in fact coincides with H_1, although this fact lies rather deep, and cannot be proved until Section 7.

1C. To prepare the way for Theorem IV we introduce further subgroups of H_1, as follows. Let $p \geqslant 2$ be prime, and let $R(p) \neq \emptyset$. Then, choosing any $x \in R(p)$, we have $R(p) = xB$, where $1_A \in B = B_{p,x}$. In 2^A we have an increasing chain $\emptyset \neq B \subseteq B^2 \subseteq B^3 \subseteq \ldots$ Since 2^A is finite there exists an $n_0 = n_0(x, p) \geqslant 1$ such that $W := B^{n_0} = B^{2n_0} = W^2$. In particular $W = W_{x,p}$ is a subgroup of A. It is trivial to check that this subgroup is independent of the choice of $x \in R(p)$, and coincides with $\langle tu^{-1}; t, u \in R(p) \rangle$, which we denote by W_p. It follows that $R(p)^n$ is a single coset of W_p, for all large n. If $R(p) = \emptyset$ it is convenient to define $W_p = \{1_A\}$. In [5], [6] we proved that $H = H_1 = \langle W_p; p \nmid d \rangle$, for any choice of $d \geqslant 1$, in the special cases where $\mathfrak{f}' = \mathfrak{D}_K$ and K/Q is either Galois or "generic cubic" (i.e. $K = Q(\theta)$, where θ is cubic over Q and the minimal polynomial for θ over Q is irreducible, with Galois group S_3). We shall prove later that

$$H_1 = \tilde{H} = H_d = \langle W_p; p \nmid d \rangle, \tag{1.2}$$

for arbitrary K, $\mathfrak{f}$ and d. This is a rather curious result, which cannot easily be translated into the modern language of cohomology and idèles; it appears to be connected with some kind of "nonabelian cohomology" of idèle-class groups, lying outside the scope of standard theories.

2. Frobenian properties of ranges.

2A. Corresponding to any pair K, $\mathfrak{f}$ in Section 0, there exists, by global classfield theory ([3], p. 179) a unique finite abelian extension $\tilde{R}/K$, of conductor $\mathfrak{f}$, equipped with a canonical isomorphism $\operatorname{Gal} \tilde{R}/K \to A = A(K, \mathfrak{f})$ (the Artin map), induced by sending the Artin symbol $\left(\frac{\tilde{R}/K}{\mathfrak{p}}\right)$ to the ray-class $[\mathfrak{p}]$ of $\mathfrak{p} (\bmod^{\times} \mathfrak{f})$, for all prime $\mathfrak{p} \lhd \mathfrak{D}_K$ not dividing $\mathfrak{f}'$. To study the distribution of ranges in greater depth than in Section 1 it is necessary to introduce the Galois hull F/Q of $\tilde{R}/Q$; thus F/Q is finite Galois, and minimal with respect to the inclusion $F \supseteq \tilde{R}$. We first show that, in a certain sense, ranges of norms are determined by a knowledge of the Frobenius classes of (rational) primes in $\operatorname{Gal} F/Q$. Let $p, q \geqslant 2$ be primes in Z unramified in F/Q. (This condition is equivalent to $p, q \nmid N(\mathfrak{f}'\,\partial_K)$, where ∂_K is the different of K/Q). Then the Frobenius classes $\left(\frac{F/Q}{p}\right)$ and $\left(\frac{F/Q}{q}\right)$ are well-defined conjugacy classes in $G = \operatorname{Gal} F/Q$. Assume now that they are equal. By an argument spelled out in detail in [6], the prime ideal factorisations $p\mathfrak{D}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_g$ and $q\mathfrak{D}_K = \mathfrak{q}_1 \ldots \mathfrak{q}_h$ have the following close degree of similarity. First $g = h$. Secondly the labelling of the $\mathfrak{p}_i$ and $\mathfrak{q}_i$ can be arranged in such a way that $[\mathfrak{p}_i] = [\mathfrak{q}_i]$ and $\mathfrak{p}_i$ and $\mathfrak{q}_i$ have the same residual degree (relative to K/Q), for $1 \leqslant i \leqslant g$. For such p, q it follows that $R(p^n) = R(q^n)$ for all $n \geqslant 0$. Together with (1.1) this is enough to prove that the map $n \mapsto R(n)$ is *Frobenian multiplicative*: $N_d \to 2^A$, provided that d is divisible by all primes ramified in F/Q ([7], [8]). (Incidentally, the definition of N_d allows us always to assume that d is squarefree, although this is of no real advantage.)

Now let $e(K, \mathfrak{f})$ be the product of all p ramified in F/Q. We shall assume until further notice that $d \equiv 0 (\bmod\ e(K, \mathfrak{f}))$. To exploit the Frobenian multiplicative property of $n \mapsto R(n)$ we introduce some numerical functions associated with $R(n)$. Let $\hat{A} = \operatorname{Hom}(A, C^*)$ be the character (or dual) group of A. If $n \in N_d$, $\alpha \in A$ and $\chi \in \hat{A}$, we define

$$r(n) = \# \{\mathfrak{a} \lhd \mathfrak{D}_K;\ \mathfrak{a} + \mathfrak{f}' = \mathfrak{D}_K,\ N\mathfrak{a} = n\}, \tag{2.1}$$

$$r(\alpha, n) = \# \{\mathfrak{a} \lhd \mathfrak{D}_K,\ \mathfrak{a} + \mathfrak{f}' = \mathfrak{D}_K,\ [\mathfrak{a}] = \alpha,\ N\mathfrak{a} = n\} \tag{2.2}$$

and

$$S(\chi, n) = \sum_{\substack{\mathfrak{a} + \mathfrak{f}' = \mathfrak{D}_K \\ N\mathfrak{a} = n}} \chi(\mathfrak{a}). \tag{2.3}$$

It is clear that $r(n)$ and $S(\chi, n)$ are multiplicative, while the orthogonality relations for characters yield

$$(2.4)\qquad r(\alpha, n) = (\# A)^{-1} \sum_{\chi \in \hat{A}} \bar{\chi}(\alpha) S(\chi, n).$$

From the above discussion of $R(n)$ we see that $\left(\frac{F/Q}{p}\right) = \left(\frac{F/Q}{q}\right)$ implies $r(p^n) = r(q^n)$, $r(\alpha, p^n) = r(\alpha, q^n)$ and $S(\chi, p^n) = S(\chi, q^n)$ for all $n \geqslant 0$, all $\alpha \in A$ and all $\chi \in \hat{A}$. Moreover the groups W_p and W_q (defined in §1C) coincide, while $\mathscr{R}_d = \mathscr{R}_{e(K,\mathfrak{f})}$ for all $d \equiv 0(\operatorname{mod} e(K, \mathfrak{f}))$, and so $H_d = \tilde{H}$ in §1B. The proof that $\tilde{H} = H_1$ cannot be given at this stage.

2B. The analysis in [7] and [8] yields the following asymptotic expansion. Let $(\emptyset \neq)\ L \in 2^A$, and let $d \equiv 0(\operatorname{mod} e(K, \mathfrak{f}))$. Then, as $x \to \infty$, we have

$$(2.5)\qquad \# \{n \in N_d;\ n \leqslant x,\ R(n) = L\}$$
$$\sim x \sum_{j \in J_L} P_{jLd}(\log\log x)(\log x)^{\varrho_{jL}-1} \Big\{\sum_{m=0}^{\infty} c(d, j, L, m)(\log x)^{-m}\Big\}$$
$$+ O_{d,K,\mathfrak{f}}\big(x \exp(-C^*(K, \mathfrak{f})\sqrt{\log x})\big).$$

Here J_L is a finite index set, $P_{jLd}(T) \in \boldsymbol{C}[T]$ and the ϱ_{jL} are complex numbers whose real parts do not exceed ∂, the Dirichlet density of the set of primes p in $\boldsymbol{Z}$ for which $R(p) \neq \emptyset$ (∂ only depends on K, not on $\mathfrak{f}$ or d), while $C^*(K, \mathfrak{f}) > 0$. The dependence of all quantities occurring in (2.5) on the various parameters is made explicit by the notation.

The general nature of the discussion in [7] and [8] makes it difficult to determine the precise values of the various exponents, degrees and coefficients in (2.5), and we shall have to introduce some alternative methods which at least determine the net dominant term in (2.5) with sufficient precision. We shall eventually show that the net dominant term in (2.5) has the form $b(d, L)\, x (\log x)^{\partial - 1}$ with $b(d, L) > 0$, precisely when L is a d-maximal range, and that (2.5) is definitely of smaller order of magnitude otherwise. (Essentially this is one of the main assertions of Theorem II – see §3.) Whereas (2.5) is vague for particular L, it is possible to derive directly from [7], [8] and [10] a more informative result about the sum of $\# \{n \in N_d;\ n \leqslant x,\ R(n) = L\}$ over all $L \neq \emptyset$, that is, about $\# \{n \in N_d;\ n \leqslant x,\ R(n) \neq \emptyset\}$. Writing $\delta(n) = 1$ or 0, according as or not $n \in N_d$ and $R(n) \neq \emptyset$, we find that δ is Frobenian multiplicative: $N_d \to \{0, 1$ (multiplication)$\}$. A simple inspection of the appropriate generating functions in [8], relevant to δ, yields

$$(2.6)\qquad \# \{n \in N_d;\ n \leqslant x,\ R(n) \neq \emptyset\} \sim x (\log x)^{\partial - 1} \Big\{b_{d0} + \sum_{m=1}^{\infty} b_{dm} (\log x)^{-m}\Big\},$$

with $b_{d0} > 0$. If the various Dirichlet series in [8] are adjusted by allowing prime factors of $e(K, \mathfrak{f})$ to enter, it is easily seen that an analogue of (2.6) is still valid without the restriction $d \equiv 0(\operatorname{mod} e(K, \mathfrak{f}))$. We shall make frequent use of (2.6) later.

