In gleicher Weise erhält man

$$(C_0^n : K^{\times n}) = (C_{0(n_2)}^{n_2} : K^{\times n_2}),$$

und es genügt nun, $C_{0(n_2)} = C_{n_2}(K(w)/K)$ zu beweisen, denn dann ist $(C_0^n : K^{\times n}) = [K(w) : K]$, und aus Lemma 7 folgt $K(w) = K(C_0)$.

Offensichtlich ist $C_{0(n_2)} \subseteq C_{n_2}(K(w)/K)$. Sei nun

$$x \in C_{n_2}(K(w)/K) = \langle K^{\times}, C_{n_2}(K(w)/K)^{n_1}\rangle,$$

$x = zx_1^{n_1}$ mit $z \in K^{\times}$, $x_1 \in C_{n_2}(K(w)/K) \subseteq C_n(L/K) = \langle C, W_{n_1} \cap L\rangle$ (Lemma 12(d)), also $x_1 = x_2\xi$ mit $x_2 \in C$, $\xi \in W_{n_1} \cap L$. Damit folgt

$$x = zx_2^{n_1} \in \langle K^{\times}, C^{n_1}\rangle \subseteq C_{(n_2)} \subseteq C_1,$$

da $(T : K^{\times})$ zu n_2 prim ist, und ich erhalte

$$x \in \big(C_1 \cap K(w)\big)_{(n_2)} = C_{0(n_2)};$$

also gilt auch $C_{n_2}(K(w)/K) \subseteq C_{0(n_2)}$. □

Literaturverzeichnis

[1] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), S. 40–64.

[2] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 26 (1975), S. 307–308.

[3] S. Lang, *Algebra*, New York 1967.

[4] A. Schinzel, *On linear dependence of roots*, Acta Arith. 28 (1975), S. 161–175.

[5] — *Abelian binomials, power residues and exponential congruences*, ibid. 33 (1977), S. 245–274.

UNIVERSITÄT ESSEN – GESAMTHOCHSCHULE
Essen

Eingegangen am 30. 3. 1977
und in reviedierter Form am 20. 6. 1977 (930)

ACTA ARITHMETICA
XXXVI (1980)

The number of different lengths of irreducible factorization of a natural number in an algebraic number field

by

S. Allen (Milton Keynes)* and P. A. B. Pleasants (Cardiff)

1. Introduction. An integer in an algebraic number field k is *irreducible* if it is not a product of two other integers of k neither of which is a unit (or, equivalently, if it is not a product of two integers of smaller norm). Clearly every integer of k can be expressed as a product of irreducibles, and it is well known that every integer of k has a unique irreducible factorization (apart from the order of the factors and multiplying the factors by units of k) if and only if the class number h of k is 1. This remains true if we restrict attention to the irreducible factorization in k of rational integers only (instead of considering all integers of k). The number of irreducibles in such a factorization (counting each as many times as it occurs) is called the *length* of the factorization, and L. Carlitz [4] has pointed out the interesting fact that a necessary and sufficient condition for no integer of k to have irreducible factorizations of different lengths is that $h \leqslant 2$. Again, this remains true if we restrict attention to the lengths of irreducible factorizations in k of rational integers.

Let $f(m) = f_k(m)$ be the number of essentially different irreducible factorizations in k of the rational integer m, and let $g(m) = g_k(m)$ be the number of different lengths of irreducible factorizations of m in k. If $\varphi(m)$ is an arithmetic function then a function $\psi(m)$ is an *average order* for it if

$$\sum_{m\leqslant x}\varphi(m) \sim \sum_{m\leqslant x}\psi(m)$$

and is a *normal order* for it if, for every positive ε and x,

$$(1-\varepsilon)\psi(m) < \varphi(m) < (1+\varepsilon)\psi(m)$$

for all except $o_\varepsilon(x)$ of the positive integers less than x. In a conversation with W. Narkiewicz in 1965 P. Turán asked whether the functions $f(m)$

* This author was in receipt of financial support from the Science Research Council during the period in which the initial work for this paper was carried out.

and $g(m)$ have increasing normal orders, and Narkiewicz [7] showed that if k is a quadratic field with $h = 2$ then $f(m)$ has no increasing normal order but that $\log f(m)$ has $\frac{1}{4}(\log\log m)(\log\log\log\log m)$ as both a normal order and an average order. Narkiewicz conjectured that $f(m)$ never has an increasing normal order, and this was recently proved by J. Rosiński and J. Śliwa [14]. Narkiewicz also showed in [7] that $g(m)$ has average and normal order $\frac{1}{9}\log\log m$ for quadratic fields with $h = 3$ and $\frac{1}{8}\log\log m$ for quadratic fields with class group $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ (so that $h = 4$), and he stated that his method applied to any quadratic field with a given class group.