2C. We conclude Section 2 with a simple device from classical analysis which saves much tedious complication in deriving asymptotic expansions. Suppose that $f\colon N_1 \to \boldsymbol{C}$ is bounded, and that we have an asymptotic expansion of the type

$$(2.7)\qquad \sum_{1 \leqslant n \leqslant x} f(n) \log \frac{x}{n} \sim (2.5)' \qquad (x \to \infty)$$

where (2.5)′ denotes an expansion of the same general type as (2.5). Then a simple Tauberian argument [10] based on summation-by-parts, yields

$$(2.8)\qquad \sum_{1 \leqslant n \leqslant x} f(n) \sim (2.5)'',$$

where (2.5)″ is again of the same type as (2.5), and has the same net dominant term as (2.5)′. Conversely, an "Abelian" argument (again based on summation-by-parts) leads easily from (2.8) to (2.7).

The relevance of this discussion is that, if $f(n)$ is, for example, the characteristic function of some suitable subset of N_1, it is often possible to derive (2.7) by a straightforward application of the Mellin transformation and Perron's summation formula to the Dirichlet series $\sum_{n \geqslant 1} f(n) n^{-s}$ (and its meromorphic continuation, if it has one), whereas (2.8) cannot be obtained in this way. In such cases the equivalence of (2.7) and (2.8) is important in deriving the asymptotics of $\sum_{1 \leqslant n \leqslant x} f(n)$. We shall use this process several times, referring to it simply as "weight-stripping".

3. Formulation of the main theorems. Having now given all the relevant background material and definitions we are in a position to state our main theorems. They will, in part, consist of assertions that various sets have assymptotically equal cardinalities. We define

$$\mathscr{U}_d(x, \alpha) = \{n \in N_d;\ n \leqslant x,\ R(n) = \alpha H_d\}, \qquad U_d(x, \alpha) = \#\, \mathscr{U}_d(x, \alpha);$$
$$(3.1)\quad \mathscr{U}_d^{+}(x, \alpha) = \{n \in N_d;\ n \leqslant x,\ \alpha \in R(n)\}, . \qquad U_d^{+}(x, \alpha) = \#\, \mathscr{U}_d^{+}(x, \alpha);$$
$$\mathscr{U}_d^{++}(x, \alpha) = \{n \in N_\alpha;\ n \leqslant x,\ \emptyset \neq R(n) \subseteq \alpha H_d\},$$
$$U_d^{++}(x, \alpha) = \#\, \mathscr{U}_d^{++}(x, \alpha).$$

Here $d \geqslant 1$ is arbitrary, $\alpha \in A$ is also arbitrary and x is large positive. It is clear from Section 1 that $\mathscr{U}_d(x, \alpha) \subseteq \mathscr{U}_d^{+}(x, \alpha) \subseteq \mathscr{U}_d^{++}(x, \alpha)$, so that

$U_d(x, \alpha) \leqslant U_d^+(x, \alpha) \leqslant U_d^{++}(x, \alpha)$ for all x, d, α. In view of (2.5) it is clear that all three quantities U, U^+, U^{++} have expansions of the type (2.5)″, obtained from (2.5) by elementary manipulations. The following results will be proved.

THEOREM I. *For any $d \geqslant 1$, $\alpha_1, \alpha_2 \in A$, we have*

$$U_d^{++}(x, \alpha_1) \approx U_d^{++}(x, \alpha_2)$$

(i.e. the ratio of these quantities tends to 1 as $x \to \infty$).

THEOREM II. *For each $1 \leqslant d \equiv 0(\operatorname{mod} e(K, f))$ we have $H_d = \tilde{H}$ and, for all $\alpha \in A$,*

$$U_d(x, \alpha) \approx U_d^+(x, \alpha) \approx U_d^{++}(x, \alpha).$$

THEOREM III. *$\tilde{H} = H_d = H_1$ for all $d \geqslant 1$.*

THEOREM IV. *We have $H_1 = \langle W_p;\, p \nmid d \rangle$ for any $d \geqslant 1$.*

Before outlining the proofs of these theorems we first derive an interesting heuristic reinterpretation of Theorems I and II. Let $\alpha_1, \ldots, \alpha_k$ be any transversal for the cosets of $\tilde{H}$ in A, so that $k = (A : \tilde{H})$. Then $\{n \in N_d;\, n \leqslant x,\, R(n) \neq \emptyset\}$ is the disjoint union of the $\mathscr{U}_d^{++}(x, \alpha_j)$, $j = 1, \ldots, k$. (Here we are assuming that $d \equiv 0(\operatorname{mod} e(K, \mathfrak{f}))$.) By Theorem I the latter sets have asymptotically equal cardinalities. Applying (2.6) we deduce that $U_d^{++}(x, \alpha)$ has net dominant term $(A : \tilde{H})^{-1} b_{d0}\, x(\log x)^{\partial - 1}$ for all $\alpha \in A$. By Theorem II this is also the net dominant term in the expansions for $U_d(x, \alpha)$ and $U_d^+(x, \alpha)$. Moreover, if $(\emptyset \neq)$ L is a non-maximal range in $\mathscr{R}_d$, then $\emptyset \neq L \subsetneqq \alpha H_d = \alpha \tilde{H}$, for some $\alpha \in L$, so that

$$\# \{n \in N_d;\, n \leqslant x,\, R(n) = L\} \leqslant U_d^{++}(x, \alpha) - U_d(x, \alpha). \tag{3.2}$$

Applying Theorems I and II again, we see that the right-hand side of (3.2) is negligible in comparison with $x(\log x)^{\partial - 1}$ and hence so is the left-hand side. We therefore have a simple, informal reinterpretation of Theorem II – "almost all norms in N_d have a d-maximal range".

In Section 7 we shall remove the hypothesis that $d \equiv 0(\operatorname{mod} e(K, \mathfrak{f}))$; it is not convenient to prove the stronger form directly, since it requires a further idea of a quite different kind from those used in the proofs of Theorems I and II.

Theorem I will be proved in Section 5; it is the least demanding of the main theorems, and the proof does not require any very intricate arguments. Theorems II–IV lie much deeper, and only emerge after a rather delicate chain of arguments involving tensor products of induced representations of $\operatorname{Gal} F/Q$. Theorem II is proved in Section 6, Theorem III (and the stronger form of Theorem II) in Section 7, and Theorem IV in Section 8. An interesting by-product of our proof of Theorem II is another characterisation of $\tilde{H}$ in terms of a certain induction process applied to characters of A, described in precise terms in Section 6. This characterisation is important in Section 7, and is also the basis of our general definition of central classfield given in Section 9.

The proof of Theorem IV is rather curious, and is based on the construction of an unusual kind of Dirichlet series.

Before we embark on the proofs of our main theorems we shall need some (mostly) elementary results on group characters; we prove these in the next section, to avoid complicated digressions in Sections 5–8.

4. Lemmas on group characters. Let $A = A(K, \mathfrak{f})$, $\tilde{R}$ and F be as in Sections 0–2. We identify A with $\operatorname{Gal} \tilde{R}/K$ via the Artin map. Let $G = \operatorname{Gal} F/Q$ and $\Gamma = \operatorname{Gal} F/K$. If $\chi \in \dot{A}$ then χ lifts to a (degree-one) character χ_* of Γ. Since Γ is a subgroup of G we may therefore construct from χ_* an induced character χ_*^G of G, of degree $(G : \Gamma) = [K : Q]$. The properties of these χ_*^G are very important in the sequel.

LEMMA 4.1. *Let $2 \leqslant p \in \mathbf{Z}$ be prime, $p \nmid e(K, \mathfrak{f})$, and let $\chi \in \hat{A}$, $g \in \left(\frac{F/Q}{p}\right)$. Then $\chi_*^G(g) = \sum \chi(p)$, where the sum is taken over all $\mathfrak{p} \lhd \mathfrak{O}_K$ with $\mathfrak{p} + \mathfrak{f}' = \mathfrak{O}_K$ and $N\mathfrak{p} = p$.*

This is a well-known result, and corresponds to part of the proof of the induction formula for Artin L-functions ([4], pp. 233–239).

We recall that the inner product of two C-valued class functions θ, φ on G is defined to be

$$\langle \theta, \varphi \rangle_G := (\#G)^{-1} \sum_{g \in G} \overline{\theta(g)}\, \varphi(g).$$

LEMMA 4.2. *Let $T = \{\chi \in \hat{A};\, \langle \chi_*^G, \chi_*^G \rangle_G = \langle 1_*^G, 1_*^G \rangle_G\}$, where $1 \in \hat{A}$ is the identity character. Then T is a subgroup of $\hat{A}$.*

Proof. We have $\chi_*^G(g) = (\#\Gamma)^{-1} \sum_{x \in G} \dot{\chi}_*(xgx^{-1})$ for all $g \in G$, $\chi \in \hat{A}$, where

$$\dot{\chi}_*(u) = \begin{cases} \chi_*(u) & \text{if } u \in \Gamma, \\ 0 & \text{if not.} \end{cases}$$

Then, since $|\dot{\chi}_*(xgx^{-1})| = |\dot{1}_*(xgx^{-1})| = \dot{1}_*(xgx^{-1})$ for all $\chi \in \hat{A}$, $g, x \in G$, we have $|\chi_*^G(g)|^2 \leqslant |1_*^G(g)|^2$ for all $g \in G$, $\chi \in \hat{A}$, with equality for all g if and only if $\dot{\chi}_*(xgx^{-1}) = \lambda(g)\, \dot{1}_*(xgx^{-1})$ for all $x \in G$, where $|\lambda(g)| = 1$ for all $g \in G$. Hence $\chi \in T$ if and only if $\dot{\chi}_*(xgx^{-1}) = \lambda(g)\, \dot{1}_*(xgx^{-1})$ for all x, g in G. In particular the latter requires that $\chi_*(\gamma) = \lambda(\gamma)$ for all $\gamma \in \Gamma$, and it is now clear that $\chi \in T$ if and only if

$$(4.1) \qquad \chi_*(g) = \chi_*(xgx^{-1}) \quad \text{for all } g \in \Gamma \cap x^{-1}\Gamma x \quad (x \in G).$$

It is obvious that if $\chi, \psi \in \hat{A}$ both satisfy (4.1) then so also do $\bar{\chi}$ and $\bar{\chi}\psi$, so that T is, indeed, a subgroup of $\hat{A}$.

If B is a subgroup of A we define

$$(4.2a) \qquad B^{\perp} = \{\chi \in \hat{A};\, \chi(\beta) = 1,\ \forall \beta \in B\} = \{\chi \in \hat{A};\, B \subseteq \ker \chi\},$$

while, if D is a subgroup of $\hat{A}$, we write

$$(4.2b) \qquad D^{\perp} = \{\alpha \in A;\, \chi(\alpha) = 1,\ \forall \chi \in D\} = \bigcap_{\chi \in D} \ker \chi.$$

Then, by "Pontryagin duality", we have $B^{\perp\perp} = B$, $D^{\perp\perp} = D$.

Lemma 4.3. *Let B be a subgroup of A, and let $r(\alpha, n)$ be as in* (2.2). *Then*

$$(4.3) \qquad \sum_{\alpha \in A} \sum_{\beta \in B} (r(\alpha\beta, n) - r(\alpha, n))^2 = 2(A:B)^{-1} \sum_{\chi \notin B^{\perp}} |S(\chi, n)|^2,$$

with $S(\chi, n)$ as in (2.3).

Proof. We start from (2.4). This gives

$$(4.4) \qquad r(\alpha\beta, n) - r(\alpha, n) = (\#A)^{-1} \sum_{\chi \in \hat{A}} \bar{\chi}(\alpha)(\bar{\chi}(\beta) - 1) S(\chi, n).$$

The left-hand side of (4.4) is real. Taking $|\cdot|^2$ in (4.4), we have

$$(r(\alpha\beta, n) - r(\alpha, n))^2$$
$$= (\#A)^{-2} \sum_{\chi, \psi \in \hat{A}}\sum \bar{\chi}(\alpha)\psi(\alpha)(\bar{\chi}(\beta) - 1)(\psi(\beta) - 1) S(\chi, n) S(\bar{\chi}, n).$$

Summing over all $\alpha \in A$, and using orthogonality relations, we deduce that

$$\sum_{\alpha \in A} (r(\alpha\beta, n) - r(\alpha, n))^2 = (\#A)^{-1} \sum_{\chi \in \hat{A}} |S(\chi, n)|^2 (2 - \chi(\beta) - \bar{\chi}(\beta)).$$

Finally, summing over all $\beta \in B$, and noting that

$$\sum_{\beta \in B} (2 - \chi(\beta) - \bar{\chi}(\beta)) = 0 \quad \text{or} \quad 2\#B,$$

according as or not χ is trivial on B, the lemma is proved.

The relevance of Lemma 4.3 will be seen in Section 6. We shall show there that if B is the image under the Artin map of $\tilde{H}$ of Section 2 then $B^{\perp}$ is precisely T of Lemma 4.2.

For the next two lemmas we denote by $[a_1, \dots, a_s]$ the (positive) highest common factor of $a_1, \dots, a_s \in \mathbf{Z}$ (not all zero).

Lemma 4.4. *Let $k \geqslant 1$ and let $f_1, \dots, f_{k+1} \in \mathbf{Z}$, with $f_i > 0$. Let $[f_1, \dots, f_{k+1}] = d$, $f_i = d\dot{f}_i$ $(1 \leqslant i \leqslant k+1)$, and let $e = [\dot{f}_1, \dots, \dot{f}_k]$. Suppose that $b_1, \dots, b_k \in \mathbf{Z}$ satisfy $\sum_{i \leqslant k} b_i \dot{f}_i = e$. Then the solutions $\mathbf{n} \in \mathbf{Z}^{k+1}$ of $\sum_{i \leqslant k+1} n_i f_i = 0$ are precisely the vectors of the type*

$$\mathbf{n} = y(-b_1 \dot{f}_{k+1}, \dots, -b_k \dot{f}_{k+1}, e) + \mathbf{n}^*$$

with $y \in \mathbf{Z}$ and $\mathbf{n}^*$ a solution with $n^*_{k+1} = 0$.

Proof. This result could be derived from the theory of elementary divisors, but this is hardly necessary, in view of the following elementary argument. Let $n_{k+1} \in \mathbf{Z}$ be fixed. In order that there should exist $n_1, \dots, n_k \in \mathbf{Z}$ such that $\sum_{i \leqslant k+1} n_i \dot{f}_i = 0$, it is necessary and sufficient that $n_{k+1} \equiv 0 \pmod e$. Writing $n_{k+1} = ye$ $(y \in \mathbf{Z})$, one solution is $\mathbf{n} = y(-b_1 \dot{f}_{k+1}, \dots, -b_k \dot{f}_{k+1}, e)$, while the difference of two solutions $\mathbf{n}, \mathbf{n}'$ of $\sum_{i \leqslant k+1} n_i f_i = 0 = \sum_{i \leqslant k+1} n'_i f_i$ with $n_{k+1} = n'_{k+1} = ye$ is a solution of the type $\mathbf{n}^*$. Conversely, to any solution $\mathbf{n}$ we may add any solution of the type $\mathbf{n}^*$ without changing the last coordinate of $\mathbf{n}$.

Lemma 4.5. *Let G, Γ, T be as above, and let $g \in G$ be fixed. Suppose that X is any subset of G. For each $x \in X$ let $f(x)$ be the smallest positive integer such that $(xgx^{-1})^{f(x)} \in \Gamma$. Then if $n(x)$ $(x \in X)$ are integers such that $\sum_{x \in X} n(x) f(x) = 0$, we have*

$$\prod_{x \in X} \chi_*((xgx^{-1})^{f(x)n(x)}) = 1 \quad \textit{for all } \chi \in T.$$

Proof. The result is obvious if $\#X = 0$ or 1. We first give a proof for the case $\#X = 2$, and then set up an induction which proves the lemma when $\#X > 2$. Suppose first that $X = \{x, y\}$, where $x \neq y$. If $[f(x), f(y)] = d$ and $f(x) = d\dot{f}(x)$, $f(y) = d\dot{f}(y)$, we have $n(x)f(x) + n(y)f(y) = 0$ if and only if $n(x) = k\dot{f}(y)$ and $n(y) = -k\dot{f}(x)$ for some $k \in \mathbf{Z}$ (a special case of Lemma 4.4). Then $\lambda := (xgx^{-1})^{n(x)f(x)} = (xgx^{-1})^{kf(x)\dot{f}(y)}$ and $\mu := (ygy^{-1})^{-n(y)f(y)} = (ygy^{-1})^{k\dot{f}(x)f(y)}$ are two elements of Γ which are G-conjugate. The proof of Lemma 4.2 shows that $\chi_*(\lambda) = \chi_*(\mu)$ for all $\chi \in T$, and so we have proved the lemma when $\#X = 2$. Now let $k \geqslant 2$ and suppose the lemma proved when $\#X \leqslant k$. Let $\#X = k+1$; we denote the elements of X by $x_1, \dots, x_{k+1}$, the quantities $f(x_i)$ by f_i and the $n(x_i)$ by n_i $(1 \leqslant i \leqslant k+1)$. We assume that $\sum_{i \leqslant k+1} n_i f_i = 0$. If $n_{k+1} = 0$ the problem at hand reduces to that of the case of the set $X \setminus \{x_{k+1}\}$, for which the lemma is already proved. By Lemma 4.4 we need only prove the lemma when $\mathbf{n}$ is the special vector $(-b_1 \dot{f}_{k+1}, \dots, -b_k \dot{f}_{k+1}, e)$. Let $\gamma_i = (x_i g x_i^{-1})^{f_i} \in \Gamma$. Then $\gamma_{k+1}^{e} = \gamma_{k+1}^{(b_1 \dot{f}_1 + \dots + b_k \dot{f}_k)}$. But $\gamma_{k+1}^{b_i \dot{f}_i}$ is G-conjugate to $\gamma_i^{b_i \dot{f}_{k+1}}$, so that

$$\chi_*(\gamma_{k+1}^{b_i \dot{f}_i}) = \chi_*(\gamma_i^{b_i \dot{f}_{k+1}}) \quad \text{for all } \chi \in T \text{ and all } 1 \leqslant i \leqslant k.$$

On multiplying these relations together for $1 \leqslant i \leqslant k$, we obtain the lemma.

This rather curious result turns out to be important in Sections 6–8.

5. Proof of Theorem I. We recall the definition (3.1) of the set $\mathscr{W}_d^{++}(x, \alpha)$. Let $d \geqslant 1$ and $\chi \in \hat{A}$. If χ is trivial on H_d (i.e. $\chi \in H_d^{\perp}$) then, for any $n \in N_d$, χ takes the same value at all members of $R(n)$ (if $R(n) \neq \emptyset$), in other words we may write this value unambiguously as $\chi(R(n) H_d)$, since $R(n)$ is contained in a single coset of H_d. For $\chi \in H_d^{\perp}$ we write $\chi(\emptyset H_d) = 0$. Then we have

$$(5.1) \qquad (A : H_d)^{-1} \sum_{\chi \in H_d^{\perp}} \bar{\chi}(\alpha H_d) \chi(R(n) H_d) = 1 \text{ or } 0,$$

according as or not $R(n) H_d = \alpha H_d$, for any choice of $\alpha \in A$.