Here we take up the question of the order of $g(m)$. We show that for every algebraic number field k with $h \geqslant 3$ there is a positive constant $C = C_k$ such that $g_k(m)$ has average and normal order $C_k \log\log m$. (This has recently been proved independently, for the normal order at least, by Narkiewicz and Śliwa [11]. More recently still Narkiewicz [10] has shown that $\log f(m)$ has normal order $D_k \log\log m \log\log\log m$ for every algebraic number field k with $h \geqslant 2$.) We shall deal with the average and normal orders at the same time by showing that

$$\sum_{m \leqslant x} \big(g_k(m) - C_k \log\log m\big)^2 = O(x \log\log x).$$

This clearly implies that $g(m)$ has normal order $C\log\log m$, and by Cauchy's inequality

$$\sum_{m \leqslant x} |g_k(m) - C_k \log\log m| \leqslant \Big(x \sum_{m \leqslant x} \big(g_k(m) - C_k \log\log m\big)^2\Big)^{1/2}$$
$$= O\big(x(\log\log x)^{1/2}\big),$$

so that $g(m)$ has average order $C\log\log m$ too. For given k the constant C_k can be calculated in terms of the class group H of k and the densities $\delta(X)$ (X in H) of rational primes with a prime ideal factor in k belonging to the ideal class X. (The definition of $\delta(X)$ will be made precise in the next section.) We find C_k explicitly (in terms of the $\delta(X)$'s) when H is a cyclic p-group and when $H = \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ or $\boldsymbol{Z}_6$. We also show that there is a number $C(H)$, depending only on the class group H, such that $C_k \geqslant C(H)$, with equality when (but not only when) k is normal of prime degree, and we find $C(H)$ explicitly when H is a homocyclic p-group (that is, a direct product of cyclic p-groups of the same order). In addition we find bounds for C_k and $C(H)$, showing, in particular, that

$$\tfrac{1}{9} \leqslant C_k < \tfrac{1}{4}[k:\boldsymbol{Q}] + \tfrac{1}{2}, \qquad \tfrac{1}{9} \leqslant C(H) < \tfrac{1}{2}$$

and

$$C(H) \to \tfrac{1}{2} \quad \text{as} \quad h \to \infty,$$

and we calculate $C(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4)$ (to show that our treatment of homocyclic p-groups does not always work for non-homocyclic ones).

A related topic that has received more attention (see, for example, [9], Chapter IX, [8], [1] and [12]) is the problem of finding asymptotic formulae for the number of rational integers less than x, and the number of integers of k with norm less than x, that have unique factorization or unique length of factorization in k (or, more generally, that have f_k or g_k below a given bound).

We shall assume throughout that $h \geqslant 3$. (We already know that $g(m) = 1$ for all m when $h = 1$ or 2.) All O-constants depend on the field k.

We are indebted to Dr. R. W. K. Odoni and Prof. W. Narkiewicz for giving us access to their work before publication and for much helpful correspondence.

2. The densities $\delta(X)$. We now define the densities $\delta(X)$, explain why they exist, prove the useful relation $\delta(X^{-1}) = \delta(X)$ and obtain some inequalities for them.

For an ideal class X of k and a rational integer m we denote by $\Omega_X(m)$ the number of prime ideals belonging to the class X in the prime ideal factorization of m in k (counting each ideal as many times as it occurs). Then $\delta(X)$, the natural asymptotic density of the set of rational primes (with multiplicities) that are divisible by a prime ideal of k belonging to the class X, is

$$\lim_{x \to \infty} \frac{\log x}{x} \sum_{p \leqslant x} \Omega_X(p).$$

R. W. K. Odoni [12] has pointed out that there is a normal field $\bar{K}$ such that rational primes p and q belonging to the same conjugacy class of $\mathrm{Gal}(\bar{K}/\boldsymbol{Q})$ have $\Omega_X(p) = \Omega_X(q)$ for every X in H, and hence the densities $\delta(X)$ exist by Čebotarev's density theorem. We repeat Odoni's argument in order to get more information from it (namely, Lemma 1 (ii) and Lemma 2). The facts we use about Frobenius automorphisms and the Hilbert class field can all be found in [5], Chapter III, §2 and Chapter V, §13.

Let K be the Hilbert class field of k and $\bar{K}$ the normal closure of K over $\boldsymbol{Q}$. (This is not quite the same as the corresponding field used by Odoni, but it serves the same purpose.) Then the Galois group $\mathrm{Gal}(K/k)$ is isomorphic to the class group H of k. Define $\bar{H} = \mathrm{Gal}(\bar{K}/k)$ and $G = \mathrm{Gal}(\bar{K}/\boldsymbol{Q})$, so that $\bar{H}$ is a subgroup of G. Take a prime $\bar{\mathfrak{P}}$ in $\bar{K}$ that is unramified over $\boldsymbol{Q}$ and let $\mathfrak{P}$, $\mathfrak{p}$ and p be the primes in K, k and $\boldsymbol{Q}$ that it divides. If $\left[\dfrac{\bar{K}/k}{\bar{\mathfrak{P}}}\right] = \sigma \in G$ then p factorizes

$$\begin{tikzcd}
\boldsymbol{Q} \arrow[r, dash] & k \arrow[r, dash, "H"] & K \arrow[r, dash] & \bar{K} \\
p & \mathfrak{p} & \mathfrak{P} & \bar{\mathfrak{P}}
\end{tikzcd}$$

in k like the cycle structure of σ acting on the cosets of $\bar{H}$ (or, equivalently, like the cycle structure of σ acting on a set of conjugates of a generator of k over $\boldsymbol{Q}$). In fact the degree of $\mathfrak{p}$ is the smallest number f such that $\sigma^f \in \bar{H}$. Also

$$\left[\frac{K/k}{\mathfrak{P}}\right] = \left[\frac{\bar{K}/k}{\bar{\mathfrak{P}}}\right]\Big|_K = \left[\frac{\bar{K}/\boldsymbol{Q}}{\bar{\mathfrak{P}}}\right]^f\Big|_K,$$

and $\left[\frac{K/k}{\mathfrak{P}}\right] = \left(\frac{K/k}{\mathfrak{p}}\right)$ (the Artin symbol) determines the class of $\mathfrak{p}$. Now take any τ in G and define (with utter insensitivity to notation) $\tau\mathfrak{P} = (\tau\bar{\mathfrak{P}})\cap K$ and $\tau\mathfrak{p} = (\tau\bar{\mathfrak{P}})\cap k$. Then $\left[\frac{\bar{K}/\boldsymbol{Q}}{\tau\bar{\mathfrak{P}}}\right] = \tau\sigma\tau^{-1}$ and hence, $\left[\frac{K/k}{\tau\mathfrak{P}}\right] = (\tau\sigma\tau^{-1})^{\tau f}\big|_K$, where τf is the smallest number such that $(\tau\sigma\tau^{-1})^{\tau f} \in \bar{H}$ (or, equivalently, such that $\bar{H}\tau\sigma^{\tau f} = \bar{H}\tau$). Also $\tau_1\mathfrak{p} = \tau_2\mathfrak{p}$ if and only if $\bar{H}\tau_1 = \bar{H}\tau_2\sigma^i$ for some i. [Notice that if k is normal over $\boldsymbol{Q}$ then so is K, so that $\bar{K} = K$ and $\mathrm{Gal}(k/\boldsymbol{Q}) = G/H$. In this case the notation is not an abuse, as $\tau\mathfrak{p}$ is the image of $\mathfrak{p}$ by the restriction of τ to k. Since H is normal in G all the τf's are equal (for given σ) and the action of an element of $\mathrm{Gal}(k/\boldsymbol{Q})$ on the class group H is the same as the inner automorphism action of an element of the corresponding coset of H (on H considered as a normal subgroup of G).] Since the product of the primes of k dividing p is principal, we have, for each σ in G,

$$\left\{\prod{}'(\tau\sigma\tau^{-1})^{\tau f}\right\}\Big|_K = X_0,$$

where X_0 is the identity element of H and the product is taken over one representative τ from each cycle of cosets $\{\bar{h}\tau\sigma^i \mid \bar{h} \in \bar{H},\ i \in \boldsymbol{Z}\}$. Equivalently, since there are τf cosets in the cycle containing τ,

$$\left\{\prod(\tau\sigma\tau^{-1})\right\}\Big|_K = X_0,$$

where the product is taken over a set of coset representatives of $\bar{H}$ in G. When k is normal this becomes $\prod \tau X = X_0$, for every X in H, where the product is over all automorphisms τ in $\mathrm{Gal}(k/\boldsymbol{Q})$, and this can be written as $\operatorname{norm} X = X_0$.

If q is any rational prime belonging to the conjugacy class of σ (that is, which is unramified in $\bar{K}$ and whose prime factors in $\bar{K}$ have Frobenius automorphism in this conjugacy class) then there is some prime factor $\bar{\mathfrak{Q}}$ of q in $\bar{K}$ with $\left[\frac{\bar{K}/\boldsymbol{Q}}{\bar{\mathfrak{Q}}}\right] = \sigma$. Write $\mathfrak{q} = \bar{\mathfrak{Q}}\cap k$ and $\tau\mathfrak{q} = (\tau\bar{\mathfrak{Q}})\cap k$. Then $\tau\mathfrak{p} \leftrightarrow \tau\mathfrak{q}$ gives a one-one correspondence between the prime factors of p in k and the prime factors of q in k, corresponding factors having the same degree and belonging to the same ideal class.

We can now prove

LEMMA 1. (i) *For each class X the density $\delta(X)$ exists and is an integer multiple of $1/|G|$.*

(ii) $\delta(X^{-1}) = \delta(X)$.

(iii) $\sum_{m\le x} \Omega_X(m)/\delta(X) = x\log\log x + O(x)$.

(iv) $\sum_{m\le x} \big(\Omega_X(m)/\delta(X) - \log\log m\big)^2 = O(x\log\log x)$.

Proof. (i) We have just seen that for any conjugacy class $\mathscr{C}$ of G the value of $\Omega_X(p)$ is the same, $\Omega_X(\mathscr{C})$ say, for all rational primes that belong to it. Also, by the strong (natural density) form of Čebotarev's density theorem, the number of primes $p \le x$ that belong to $\mathscr{C}$ is $\mathrm{li}\,x|\mathscr{C}|/|G| + O\big(x\exp(-c\log^{1/2}x)\big)$, for some constant c. (This form of Čebotarev's theorem had already been stated by E. Artin as Satz 4 of [2], where it was derived from his reciprocity theorem. The reciprocity theorem itself was proved later [3] using an idea from Čebotarev's proof of his theorem about Dirichlet densities which had been published in the meantime.) Hence

$$(1)\qquad \sum_{p\le x}\Omega_X(p) = \Big(\sum_{\mathscr{C}}\Omega_X(\mathscr{C})|\mathscr{C}|/|G|\Big)\mathrm{li}\,x + O\big(x\exp(-c\log^{1/2}x)\big),$$

where the sum on the right runs over all conjugacy classes of G. (The finitely many rational primes that ramify in $\bar{K}$ contribute only $O(1)$.)