We now consider

$$(5.2) \qquad Y^{++} = Y_d^{++}(x, \alpha) = \sum_{n \in \mathscr{W}_d^{++}(x, \alpha)} \log(x/n).$$

Using (5.1), we have

$$(5.3) \qquad Y^{++} = (A : H_d)^{-1} \sum_{\chi \in H_d^{\perp}} \bar{\chi}(\alpha H_d) \Big\{ \sum_{\substack{n \leqslant x \\ n \in N_d}} \chi(R(n) H_d) \log(x/n) \Big\}.$$

We shall prove that the trivial character alone gives rise to the dominant term in the asymptotic expansion of (5.3). We introduce the Dirichlet series

$$(5.4) \qquad \mathscr{L}_d(s, \chi) = \sum_{n \in N_d} \chi(R(n) H_d) n^{-s},$$

which is clearly absolutely convergent for $\sigma = \operatorname{Re} s > 1$, where it is an analytic function of s. When $\sigma > 1$, $\mathscr{L}_d(s, \chi)$ has an Euler product $\prod_{p \nmid d} \lambda_p(s, \chi)$, where $\lambda_p(s, \chi) = 1 + \sum_{k \geqslant 1} p^{-ks} \chi(R(p^k) H_d)$ for p prime. Hence, after adjusting a finite number of Euler factors, we can write $\mathscr{L}_d(s, \chi) = \mathscr{L}_e(s, \chi) \cdot \mathscr{M}_d(s, \chi)$, where $e = e(K, \mathfrak{f})$ of Section 2 and $\mathscr{M}_d(s, \chi)$ is analytic and uniformly bounded in any closed half-plane $\sigma \geqslant \delta$ $(\delta > 0)$, while $\mathscr{M}_d(1, \chi) \neq 0$.

We proceed to obtain a continuation of $\mathscr{L}_e(s, \chi)$ into a region extending some way to the left of $\sigma = 1$, cut along the real axis leftwards from $s = 1$; this will be achieved by using the Frobenian properties derived in Section 2. Let $\mathscr{C}$ be the set of all Frobenius classes $\left(\dfrac{F/Q}{p}\right)$ (p unramified) for which $R(p) \neq \emptyset$. If p has Frobenius class C we write $p \leftrightarrow C$. Then, by Section 2, the values of $\chi(R(p^k) H_d)$ $(k \geqslant 0)$ are determined by the choice of C; for $p \leftrightarrow C$ we write

$$a_k(\chi, C) = \chi(R(p^k) H_d) \qquad (k \geqslant 1).$$

Clearly we have

$$(5.5) \qquad \mathscr{L}_e(s, \chi) = \Big\{ \prod_{C \in \mathscr{C}} \mathscr{L}^*(s, \chi, C) \Big\} \cdot \mathscr{M}^*(s, \chi)$$

for $\sigma > 1$, where

$$(5.6) \qquad \mathscr{L}^*(s, \chi, C) = \prod_{p \leftrightarrow C} \Big\{ 1 + \sum_{k \geqslant 1} p^{-ks} a_k(\chi, C) \Big\},$$

while $\mathscr{M}^*(s, \chi)$ involves only the $p \nmid e$ for which $R(p) = \emptyset$, and thus is analytic, non-zero and uniformly bounded for $\sigma \geqslant 3/4$ (say).

Now we also have

$$(5.7) \qquad \mathscr{L}^*(s, \chi, C) = \mathscr{L}^{**}(s, \chi, C) \cdot \mathscr{M}^{**}(s, \chi, C),$$

where

$$(5.8) \qquad \mathscr{L}^{**}(s, \chi, C) = \prod_{p \leftrightarrow C} \exp\big(a_1(\chi, C) p^{-s}\big)$$

for $\sigma > 1$, and $\mathscr{M}^{**}(s, \chi, C)$ is analytic, non-zero and uniformly bounded for $\sigma \geqslant 3/4$. Taking logarithms (principal branch) in (5.8), and summing over all $C \in \mathscr{C}$, we have

$$(5.9) \qquad \sum_{C \in \mathscr{C}} \log \mathscr{L}^{**}(s, \chi, C) = \sum_{C \in \mathscr{C}} a_1(\chi, C) \Big\{ \sum_{p \leftrightarrow C} p^{-s} \Big\}$$

when $\sigma > 1$. We can now apply the Chebotarev density theorem ([8], [10]) to determine the singularity of (5.9) at $s = 1$, and to prove the existence of a continuation some way to the left of $s = 1$. We find that

$$(5.10) \qquad \sum_{C \in \mathscr{C}} \log \mathscr{L}^{**}(s, \chi, C) = \Big\{ \sum_{C \in \mathscr{C}} a_1(\chi, C) \frac{\# C}{\# G} \Big\} \log \frac{1}{s-1} + P(s, \chi),$$

where $P(s, \chi)$ is analytic in a region of the type

$$(5.11) \qquad s = \sigma + it, \quad \sigma \geqslant 1 - \frac{k(F)}{\log(t^2 + 20)},$$

where $k(F) > 0$, and satisfies $|P(s, \chi)| = O_F(\log\log(20 + t^2))$ there.

Now the quantities $a_1(\chi, C)$ are just the $\chi(R(p) H_d)$ for $p \leftrightarrow C$, and have absolute value 1 when $C \in \mathscr{C}$. It follows that

$$(5.12) \qquad \operatorname{Re} \sum_{C \in \mathscr{C}} a_1(\chi, C) \frac{\# C}{\# G} \leqslant \sum_{C \in \mathscr{C}} \frac{\# C}{\# G} = \partial,$$

(with ∂ as in §2B), with equality if and only if $a_1(\chi, C) = 1$ for all $C \in \mathscr{C}$. The latter occurs if and only if $\chi(R(p) H_d) = 1$ for all $p \nmid e = e(K, \mathfrak{f})$ with $R(p) \neq \emptyset$. Now the sum $\sum N\mathfrak{p}^{-1}$, taken over all prime $\mathfrak{p} \lhd \mathfrak{O}_K$ with $[\mathfrak{p}] = \alpha$, is divergent, for any choice of $\alpha \in A$, a classical result of E. Hecke ([3], p. 182). Hence, for all $\alpha \in A$, we can find a prime $p \nmid e(K, \mathfrak{f})$ with $\alpha \in R(p)$. It follows that equality holds in (5.12) if and only if $\chi = 1 \in \hat{A}$.

It is now clear that the series $\mathscr{L}_e(s, 1)$ has a singularity of the type $(s-1)^{-\partial} F(s, 1)$, where $F(s, 1)$ is analytic near $s = 1$, with $F(1, 1) > 0$, while, if $\chi \neq 1$, $\mathscr{L}_e(s, \chi)$ is of the form $(s-1)^{-b(\chi)} F(s, \chi)$, with $F(s, \chi)$ analytic near $s = 1$ and $\operatorname{Re} b(\chi) < \partial$.

A simple application of Perron's summation formula [10] gives

$$(5.13)\qquad \sum_{\substack{n \in N_d \\ n \leqslant x}} \chi\big(R(n) H_d\big) \log(x/n) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{s^2} \mathscr{L}_d(s, \chi)\, ds.$$

The singularity structure and meromorphic continuation of $\mathscr{L}'_d(s, \chi)$ determined above, together with the growth estimate for $P(s, \chi)$ given after (5.11), enable us to move the contour of integration in (5.13) to the left (but avoiding the cut along the real axis leftwards from $s = 1$). Applying the methods of [7], [8], [10] we obtain easily the estimate

$$(5.14)\qquad \sum_{\substack{n \in N_d \\ n \leqslant x}} \chi\big(R(n) H_d\big) \log(x/n) = o\big(x (\log x)^{\partial - 1}\big)$$

for $\chi \neq 1$, while, when $\chi = 1$, we recover (2.6) in its equivalent weighted form (2.7). In view of (5.14), (2.6) and (5.3) we thus see that

$$(5.15)\qquad Y^{++} \approx (A : H_d)^{-1} \sum_{\substack{n \in N_d \\ n \leqslant x \\ R(n) \neq \emptyset}} \log(x/n).$$

Stripping weights in (5.15), we find that

$$(5.16)\qquad U_d^{++}(x, \alpha) \approx (A : H_d)^{-1}\, \#\{n \leqslant x;\ n \in N_d,\ R(n) \neq \emptyset\}.$$

The right-hand side here is independent of the choice of $\alpha \in A$, and so Theorem I is proved.

6. Proof of Theorem II. We shall make full use here of the lemmas on characters given in Section 4, taking the subgroup B of A in Lemma 4.3 to be $T^{\perp}$, with T as in Lemma 4.2. Thus $B^{\perp} = T$, by duality. At this stage the result $T^{\perp} = B = \tilde{H} = H_d$ $(d \equiv 0(\operatorname{mod}(e(K, \mathfrak{f}))))$ is not relevant, but will emerge as a by-product of our analysis.