(ii) For $\mathfrak{p}$ and σ as above, if $\bar{\mathfrak{Q}}$ is an unramified prime of $\bar{K}$ with $\left[\frac{\bar{K}/\boldsymbol{Q}}{\bar{\mathfrak{Q}}}\right] = \sigma^{-1}$, $\mathfrak{q} = \bar{\mathfrak{Q}}\cap k$ and $\tau\mathfrak{q} = (\tau\bar{\mathfrak{Q}})\cap k$, then $\tau\mathfrak{q}$ has the same degree as $\tau\mathfrak{p}$ but is in the ideal class inverse to the class of $\tau\mathfrak{p}$. Since also $\tau_1\mathfrak{q} = \tau_2\mathfrak{q}$ if and only if $\tau_1\mathfrak{p} = \tau_2\mathfrak{p}$, we have

$$\Omega_{X^{-1}}(\mathscr{C}^{-1}) = \Omega_X(\mathscr{C}),$$

where $\mathscr{C}^{-1}$ is the conjugacy class consisting of the inverses of the elements of $\mathscr{C}$. Hence

$$\delta(X) = \sum_{\mathscr{C}}\Omega_X(\mathscr{C})|\mathscr{C}|/|G| = \sum_{\mathscr{C}}\Omega_{X^{-1}}(\mathscr{C}^{-1})|\mathscr{C}^{-1}|/|G| = \delta(X^{-1}).$$

(iii) From (1) we get

$$(2)\qquad \sum_{p\le x}\frac{\Omega_X(p)}{p} = \delta(X)\log\log x + O(1),$$

by partial summation. If $m = p_1^{a_1}\dots p_j^{a_j}$ then

$$\Omega_X(m) = a_1\Omega_X(p_1) + \dots + a_j\Omega_X(p_j),$$

and consequently

$$\sum_{m\leqslant x}\Omega_X(m) = \sum_{p^a\leqslant x}\Omega_X(p)\left[\frac{x}{p^a}\right] = x\sum_{p\leqslant x}\frac{\Omega_X(p)}{p} + x\sum_{\substack{p^a\leqslant x\\ a\geqslant 2}}\frac{\Omega_X(p)}{p^a} + O(x)$$
$$= \delta(X)x\log\log x + O(x),$$

since the second sum on the right is $O\left(\sum_p \frac{1}{p(p-1)}\right) = O(1)$.

(iv) This follows from (2) and Lemma 3.1 of [6] (look at the notation section at the beginning of the book to decipher it), since

$$\sum_{p^a\leqslant x}\frac{\Omega_X^2(p^a)}{p^a} = \sum_{p^a\leqslant x}\Omega_X^2(p)\frac{a^2}{p^a} = O\left(\sum_{p\leqslant x}\frac{1}{p} + \sum_p\frac{1}{p^2}\sum_{a\geqslant 2}\frac{a^2}{p^{a-2}}\right)$$
$$= O(\log\log x)$$

and

$$\sum_{m\leqslant x}(\log\log x - \log\log m)^2 = O(x),$$

as can be seen by splitting the sum at $x^{1/2}$, for example.

Another account of results of this sort can be found in [15] and [16].

Let X be an ideal class of k. Then X can be identified with an automorphism of K over k, and there are exactly $|\overline{H}|/|H|$ different automorphisms of $\overline{K}$ over k that extend X. If σ is one of these (in the conjugacy class $\mathscr{C}$, say) then the contribution to $\Omega_X(\mathscr{C})$ of primes $\mathfrak{p}$ of the form $\overline{\mathfrak{P}}\cap k$, where $\overline{\mathfrak{P}}$ has Frobenius automorphism σ, is $|G|/|\mathscr{C}|\,|\overline{H}|$, since there are $|G|/|\mathscr{C}|$ τ's with $\tau\sigma\tau^{-1} = \sigma$, but τ's in the same coset of $\overline{H}$ give rise to the same prime $\mathfrak{p}$ (and only τ's in the same coset, since the cycle of σ containing $\overline{H}$ has length 1). Hence the contribution of these primes to $\delta(X)$ is $(|G|/|\mathscr{C}|\,|\overline{H}|)(|\mathscr{C}|/|G|) = 1/|\overline{H}|$, and so

$$\delta(X) \geqslant \frac{|\overline{H}|}{|H|}\,\frac{1}{|\overline{H}|} = \frac{1}{h}.$$

(What we have done here is just to count the primes of k of degree 1 in the class X, and in fact the statement that $\delta_1(X) = 1/h$, where $\delta_1(X)$ is the contribution to $\delta(X)$ of the primes of degree 1 in k, is nothing but the prime ideal theorem ([9], Proposition 7.9, Corollary 4).)

The fact that $\delta(X^{-1}) = \delta(X)$ will be very useful later, and knowing that $\delta(X) = \delta(Y)$ for all pairs of ideal classes X and Y for which there is an automorphism α of H with $\alpha X = Y$ would be even more useful. However, Odoni has pointed out to us that this is almost certainly not true. If k is a normal field with Galois group $\boldsymbol{Z}_4$ generated by the automorphism τ and $\mathfrak{p}$ is a prime of k of degree 2 then $\mathfrak{p}(\tau\mathfrak{p})$ is principal, and so $\tau X = X^{-1}$, where X is the ideal class of $\mathfrak{p}$. Hence $\tau^2 X = X$ but τ^2 is not the identity. For a general cyclic quartic field one would expect some classes to be fixed by τ^2 and others (automorphic ones even) not. Any class X not fixed by τ^2 can contain no primes of degree 2, and so $\delta(X) = \delta_1(X) = 1/h$. On the other hand, the primes with Frobenius automorphism τ^2 have degree 2, and some ideal class X must contain a positive proportion of these primes. For such an X, $\delta(X) > 1/h$.