Let $\mathscr{M}(d) = N_d \cap \{n;\ R(n) \neq \emptyset\}$. We shall obtain the asymptotic formula

$$(6.1)\qquad \sum_{\substack{n \leqslant x \\ n \in \mathscr{M}(d)}} \big(\log(x/n)\big) r(n)^{-2} V(n) \approx q(d)\, x (\log x)^{\partial' - 1}$$

later in this section. Here we assume $d \equiv 0(\operatorname{mod}(e(K, \mathfrak{f})))$, while $q(d) > 0$ and $\partial' < \partial$ (and is independent of d), while

$$(6.2)\qquad V(n) = \sum_{\alpha \in A} \sum_{\beta \in B} \big(r(\alpha\beta, n) - r(\alpha, n)\big)^2,$$

all other notation being the same as in Sections 0–4. The weights $\log(x/n)$ are effectively irrelevant here, since $r(n)^{-2} V(n)$ is bounded on $\mathscr{M}(d)$, so that weight-stripping (§ 2C) is legitimate. Hence we can deduce from (6.1) and (2.6) that

$$(6.3)\qquad \sum_{\substack{n \leqslant x \\ n \in \mathscr{M}(d)}} r(n)^{-2} V(n) = O_d\big((\log x)^{-2\gamma}\, \#(\mathscr{M}(d) \cap [1, x])\big),$$

where $\gamma > 0$ depends only on K and $\mathfrak{f}$.

6A. Let us assume for the moment that (6.3) has already been proved, and deduce Theorem II (and the result $\tilde{H} = H_d = B = T^{\perp}$) from it. Let

$$\mathscr{M}(x, d) = \mathscr{M}(d) \cap [1, x],\quad M(x, d) = \#\, \mathscr{M}(x, d),$$

$$\mathscr{E}(x, d) = \{n \in \mathscr{M}(x, d);\ V(n) \geqslant (\log x)^{-\gamma} r(n)^2\} \text{ and } E(x, d) = \#\, \mathscr{E}(x, d).$$

Then, by (6.3), we have

$$(6.4)\qquad E(x, d)(\log x)^{-\gamma} \leqslant \sum_{n \in \mathscr{M}(x,d)} r(n)^{-2} V(n) = O_d\big(M(x, d)(\log x)^{-2\gamma}\big),$$

so that $E(x, d) = O_d\big(M(x, d)(\log x)^{-\gamma}\big)$. Thus, as $x \to \infty$, only a negligible fraction of $\mathscr{M}(x, d)$ is in $\mathscr{E}(x, d)$, and "almost all" $n \in \mathscr{M}(x, d)$ satisfy $V(n) < (\log x)^{-\gamma} r(n)^2$.

We now choose $\varepsilon > 0$, subject only to the restriction that $\varepsilon \cdot 2\, \# A < 1$. Corresponding to ε we can find $x_0(\varepsilon)$ such that $E(x, d) < \varepsilon M(x, d)$ and $\#\{n \in \mathscr{M}(x, d);\ r(n)^{-2} V(n) < \varepsilon^2\} > (1-\varepsilon) M(x, d)$ for all $x > x_0(\varepsilon)$. We then take $x > x_0(\varepsilon)$, $n \in \mathscr{M}(x, d) \setminus \mathscr{E}(x, d)$, and assume that $n \in \mathscr{M}(x, d)$ is "typical", in that $r(n)^{-2} V(n) < \varepsilon^2$. Then $r(n) > 0$, and so, for some $\alpha_0 \in A$, we have $r(\alpha_0, n) = \max\{r(\alpha, n);\ \alpha \in A\} \geqslant (\# A)^{-1} r(n)$. Since $V(n) < \varepsilon^2 r(n)^2$ we see that $|r(\alpha\beta, n) - r(\alpha, n)| < \varepsilon r(n) \leqslant \varepsilon(\# A) r(\alpha_0, N)$ for all $\alpha \in A$, $\beta \in B = T^{\perp}$. But $2\varepsilon(\# A) < 1$ and $r(\alpha_0, n) \geqslant 1$, so that $r(\alpha_0 \beta, n) \geqslant 1$ for all $\beta \in B$. This implies that $\alpha_0 B \subseteq R(n)$, while $R(n) \subseteq \alpha_0 H_d$, so that $B \subseteq H_d$.

6B. We now show, conversely, that $H_d \subseteq B$ or, equivalently, that $T = B^{\perp} \subseteq H_d^{\perp}$. To do this we must show that $\chi(\mathfrak{a}) = 1$ for all fractional ideals $\mathfrak{a}$ prime to $d\mathfrak{f}'$ and of norm 1, whenever $\chi \in T$. Since the group $L^{d\mathfrak{f}'}$ of such $\mathfrak{a}$ is the (internal) direct product of the subgroups L_p (p prime), consisting of fractional ideals of norm 1 composed only of prime ideals dividing p and not $d\mathfrak{f}'$, we need only show that $\chi(L_p) = 1$ for all p and all $\chi \in T$. We have assumed that $d \equiv 0(\operatorname{mod}(e(K, \mathfrak{f})))$, so that the p with $L_p \neq \{1\}$ are unramified in $F/\boldsymbol{Q}$. Let p be such a prime, and let $g \in \left(\frac{F/\boldsymbol{Q}}{p}\right)$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are the distinct prime ideal factors of p in $\mathfrak{O}_K$, with respective residual degrees $f_1, \ldots, f_k$ (relative to $K/\boldsymbol{Q}$), we can find $x_1, \ldots, x_k \in G = \operatorname{Gal} F/\boldsymbol{Q}$ such that f_i is the smallest positive integer such that $(x_i g x_i^{-1})^{f_i} \in \Gamma = \operatorname{Gal} F/K$, and then $\chi(\mathfrak{p}_i) = \chi_*\big((x_i g x_i^{-1})^{f_i}\big)$ for $1 \leqslant i \leqslant k$ and every $\chi \in \hat{A}$. This is a consequence of Sections 2 and 4, and the relations connecting Frobenius elements of primes in F relative to the Galois extensions F/Q and F/K. In order that $\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k} \in L_p$ it is necessary and sufficient that $\sum_{1 \leqslant i \leqslant k} n_i f_i = 0$. But then, in view of Lemma 4.5, we have

$$\chi(\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k}) = \prod_{1 \leqslant i \leqslant k} \chi_*((x_i g x_i^{-1})^{n_i f_i}) = 1 \qquad \text{for all } \chi \in T.$$

We have thus proved that $B = H_d$.

Having established that $B = H_d$ we can now see that the arguments of §6A give more information than it would seem at first sight. Indeed, most of $\mathscr{M}(x, d)$ is not in $\mathscr{E}(x, d)$, and, in fact, most $n \in \mathscr{M}(x, d)$ have a coset of H_d contained in $R(n)$. Thus we see that "almost all $n \in \mathscr{M}(x, d)$ have a d-maximal range".

6C. Still assuming that (6.3) has been proved, we are now in a position to deduce Theorem II from Theorem I. The latter shows that

$$U_d^{++}(x, \alpha) \approx (A : H_d)^{-1} M(x, d).$$

Let $\alpha_1, \dots, \alpha_k$ be a transversal for the cosets of H_d in A. Then $\mathscr{M}(x, d)$ is the disjoint union of the $\mathscr{U}_d^{++}(x, \alpha_j)$, $1 \leqslant j \leqslant k$. But the arguments of §6A and §6B show that $\sum_{1 \leqslant j \leqslant k} U_d(x, \alpha_j) \approx M(x, d)$, the $\mathscr{U}_d(x, \alpha_j)$ being pairwise disjoint. Since $U_d(x, \alpha_j) \leqslant U_d^{++}(x, \alpha_j)$ for all j we deduce that

$$U_d(x, \alpha) \approx U_d^{++}(x, \alpha) \qquad \text{for all } \alpha \in A.$$

Finally, as $U_d(x, \alpha) \leqslant U_d^{+}(x, \alpha) \leqslant U_d^{++}(x, \alpha)$, all three quantities are asymptotically equal, provided that $d \equiv 0 (\operatorname{mod} e(K, \mathfrak{f}))$.

6D. It now remains to prove (6.1). We shall in fact obtain a rather more precise version. Let $\lambda(n) = 0$ if $r(n) = 0$, $\lambda(n) = r(n)^{-2}$ otherwise; then $\lambda(n)$ is multiplicative, by Section 2. The left-hand side of (6.1) can be rewritten as

$$(6.5) \qquad \sum_{\substack{n \in N_d \\ n \leqslant x}} (\log(x/n)) \lambda(n) 2(A:B)^{-1} \sum_{\chi \notin B^{\perp}} |S(\chi, n)|^2$$

$$= 2(A:B)^{-1} \sum_{\chi \notin B^{\perp}} \sum_{\substack{n \in N_d \\ n \leqslant x}} (\log(x/n)) \lambda(n) |S(\chi, n)|^2,$$

by Lemma 4.3. It therefore suffices to obtain appropriate asymptotic expansions for the various

$$(6.6) \qquad W_\chi := \sum_{\substack{n \in N_d \\ n \leqslant x}} (\log(x/n)) \lambda(n) |S(\chi, n)|^2.$$

We introduce the Dirichlet series

$$(6.7) \qquad F(\chi, s, d) := \sum_{n \in N_d} n^{-s} \lambda(n) |S(\chi, n)|^2.$$

This converges for $\sigma > 1$ to an analytic function of s, since

$$|S(\chi, n)| \leqslant r(n) = O(n^{\varepsilon}) \qquad \text{for any } \varepsilon > 0.$$