The sum $\sum'\delta(X)$, over all ideal classes X except the principal class X_0, is an important constituent of C_k, so it is worth saying something about its size. A lower bound is given by

$$\sum{}'\delta(X) \geqslant \sum{}'\delta_1(X) = 1-1/h.$$

Moreover if k is normal of prime degree q then every prime in k has degree either 1 or q, and the primes of degree q are principal. Consequently this lower bound is attained in this case. The normal fields of prime degree are almost certainly not the only fields for which the lower bound is attained. Suppose, for example, that k is normal with Galois group $\boldsymbol{Z}_{q^2}$, for some prime q, generated by τ. Suppose further that the class group H of k has odd order and that $\tau X = X^2$ for every X in H. (Since h is odd this does define an automorphism on H.) The condition norm $X = X_0$ becomes in this case

$$X^{1+2+4+\ldots+2^{q^2-1}} = X_0,$$

that is,

$$X^{2^{q^2}-1} = X_0,$$

and this will be satisfied for every X in H provided that H has exponent dividing $2^{q^2}-1$. Since k is normal, K is normal over $\boldsymbol{Q}$ with Galois group G, say. Suppose, finally, that $G = \boldsymbol{Z}_{q^2}\ltimes H$, the semidirect product of $\boldsymbol{Z}_{q^2}$ and H according to the action of $\boldsymbol{Z}_{q^2}$ on H just described. (This means that $G = \{(\tau^i, X)|\ i\in\boldsymbol{Z},\ X\in H\}$ with multiplication defined by $(\tau^i, X)\times$ $\times(\tau^j, Y) = (\tau^{i+j}, X^{2^j}Y)$.) The possible degrees of primes of k are 1, q and q^2, and primes of degree q^2 are necessarily principal. If $\mathfrak{p}$ is a prime of degree q and σ is the Frobenius automorphism of a prime in K dividing it, then $\sigma^q\in H$, and so $\sigma = (\tau^q, X)$ for some X in H. The class of $\mathfrak{p}$ is given by

$$\sigma^q = (1,\ X^{1+2^q+2^{2q}+\ldots+2^{(q-1)q}}),$$

so if H has exponent dividing $1+2^q+\ldots+2^{(q-1)q} = (2^{q^2}-1)/(2^q-1)$ then every prime of degree q is principal and $\delta(X) = \delta_1(X) = 1/h$ for all X other than X_0. There seems no reason why there should not be fields k fulfilling all these conditions. This example can be varied in several ways, the simplest of which is to take τX to be X^a for any fixed integer a (not necessarily 2).

To get an upper bound for $\sum' \delta(X)$ we first find an upper bound for the density of primes (counted with multiplicities) that are divisible by primes of k with degree greater than 1. Let $\bar{k}$ be the normal closure of k and put $n = [k:\boldsymbol{Q}]$ and $\bar{n} = [\bar{k}:\boldsymbol{Q}]$. Then no prime can have more than $[n/2]$ prime factors in k of degree greater than 1, and moreover the primes that belong to the identity element of $\mathrm{Gal}(\bar{k}/\boldsymbol{Q})$ have all their prime factors of degree 1. Since this set of primes has density $1/\bar{n}$ we have

$$\sum_{X\in H} \big(\delta(X)-\delta_1(X)\big) \leqslant \left(1-\frac{1}{\bar{n}}\right)\left[\frac{n}{2}\right].$$

Hence

$$\sum{}' \, \delta(X) \leqslant \left(1-\frac{1}{\bar{n}}\right)\left[\frac{n}{2}\right]+1-\frac{1}{h}. \tag{3}$$

This upper bound probably cannot be improved on. For example, to return to the situation in the diagram, there seems no reason why there should not be normal fields k with $G = \mathrm{Gal}(K/\boldsymbol{Q}) = \boldsymbol{Z}^r_{2^{s+1}}$, the direct product of r cyclic groups of order 2^{s+1} $(r, s \geqslant 1)$, and $H = \boldsymbol{Z}^r_{2^s}$, the direct product of the subgroups of index 2 in each factor of G. Then $\mathrm{Gal}(k/\boldsymbol{Q}) = G/H = \boldsymbol{Z}^r_2$, and since G is Abelian $\mathrm{Gal}(k/\boldsymbol{Q})$ acts trivially on H. Consequently the condition $\mathrm{norm}\, X = X_0$ reduces to $X^{2^r} = X_0$, and this is satisfied for all X in H provided that $r \geqslant s$. If σ is any element of G not in H then $\sigma^2 \in H$, $\sigma^2 \neq X_0$ and σ acts on the cosets of H as a product of 2^{r-1} 2-cycles (since σ has order 2 in G/H but fixes no coset). So primes p with $\left(\frac{K/\boldsymbol{Q}}{p}\right)$ not in H factorize into 2^{r-1} primes of k of degree 2 which are all non-principal, whereas primes p with $\left(\frac{K/\boldsymbol{Q}}{p}\right)$ in H factorize into 2^r primes of degree 1. Hence (3) holds with equality, where $n = \bar{n} = 2^r$ and $h = 2^{rs}$. When $s = 1$ here the $\delta(X)$'s with $X \neq X_0$ are all the same (equal to $1/2+1/h$), but when $s > 1$ they are not.

To sum up:

Lemma 2. *We have $\delta(X) \geqslant 1/h$ for all classes X, and if k is normal of prime degree (and most likely for some other fields k too) $\delta(X) = 1/h$ for all X except the principal class X_0. Also*

$$\sum_{X\neq X_0} \delta(X) \leqslant \left(1-\frac{1}{\bar{n}}\right)\left[\frac{n}{2}\right]+1-\frac{1}{h}.$$

3. The existence of C_k. It makes things simpler now if we regard the functions g and Ω_X as ranging over the integers of k (in the obvious way) instead of just the rational integers. We shall denote by $\boldsymbol{\Omega}(\mu)$ and δ the $(h-1)$-vectors whose components are $\Omega_X(\mu)$ and $\delta(X)$ for $X \neq X_0$ (where μ is any integer of k).

An obvious necessary and sufficient condition for an integer μ of k to be irreducible is that no proper subproduct of its expression as a product of prime ideals of k is principal. Accordingly we define an *irreducible type* (or a *type*, for short) of an Abelian group H to be a family of elements of H (that is, a set with repetitions allowed) whose product is the identity but which has no proper subproduct equal to the identity. [These types are what are called 'minimal complexes' in [9], and are virtually the same as the types of [11]. They are not quite the same as the types of [8], however, which carry more information about the power of each individual prime in a product.] A family of prime ideals of k has as its product a principal ideal generated by an irreducible integer of k if and only if the corresponding family of ideal classes is an irreducible type of the class group H. Consequently an integer μ of k is a product of $v(\mathscr{X})$ irreducibles from each irreducible type $\mathscr{X}$ if and only if

$$\sum_{\mathscr{X}} \Omega_X(\mathscr{X})\, v(\mathscr{X}) = \Omega_X(\mu)$$

for all X in H, and when these equations are satisfied the length of the corresponding irreducible factorization of μ is $\sum v(\mathscr{X})$. (Here $\Omega_X(\mathscr{X})$ denotes the number of X's in $\mathscr{X}$.) If $\mathscr{X}_0$ is the 'trivial' type $\langle X_0\rangle$ then the only equation containing $v(\mathscr{X}_0)$ is the one corresponding to X_0 and this is

$$v(\mathscr{X}_0) = \Omega_{X_0}(\mu).$$

Hence $g(\mu)$ is equal to the number of different values of $\sum' v(\mathscr{X})$ among the solutions in non-negative integers of the $h-1$ simultaneous equations

$$\sum{}' \, \Omega_X(\mathscr{X})\, v(\mathscr{X}) = \Omega_X(\mu) \qquad (X \neq X_0),$$

where all sums are over the set of all non-trivial types. These are equations in the $t-1$ variables $v(\mathscr{X})$ (where t is the total number of types of H), and as such they define an affine subspace $\mathscr{S}\big(\boldsymbol{\Omega}(\mu)\big)$ of $\boldsymbol{R}^{t-1}$, which is a translation of the subspace $\mathscr{S} = \mathscr{S}(\boldsymbol{0})$ defined by the associated homogeneous equations. The part of $\mathscr{S}\big(\boldsymbol{\Omega}(\mu)\big)$ in the positive quadrant is a bounded convex set (since the $\Omega_X(\mathscr{X})$'s are non-negative) and $g(\mu)$ is the number of different values of $\sum' v(\mathscr{X})$ at integer points in this part of $\mathscr{S}\big(\boldsymbol{\Omega}(\mu)\big)$. Clearly there *are* integer points on $\mathscr{S}\big(\boldsymbol{\Omega}(\mu)\big)$ (got by factorizing μ into irreducibles in any manner) and since the $\Omega_X(\mathscr{X})$'s are integers $\mathscr{S}$ has a basis consisting of rational vectors, so the integer points on $\mathscr{S}\big(\boldsymbol{\Omega}(\mu)\big)$ form a lattice of the full dimension of $\mathscr{S}$ and the lattices arising in this way from different μ's are congruent to each other. If we can find a family of classes that is both a union of two irreducible types and a union of three irreducible types, say, then it will follow that the minimum step length of the linear function $\sum' v(\mathscr{X})$ on this lattice is 1.

If there is a class X in H of order $e \geqslant 3$ then such a family is given by [1]

$$\prec X, X, X^{e-2} \succ \cup \prec X^{-1}, X^{-1}, X^2 \succ$$
$$= \prec X, X^{-1} \succ \cup \prec X, X^{-1} \succ \cup \prec X^2, X^{e-2} \succ$$

(where each uniand is a type). If, on the other hand, every class except X_0 has order 2, then there are distinct classes, X and Y, of order 2 (since $h \geqslant 3$) and such a family is given by

$$\prec X, Y, XY \succ \cup \prec X, Y, XY \succ = \prec X, X \succ \cup \prec Y, Y \succ \cup \prec XY, XY \succ.$$

Since $\sum' v(\mathscr{X})$ has step length 1 on $\mathscr{S}(\boldsymbol{\Omega}(\mu))$ the intersection $\mathscr{T} = \mathscr{T}(\boldsymbol{\Omega}(\mu), a)$ of the subspaces $\mathscr{S}(\boldsymbol{\Omega}(\mu))$ and $\sum' v(\mathscr{X}) = a$ contains an integer point whenever a is an integer, and since these subspaces are rational the integer points on $\mathscr{T}$ form a lattice of the full dimension of $\mathscr{T}$ (which is one less than the dimension of $\mathscr{S}$). The lattices corresponding to different values of a are congruent to each other, so there is a constant c_1, independent of a, such that every ball of radius c_1 in $\mathscr{T}$ contains an integer point.