Now $\lambda(n)$ and $|S(\chi, n)|^2$ are both multiplicative, so that (6.7) can be written as an Euler product

$$(6.8) \qquad \prod_{p \nmid d} \{1 + \sum_{k \geqslant 1} p^{-ks} \lambda(p^k) |S(\chi, p^k)|^2\}$$

for $\sigma > 1$. As in Section 5 we rearrange Euler factors and separate off the primes with $R(p) = \emptyset$, and those dividing e but not d, obtaining

$$(6.9) \qquad F(\chi, s, d) = G(\chi, s, d) \prod_{\substack{p \nmid e \\ r(p) > 0}} \exp\{p^{-s} \lambda(p) |S(\chi, p)|^2\}$$

for $\sigma > 1$, where $G(\chi, s, d)$ is analytic, non-zero and bounded for $\sigma \geqslant 3/4$, while $G(\chi, 1, d) \neq 0$. Taking logarithms in (6.9) we find that

$$(6.10) \qquad \log F(\chi, s, d) - \log G(\chi, s, d) = \sum_{\substack{p \nmid e \\ r(p) > 0}} p^{-s} \lambda(p) |S(\chi, p)|^2$$

for $\sigma > 1$. Now for $p \nmid e$ both $\lambda(p)$ and $|S(\chi, p)|^2$ are uniquely determined by the Frobenius class of p in $\operatorname{Gal} F/Q$, as was shown in Section 2. Applying Chebotarev's density theorem, we obtain

$$(6.11) \qquad \log F(s, \chi, d) - \log G(s, \chi, d)$$

$$= \left\{ \sum_{C \in \mathscr{C}} \lambda(C) |S(\chi, C)|^2 \frac{\#C}{\#G} \right\} \log \frac{1}{s-1} + P^*(s, \chi)$$

for $\sigma > 1$, with the same notation as in Section 5, where $P^*(s, \chi)$ is of the same type as $P(s, \chi)$ of (5.10), and has the same order of growth in (5.11). Here $\lambda(C)$ is the common value of $\lambda(p)$ for all $p \leftrightarrow C$, and $S(\chi, C) = S(\chi, p)$ for all $p \leftrightarrow C$.

The quantity

$$(\#G)^{-1} \sum_{C \in \mathscr{C}} \lambda(C) \, \#C \, |S(\chi, C)|^2$$

can be re-expressed as

$$(\#G)^{-1} \sum_{g \in G}' 1_*^G(g)^{-2} |\chi_*^G(g)|^2$$

(notation as in Section 4), where $\sum'$ is taken over all $g \in G$ with $1_*^G(g) \neq 0$. Since we have chosen $B = T^{\perp}$ and $\chi \notin B^{\perp}$, there is at least one $g \in G$ with $|\chi_*^G(g)|^2 < 1_*^G(g)^2$, while $|\chi_*^G(g)|^2 \leqslant 1_*^G(g)^2$ for every $g \in G$. Consequently, for any $\chi \notin B^{\perp}$, we have

$$\partial(\chi) := (\# G)^{-1} \sum_{C \in \mathscr{C}} \lambda(C) \# C \, |S(\chi, C)|^2 < \partial, \tag{6.12}$$

with ∂ as in Sections 2–5. Proceeding as in [7], [8] and [10] we obtain for W_χ the asymptotic expansion

$$W_\chi \sim C(\chi, d) \, x (\log x)^{\partial(\chi) - 1} \{1 + \sum_{j \geqslant 1} c_j(\chi, d) (\log x)^{-j}\}, \tag{6.13}$$

where $C(\chi, d) > 0$. Summing (6.13) over all $\chi \notin B^{\perp}$, and applying (6.5), we obtain a sharper version of (6.1). We have thus proved $\tilde{H} = H_d = T^{\perp}$ for $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$, and also Theorem II. We remark that the hypothesis $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$ has not been used in the proof of (6.13).

7. Proof of Theorem III. We shall now apply some standard global classfield theory to show that H_d always coincides with H_1. First let $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$. Then we have already shown that $H_d = T^{\perp}$ (notation as in §6). Let C be the subfield of $\tilde{R}$ fixed by B, the subgroup corresponding to $T^{\perp}$ under the identification of A with $\operatorname{Gal} \tilde{R}/K$ via the Artin map. Then C/K is finite abelian. We shall prove that $H_d = H_1$ by examining the divisor class group in K which has C as its classfield. For any modulus (conductor) $\mathfrak{m}$ let $I^{\mathfrak{m}}$ be the group of fractional ideals of K which are prime to the finite part of $\mathfrak{m}$, and let $I_0^{\mathfrak{m}}$ be the subgroup of $I^{\mathfrak{m}}$ consisting of all principal (α) with $\alpha \equiv 1 \, (\operatorname{mod}^{\times} \mathfrak{m})$.

Consider now the group Ω of all fractional ideals $\mathfrak{a}$ in K for which the Artin symbol $\varphi(\mathfrak{a}) := \left(\dfrac{C/K}{\mathfrak{a}}\right)$ is a well-defined element of $\operatorname{Gal} C/K$. Certainly $I^{\mathfrak{f}} \subseteq \Omega$ since $\left(\dfrac{\tilde{R}/K}{\mathfrak{a}}\right)$ is defined for all $\mathfrak{a} \in I^{\mathfrak{f}}$ and $\left(\dfrac{C/K}{\mathfrak{a}}\right)$ is then the image of $\left(\dfrac{R/K}{\mathfrak{a}}\right)$ under the natural projection of $\operatorname{Gal} \tilde{R}/K$ onto $\operatorname{Gal} C/K$. Moreover $I_0^{\mathfrak{f}} \subseteq \ker \varphi$ since $\left(\dfrac{\tilde{R}/K}{\mathfrak{a}}\right) = 1$ for all $\mathfrak{a} \in I_0^{\mathfrak{f}}$. The relation $H_d = T^{\perp} \cong B$ can be rephrased as $\ker \varphi \cap I^d = I^d \cap (I_0^{\mathfrak{f}} \ker N)$, where $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$, and N is the absolute norm homomorphism $I^1 \to \boldsymbol{Q}^*$. It follows that $\ker \varphi \cap I^d = X \cap I^d$, where $X = I^{\mathfrak{f}} \cap (I_0^{\mathfrak{f}} \ker N)$, since $I^d \subseteq I^{\mathfrak{f}}$. Since $\ker \varphi \cap I^{\mathfrak{f}}$ and X are both between $I_0^{\mathfrak{f}}$ and $I^{\mathfrak{f}}$, it follows by a standard argument ([3], p. 166–167) that $X = I_0^{\mathfrak{f}}(\ker \varphi \cap I^d) = I_0^{\mathfrak{f}}\big(I^d \cap (I_0^{\mathfrak{f}} \ker N)\big) = \ker \varphi \cap I^{\mathfrak{f}}$. Thus the fractional ideals in X and in $I^d \cap (I_0^{\mathfrak{f}} \ker N)$ occupy precisely the same set of ray-classes $(\operatorname{mod}^{\times} \mathfrak{f})$, and this proves that $H_1 = H_d$. It also follows that $H_1 \supseteq H_k \supseteq H_{ke} = \tilde{H} = H_1$ for any $k \geqslant 1$, i.e. we have proved Theorem III.

In view of Theorem III the notion of d-maximal range is now redundant, and can be replaced simply by that of a maximal range (meaning a 1-maximal range). In order to remove the hypothesis $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$ from Theorem II it is only necessary to observe that (6.13) is valid for arbitrary $d \geqslant 1$, as is Theorem I.

8. Proof of Theorem IV. We shall obtain this theorem as a corollary of a formula somewhat analogous to (6.1), but with more restrictions on the n involved in the summation. In the first place we restrict the summation to squarefree members of $\mathscr{N}(x, d)$. To describe the further restrictions we recall the subgroups W_p introduced in Section 1. We shall work once more under the assumption that $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$, since this hypothesis not only strengthens the asserted result but makes it easier to prove. For primes p unramified in F/Q the values of $R(p)$ and W_p only depend (by Section 2) on the Frobenius class $\left(\dfrac{F/Q}{p}\right)$; if this class is C we can thus denote these values by $R(C)$ and W_C respectively. By Section 1, given C there is a unique minimal $v = v(C) > 0$ such that $W_C = R(C)^v$, and then there is a unique minimal $k = k(C) > 0$ such that $R(C)^{v+m} = W_C$ $(m \geqslant 0)$ if and only if $0 \leqslant m \equiv 0 (\operatorname{mod} k)$.

Now let $\omega_C(n) := \# \{p; \, p \text{ prime}, \, p \mid n, \, p \leftrightarrow C\}$, for each $n \geqslant 1$ and each $C \in \mathscr{C}$ of Section 5, and let $\zeta(C)$ be any $k(C)$th root of 1. For any fixed vector $\zeta = \{\zeta(C)\}_{C \in \mathscr{C}}$ we consider the quantity

$$G(x, \zeta, d) := \sum_{\substack{n \in \boldsymbol{N}_d \\ n \leqslant x}} \mu^2(n) \lambda(n) V(n) \big(\log(x/n)\big) \prod_{C \in \mathscr{C}} \zeta(C)^{\omega_C(n) - v(C)}, \tag{8.1}$$

where $\mu(n)$ is the standard Möbius function, and the other notation is as in Section 6. We shall obtain the asymptotics of (8.1) by imitating, with appropriate changes, the methods of Sections 5 and 6. We have, to begin with,

$$\begin{aligned} &G(x, \zeta, d) \\ &= 2(A:\tilde{H})^{-1} \sum_{\chi \notin \tilde{H}^{\perp}} \sum_{\substack{n \in \boldsymbol{N}_d \\ n \leqslant x}} \mu^2(n) \lambda(n) |S(\chi, n)|^2 \big(\log(x/n)\big) \prod_{C \in \mathscr{C}} \zeta(C)^{\omega_C(n) - v(C)} \\ &= 2(A:\tilde{H})^{-1} \prod_{C \in \mathscr{C}} \zeta(C)^{-v(C)} \sum_{\chi \notin \tilde{H}^{\perp}} G(x, \zeta, d, \chi), \end{aligned} \tag{8.2}$$

in view of Lemma 4.3., where

$$G(x, \zeta, d, \chi) := \sum_{\substack{n \in \boldsymbol{N}_d \\ n \leqslant x}} \lambda(n) \mu^2(n) |S(\chi, n)|^2 \big(\log(x/n)\big) \prod_{C \in \mathscr{C}} \zeta(C)^{\omega_C(n)}. \tag{8.3}$$