Now suppose that $\boldsymbol{\Omega}(\mu)$ is proportional to $\boldsymbol{\delta}$, $\boldsymbol{\Omega}(\mu) = \Lambda\boldsymbol{\delta}$ say, and let $B = B_k$ and $b = b_k$ be the maximum and minimum values of $\sum' v(\mathscr{X})$ (the $v(\mathscr{X})$'s being real variables here) on the part of $\mathscr{S}(\boldsymbol{\delta})$ in the positive quadrant. Since this part of $\mathscr{S}(\boldsymbol{\delta})$ is convex, its intersection with the hyperplane $\sum' v(\mathscr{X}) = a/\Lambda$ contains a ball of radius $c_2 \min(B - a/\Lambda, a/\Lambda - b)$, for some constant c_2. When $\Lambda b + c_1/c_2 \leqslant a \leqslant \Lambda B - c_1/c_2$ this radius is at least c_1/Λ and hence $\mathscr{S}(\Lambda\boldsymbol{\delta})$ contains an integer point with $\sum' v(\mathscr{X}) = a$. Consequently

$$\Lambda(B-b) - 2c_1/c_2 \leqslant g(\mu) \leqslant \Lambda(B-b) + 1.$$

We shall show that $C_k = B_k - b_k$ is the constant we are looking for.

For a general rational integer m we put

$$\Lambda' = |G| \min_{X \neq X_0} [\Omega_X(m)/|G|\delta(X)],$$

where G is as in §2, so that $|G|$ is a common denominator for the $\delta(X)$'s. Then $\Lambda'\delta(X) \leqslant \Omega_X(m)$ for all $X \neq X_0$, and by multiplying together $\Lambda'\delta(X)$ of the prime ideal factors of m in the class X, for each X, we get an integer μ' of k dividing m with $\Omega_X(\mu') = \Lambda'\delta(X)$ for each X. (The ideal got in this way is principal because the equations $|G|\delta(X) = \sum \Omega_X(\mathscr{C})|\mathscr{C}|$ show that the class got by multiplying together $|G|\delta(X)$ copies of X, for each class X, is the same as the one got by multiplying together $|\mathscr{C}|$ rational primes belonging to each conjugacy class $\mathscr{C}$ of G.) If we take a fixed irreducible factorization of m/μ' of length l_1 then every factorization of μ' of length l gives rise to a factorization of m of length $l + l_1$, and hence $g(\mu') \leqslant g(m)$. In the same way, if we take Λ'' to be the least multiple of $|G|$ greater than $\max \Omega_X(m)/\delta(X)$ we can find an integer μ'' of k with $\Omega_X(\mu'') = \Lambda''\delta(X)$ for all $X \neq X_0$ and $g(\mu'') \geqslant g(m)$.

[1] We use $\prec\ \succ$ to indicate a family and $\{\ \}$ to indicate a set.

We now have

$$C \min_{X \neq X_0} \frac{\Omega_X(m)}{\delta(X)} + O(1) \leqslant g(m) \leqslant C \max_{X \neq X_0} \frac{\Omega_X(m)}{\delta(X)} + O(1). \tag{4}$$

Hence

$$(g(m) - C\log\log m)^2 = O\left(\left(\max_{X \neq X_0} \frac{\Omega_X(m)}{\delta(X)} - \log\log m\right)^2\right) +$$
$$+ O\left(\left(\min_{X \neq X_0} \frac{\Omega_X(m)}{\delta(X)} - \log\log m\right)^2\right) + O(1)$$
$$= O\left(\sum_{X \neq X_0} \left(\frac{\Omega_X(m)}{\delta(X)} - \log\log m\right)^2\right) + O(1).$$

Summing over m and using Lemma 1(iv) now gives

THEOREM 1. *For every algebraic number field k there is a constant C_k such that*

$$\sum_{m \leqslant x} (g(m) - C_k \log\log m)^2 = O(x \log\log x).$$

We have already seen that this implies that

$$\sum_{m \leqslant x} g(m) = C_k x \log\log x + O\big(x(\log\log x)^{1/2}\big).$$

When $h = 3$, however, the error term can be improved to $O(x)$. In this case there are only two non-principal classes, Y and Y^{-1} say, and $\Omega_Y(\mu) = \Omega_{Y^{-1}}(\mu)$ for every integer of k. So (4) becomes

$$g(m) = C_k \frac{\Omega_Y(m)}{\delta(Y)} + O(1),$$

and Lemma 1 (iii) gives

$$\sum_{m \leqslant x} g(m) = C_k x \log\log x + O(x).$$

(Narkiewicz [7] has this when $h = 3$ and k is quadratic.)

In [11] Narkiewicz and Śliwa define $g^+(m)$ and $g^-(m)$ to be the maximum and minimum lengths of factorizations of m into irreducibles of k, and they show that these functions have normal orders $C^+ \log\log m$

and $C^-\log\log m$, where C^+ and C^- are constants depending on k. The argument of this section can be applied to these functions too (more easily than to g, in fact) and gives $C^+ = B+\delta(X_0)$ and $C^- = b+\delta(X_0)$. Hence Theorem 2 in the next section evaluates C^+, for arbitrary k, as

$$\tfrac{1}{2}\sum_{X\in H}\delta(X)+\tfrac{1}{2}\delta(X_0).$$

Evaluating C^- (and hence C, which is C^+-C^-) is much harder.