8A. The function $\mu^2(n)\lambda(n)|S(\chi, n)|^2 \prod_{C\in\mathscr{C}} \zeta(C)^{\omega_C(n)}$ is multiplicative (by §2), with absolute value $\leqslant 1$. Hence we have an Euler product identity

$$(8.4)\qquad \sum_{n\in N_d} n^{-s}\mu^2(n)\lambda(n)|S(\chi, n)|^2 \prod_{C\in\mathscr{C}} \zeta(C)^{\omega_C(n)} = \prod_{p\nmid d} \{1+p^{-s}\lambda(p)|S(\chi, p)|^2 \prod_{C\in\mathscr{C}} \zeta(C)^{\omega_C(p)}\}$$

for $\sigma > 1$. Since we have assumed that $d \equiv 0\big(\operatorname{mod}(e(K, \mathfrak{f}))\big)$, we can simplify the right-hand side of (8.4) to

$$(8.5)\qquad \prod_{C\in\mathscr{C}} \prod_{\substack{p\leftrightarrow C\\ p\nmid d}} \{1+\lambda(C)\zeta(C)|S(\chi, p)|^2 p^{-s}\}.$$

Applying Chebotarev's density theorem once more, we see that (8.5) has the form

$$(8.6)\qquad A(s, \mathfrak{f}, \chi, \boldsymbol{\zeta})\exp\left(\log\frac{1}{s-1}\cdot\sum_{C\in\mathscr{C}} \zeta(C)\lambda(C)|S(\chi, C)|^2\frac{\#C}{\#G}\right),$$

where $A(s, \mathfrak{f}, \chi, \boldsymbol{\zeta})$ behaves like $\exp P(s, \chi)$ (with $P(s, \chi)$ as in (5.10)) in the region (5.11). Since $|\zeta(C)| = 1$ we have

$$(8.7)\qquad \operatorname{Re}\sum_{C\in\mathscr{C}} \zeta(C)\lambda(C)|S(\chi, C)|^2\frac{\#C}{\#G} \leqslant \sum_{C\in\mathscr{C}} \lambda(C)|S(\chi, C)|^2\frac{\#C}{\#G}$$

for all $\chi\in\hat{A}$, while equality holds in (8.7) if and only if $\zeta(C) = 1$ for all $C\in\mathscr{C}$. Since we only consider those $\chi\notin\tilde{H}^{\perp}$, it follows by an argument similar to that of §6C that $G(x, \boldsymbol{\zeta}, d) = O_d(x(\log x)^{\partial'-1})$ for some $\partial' = \partial'(\boldsymbol{\zeta}) < \partial$ and every choice of $\boldsymbol{\zeta}$. If we use this estimate and sum over all vectors $\boldsymbol{\zeta}$ we deduce that

$$(8.8)\qquad G^*(x, d) := \sum_{\substack{n\in\mathscr{M}(x,d)\\ \omega_C(n)\equiv v(C) (\operatorname{mod} k(C))\\ \forall C\in\mathscr{C}}} \mu^2(n)\lambda(n)V(n)\log(x/n) = O_d\big(x(\log x)^{\partial''-1}\big),$$

where $\partial'' < \partial$.

8B. Let us call $n\geqslant 1$ *defective at* $C(\in\mathscr{C})$ if we have $\omega_C(n) < v(C)$. Let $\delta(n) = 1$ if $r(n) > 0$, $\delta(n) = 0$ otherwise. Then, if $\sum_C'$ denotes summation over $n\in N_d$ defective at C, we have

$$(8.9)\qquad \sum_C{}' \delta(n)n^{-s} = P^{**}\Big(\sum_{p\leftrightarrow C} p^{-s}\Big) \prod_{\substack{r(p)>0\\ p\not\leftrightarrow C}} (1-p^{-s})^{-1}$$

for $\sigma > 1$, where $P^{**}(T)$ is a polynomial with coefficients which are analytic functions of s, uniformly bounded for $\sigma\geqslant 3/4$. It is simple to deduce from

(8.9) and the Chebotarev density theorem that

$$(8.10)\qquad \sum_C{}' \delta(n)\log(x/n) = O_d\big(x(\log\log x)^{a(C)}(\log x)^{\partial-1-\#C/\#G}\big)$$

for some $0\leqslant a(C)\leqslant v(C)-2$. (A somewhat similar estimation is carried out in [5] and [10].)

An integer $n\in\mathscr{M}(x, d)$ will be called *replete* if $\omega_C(n)\geqslant v(C)$ for all $C\in\mathscr{C}$. Then a comparison of (2.6) and (8.10) shows that almost all members of $\mathscr{M}(x, d)$ are replete. Moreover, if we make a simple modification of the generating functions in §8A and §5 it is easy to prove that the proportion of $\mathscr{M}(x, d)$ occupied by squarefree n, with $\omega_C(n)\equiv v(C)\ \big(\operatorname{mod} k(C)\big)$ for all $C\in\mathscr{C}$, tends to a positive limit as $x\to\infty$. Almost all of these n will be replete, by another comparison with (2.6) and (8.10). Also, by Theorem II, almost all of these n have a maximal range, which, since it contains the principal ray-class $(\operatorname{mod}^{\times}\mathfrak{f})$, must be $H_d = H_1$. Thus, for these n, on the one hand $R(n) = H_1$, while, on the other hand, $R(n) = \langle W_C;\, C\in\mathscr{C}\rangle$. Consequently $\tilde{H} = H_1 = H_d = \langle W_C;\, C\in\mathscr{C}\rangle$, and this certainly implies Theorem IV, since $\langle W_p;\, p\nmid d\rangle$ certainly contains $\langle W_C;\, C\in\mathscr{C}\rangle$.

9. A generalisation of central classfields.

9A. Let $\bar{K}/Q$ be a finite Galois extension. The (narrow) Hilbert classfield of $\bar{K}$ is the maximal finite abelian extension $H(\bar{K})$ of $\bar{K}$ ramified only at the real infinite places of $\bar{K}$. In fact $H(\bar{K})/Q$ is also a Galois extension, since the principal narrow ideal class is invariant under the action of $\operatorname{Gal}\bar{K}/Q$. Also $\operatorname{Gal}H(\bar{K})/\bar{K}$ is canonically isomorphic to the narrow ideal class group of $\bar{K}$, via the Artin map. Scholz and Fröhlich [1], [2], [9] studied an interesting subfield of $H(\bar{K})$, the so-called central classfield of $\bar{K}$, defined by the following procedure. Consider all fields L satisfying:

(i) $\bar{K}\leqslant L\leqslant H(\bar{K})$;
(9.1) (ii) L/Q is Galois;
(iii) $\operatorname{Gal}L/\bar{K}$ is a central subgroup of $\operatorname{Gal}L/Q$.

Then the *central classfield* $C(\bar{K})$ is the unique maximal field amongst the L satisfying (9.1).

We can characterise $C(\bar{K})$ in terms of subgroups of $G = \operatorname{Gal}H(\bar{K})/Q$. Let $A = \operatorname{Gal}H(\bar{K})/\bar{K}$; then A is abelian and $A\lhd G$. Let F' be the fixed field of the commutator subgroup $[A, G] := \langle aga^{-1}g^{-1};\, a\in A, g\in G\rangle$. Since $[A, G]$ is normal both in G and in A, it is clear that F'/Q is Galois, with group $G/[A, G]$. Moreover $A/[A, G]$ is central in $G/[A, G]$, and $A/[A, G]$ is the Galois group of $F'/\bar{K}$. Consequently F' is one of the fields satisfying (9.1).

Conversely, for any L satisfying (9.1), let $B = \operatorname{Gal}H(\bar{K})/L$, so that $B\lhd G$ and $B\leqslant A$. Then $\operatorname{Gal}L/Q = G/B$ and $\operatorname{Gal}L/\bar{K} = A/B$, so that A/B is central in G/B. The latter happens if and only if $[A, G] \quad B$, so that $L \subseteq F'$, the fixed field of $[A, G]$. It follows that $C(K)$ is, indeed, unique, and is the fixed field of $[A, G]$.

We now determine the divisor class group in K having $C(K)$ as classfield. We replace $K, \tilde{R}$ and F of Section 2 by $\bar{K}$, $H(\bar{K})$ and $H(\bar{K})$ respectively (recalling that $H(K)/\boldsymbol{Q}$ is Galois). Then G of Section 2 becomes $\operatorname{Gal} H(K)/\boldsymbol{Q}$, and Γ of Section 2 reduces to $A = A(K, \mathfrak{f}) = A(K, (1)\infty)$. By Lemma 4.2 the characters $\chi \in \hat{A}$ satisfying $\langle \chi_*^G, \chi_*^G \rangle_G = \langle 1_*^G, 1_*^G \rangle_G$ form a subgroup T of $\hat{A}$, and the proof of Lemma 4.2 shows that these are exactly those $\chi \in \hat{A}$ such that $\chi(a) = \chi(g^{-1}ag)$ for all $a \in A, g \in G$, i.e. are precisely those $\chi \in \hat{A}$ which are trivial on $[A, G]$. Consequently, by Theorem III and the arguments of Section 7 (with K replaced by $\bar{K}$), we see that $C(\bar{K})$ is classfield to the ideal group $I_0 \ker N$, where I_0 is the group of all principal fractional ideals (α) with $\alpha \in \bar{K}^*$, $\alpha \gg 0$, and N is the absolute norm morphism $I \to \boldsymbol{Q}^*$, I being the group of all fractional ideals in $\bar{K}$.

9B. We now seek to generalise the definition of central classfield by dropping the condition that $K/\boldsymbol{Q}$ be Galois, and replacing narrow ideal classes by ray-classes $(\operatorname{mod}^x \mathfrak{f})$ for arbitrary $\mathfrak{f}$. We revert to the notation and hypotheses of Section 2. In terms of classfields it appears reasonable to define the central classfield $(\operatorname{mod}^x \mathfrak{f})$ of K to be $C(K, \mathfrak{f})$, the classfield over K corresponding to the ideal group $I' \cap (I_0' \ker N)$ encountered in Section 7, and this is what we shall, in fact, do. With this definition, if $K/\boldsymbol{Q}$ is Galois, and $\mathfrak{f} = \mathfrak{O}_K \cdot \infty$, then $C(K, \mathfrak{f})$ reduces to the field considered by Scholz and Fröhlich, in view of our arguments in §9A.

By means of our main theorems we can characterise $\operatorname{Gal} C(K, \mathfrak{f})/K$ as the dual of the subgroup

$$T = \{\chi \in \hat{A};\ \langle \chi_*^G, \chi_*^G \rangle_C = \langle 1_*^G, 1_*^G \rangle_G\}.$$

In particular, if A, G and Γ are known, there is no particular difficulty in determining $C(K, \mathfrak{f})$ as the fixed field of a certain subgroup of G, as we now show. We introduce

$$\Delta := \langle g^{-1}\gamma g^{-1}\gamma^{-1};\ \gamma \in \Gamma, g \in G, g^{-1}\gamma g \in \Gamma \rangle \quad \text{and} \quad V := \operatorname{Gal} F/\tilde{R},$$

two subgroups of G, with $\Delta \leqslant \Gamma$. We consider characters $\chi \in \hat{A}$. Then we have $\chi \in T$ if and only if the lifted character χ_* of Γ satisfies all three of the following conditions:

(i) χ_* is a degree-one character of Γ;
(ii) χ_* is trivial on V;
(iii) χ_* is trivial on Δ.

(Of these, the first two are trivial, while the third is immediate from the proof of Lemma 4.2.) On the other hand, if χ_* is any character of Γ satisfying (i)–(iii), then it is obviously expressible as the lifting of a character of A, and the latter must belong to T. It follows at once that $\operatorname{Gal} F/C(K, \mathfrak{f}) = \langle V, \Delta \rangle$.

An interesting simplification occurs if the conductor $\mathfrak{f}$ is taken to be $(f)\infty$, with $0 < f \in \boldsymbol{Z}$ divisible by all primes ramified in $K/\boldsymbol{Q}$. If now $\bar{K}/\boldsymbol{Q}$ is the Galois hull of $K/\boldsymbol{Q}$, the ray-class field $H(\bar{K}, \mathfrak{f})$ of $\bar{K}(\operatorname{mod}^x \mathfrak{f})$ is also Galois over $\boldsymbol{Q}$, and $H(K, \mathfrak{f}) = \tilde{R}$ is the maximal abelian extension of K contained in $H(\bar{K}, \mathfrak{f})$. Since, in the above characterisations of $C(K, \mathfrak{f})$, we may replace $F/\boldsymbol{Q}$ by any larger finite Galois extension, we can replace F by $H(\bar{K}, \mathfrak{f})$. Thus, in this case, we obtain $V = \Gamma' = [\Gamma, \Gamma]$. Consequently any degree-one character of Γ is trivial on V and, moreover, $V \subseteq \Delta$. Thus, in this case, $C(K, \mathfrak{f})$ is the fixed field of Δ, and this characterisation is almost as straightforward as the corresponding one in the "classical" case described in §9A.

10. Relations to earlier work; lines for further research.

10A. The original motive for the research giving rise to this paper was the desire to improve upon the results of [5] and [6]. There results substantially equivalent to Theorems I, II and IV were obtained by rather different methods for certain rather special fields K, with the special conductor $\mathfrak{f} = \mathfrak{O}_K\infty$, (corresponding to the narrow ideal class group of K). The special case $K/\boldsymbol{Q}$ Galois was covered by the methods of [5], where there was no need for a result of the depth and subtlety of the present Theorem III. The crucial point in the argument of [5] is the fact that $\operatorname{Gal} K/\boldsymbol{Q}$ acts *transitively* on the set of prime ideals of $\mathfrak{O}_K$ lying over a given p in $\boldsymbol{Z}$, while the invariance of the narrow principal class under the action of $\operatorname{Gal} K/\boldsymbol{Q}$ shows that the range $R(p^f)$ (where f is the residual degree corresponding to p) consists precisely of a single orbit of the action of $\operatorname{Gal} K/\boldsymbol{Q}$ on the narrow ideal class group of K. It seems clear that it would be very difficult to handle the general non-Galois extension $K/\boldsymbol{Q}$ by any method which attemps directly to exploit Galois actions on primes in $\mathfrak{O}_K$. (As it happens, a fortunate accident enables one to prove Theorems I, II and IV by such methods in the special case where $[\bar{K}:\boldsymbol{Q}] = q[K:\boldsymbol{Q}]$, where q is prime, not dividing $[K:\boldsymbol{Q}]$, $\bar{K}/\boldsymbol{Q}$ being the Galois hull of $K/\boldsymbol{Q}$. In particular, this covers the case of "generic cubic" $K/\boldsymbol{Q}$).

10B. Prospects for generalising results on ranges. It seems fairly clear that, with minor modifications, the notion of range, and the possibility of obtaining asymptotic results on the distribution of ranges, can be generalised at least to the following context. Let A be any finite-dimensional commutative semisimple $\boldsymbol{Q}$-algebra (thus, by Wedderburn's theorem, isomorphic (in the abstract) to a direct sum of algebraic number fields). An interesting special case here would be $A = KG$, where G is a finite abelian group and K is an algebraic number field. Let $\mathfrak{O}$ be any $\mathbf{Z}$-order of maximal $\mathbf{Z}$-rank in A (e.g. $\mathfrak{O} = \mathfrak{O}_K G$ if $A = KG$). We work with invertible integral ideals of $\mathfrak{O}$, for which the classical notion of absolute norm generalises in a satisfactory manner. We then define the range $R(n)$ of $n \geqslant 1$ to be the set of all $\mathfrak{O}$-isomorphism classes of invertible integral $\mathfrak{O}$-ideals with absolute norm n. The results of Sections 1 and 2 carry over without difficulty, provided that the auxiliary field F of 2 is suitably altered. The isomorphism classes of invertible $\mathfrak{O}$-fractional ideals can be associated with ray-classes $(\mathrm{mod}^{\times} \mathfrak{f})$ of fractional ideals of $\hat{\mathfrak{O}}$, the unique maximal $\mathbf{Z}$-order in A, provided that $\mathfrak{f}$ is a multiple of the conductor of $\hat{\mathfrak{O}}$ over $\mathfrak{O}$. We shall develop this and related ideas in a forthcoming joint paper with G. Everest (UEA).

10C. Central classfields. The recent monograph [2] by A. Fröhlich reworks the earlier theory of central classfields in terms of idèles and cohomology, simplifying and clarifying many of the earlier results, and highlighting their relationship with a number of important topics in Galois theory. It would be interesting to try to extend the approach of [2] to exploit our generalised concept of central classfield $(\mathrm{mod}^{\times} \mathfrak{f})$, perhaps obtaining thereby a sort of "non-Galois" classfield theory for certain number fields. This is, of course, highly speculative at present, since there is no clear picture of what such a theory should encompass.

10D. The relation obtained in our Theorem IV appears to indicate some hitherto unexpected relations in the idèle-class group of a number field, and probably merits some kind of explicit formulation in terms of non-abelian cohomology theory. We cannot go further into this question here.

References

[1] A. Fröhlich, *On the absolute class group of abelian fields*, J. London Math. Soc. 29 (1954), 211–217; 30 (1955), 72–80.

[2] — *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics 24 (1983), American Math. Soc. Providence, R. I.

[3] G. Janusz, *Algebraic number fields*, Academic Press, 1973.

[4] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

[5] R. W. K. Odoni, *A new equidistribution property of norms of ideals in given classes*, Acta Arith. 33 (1977), 53–63.

[6] — *Some global norm density results obtained from an extended Čebotarev density theorem*; in: *Algebraic Number Fields* (ed. A. Fröhlich), Academic Press, 1977, pp. 485–495.

[7] — *Solution of some problems of Serre on modular forms; the method of Frobenian functions*; in: *Recent Progress in Analytic Number Theory* (vol. 2), Academic Press, 1981, pp. 159–169.

[8] — *Notes on the method of Frobenian functions, with applications to the coefficients of modular forms*; in: *Elementary and analytic theory of numbers*, Banach Center Publications, vol. 17, Polish Scientific Publishers, Warsaw 1985, pp. 371–403.

[9] A. Scholz, *Totale Normresten, die keinen Normen sind, als Erzeuger nicht Abel'scher Körpererweiterungen*, J. Reine Angew. Math. 175 (1936), 100–107; 182 (1940), 217–234.

[10] J.-P. Serre, *Sur la divisibilité de certaines fonctions arithmétiques*, L'Enseignment Math., 22 (1976), 227–260.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF EXETER
Exeter, Great Britain

Received on 21.12.1987 (1774)