4. Bounds for C_k. We defined C_k as B_k-b_k, where B_k and b_k are the maximum and minimum values of $\sum'v(\mathscr{X})$ among solutions of

$$\sum_{\mathscr{X}}{}' \Omega_X(\mathscr{X})v(\mathscr{X}) = \delta(X) \qquad (X\neq X_0) \tag{5}$$

in non-negative real variables. Adding these equations gives

$$\sum_{\mathscr{X}}{}'\sum_{X}{}' \Omega_X(\mathscr{X})v(\mathscr{X}) = \sum_{X}{}'\delta(X).$$

Since each non-trivial type contains at least two classes,

$$\sum_{X}{}'\Omega_X(\mathscr{X})\geqslant 2$$

for all non-trivial $\mathscr{X}$, and so

$$\sum_{\mathscr{X}}{}' v(\mathscr{X})\leqslant \tfrac{1}{2}\sum_{X}{}'\delta(X).$$

Hence

$$B\leqslant \tfrac{1}{2}\sum{}'\delta(X).$$

In fact $B=\frac{1}{2}\sum'\delta(X)$, as can be seen by taking

$$v(\mathscr{X}) = \begin{cases}\delta(X) & \text{if } \mathscr{X} = \prec X, X^{-1}\succ \text{ for some } X \text{ with } X^2\neq X_0,\\ \tfrac{1}{2}\delta(X) & \text{if } \mathscr{X} = \prec X, X\succ \text{ for some } X \text{ with } X^2 = X_0,\\ 0 & \text{otherwise.}\end{cases}$$

(Since $\delta(X) = \delta(X^{-1})$ there is no ambiguity in this definition.) Then

$$\sum_{\mathscr{X}}{}'\Omega_X(\mathscr{X})v(\mathscr{X}) = \delta(X)$$

for all $X\neq X_0$, and $\sum'v(\mathscr{X}) = \frac{1}{2}\sum'\delta(X)$.

Another way of seeing this (which is useful in finding b for certain fields too) is to add the equations corresponding to X and X^{-1}. Writing I for the inverse pair $\{X, X^{-1}\}$ (so that $I=\{X\}$ is a singleton when $X^2=X_0$) and putting

$$\delta(I) = \sum_{X\in I}\delta(X) = \begin{cases}\delta(X)+\delta(X^{-1}) = 2\delta(X) & \text{if } |I| = 2,\\ \delta(X) & \text{if } |I| = 1,\end{cases}$$

we get

$$\sum_{\mathscr{X}}{}'\sum_{X\in I}\Omega_X(\mathscr{X})v(\mathscr{X}) = \delta(I) \tag{6}$$

for every inverse pair I except the 'identity pair' $I_0 = \{X_0\}$. Each type $\mathscr{X} = \prec X_1, X_2, \ldots, X_j\succ$ has an inverse type $\mathscr{X}^{-1} = \prec X_1^{-1}, X_2^{-1}, \ldots, X_j^{-1}\succ$, and clearly $\Omega_X(\mathscr{X}) = \Omega_{X^{-1}}(\mathscr{X}^{-1})$. If we write $\mathscr{I} = \{\mathscr{X}, \mathscr{X}^{-1}\}$ for an inverse pair of types and define

$$\Omega_I(\mathscr{I}) = \sum_{X\in I}\Omega_X(\mathscr{X}) = \sum_{X\in I}\Omega_X(\mathscr{X}^{-1})$$

(the number of classes in $\mathscr{X}$ belonging to the pair I) (6) becomes

$$\sum_{\mathscr{I}}{}' \Omega_I(\mathscr{I})w(\mathscr{I}) = \delta(I), \tag{7}$$

where the sum is over all inverse pairs of non-trivial types and $w(\mathscr{I}) = \sum_{\mathscr{X}\in\mathscr{I}}v(\mathscr{X})$. Clearly any solution of (5) gives a solution of (7) with $\sum'w(\mathscr{I}) = \sum'v(\mathscr{X})$ and conversely, since $\delta(X^{-1}) = \delta(X)$ and $\Omega_{X^{-1}}(\mathscr{X}^{-1}) = \Omega_X(\mathscr{X})$, any solution of (7) gives a solution of (5) by taking

$$v(\mathscr{X}) = \begin{cases}\tfrac{1}{2}w(\mathscr{I}) & \text{if } |\mathscr{I}| = 2,\\ w(\mathscr{I}) & \text{if } |\mathscr{I}| = 1,\end{cases}$$

and $\sum'w(\mathscr{I}) = \sum'v(\mathscr{X})$. Consequently B and b are the maximum and minimum values of $\sum'w(\mathscr{I})$ among solutions of (7) in non-negative real variables. The value of B follows immediately, since $\sum_{I}'\Omega_I(\mathscr{I})\geqslant 2$ for all non-trivial $\mathscr{I}$ but for each $I = \{X, X^{-1}\}$ the variable $w(\{\prec X, X^{-1}\succ\})$ has coefficient 2 in the equation corresponding to I and coefficient 0 in all the other equations. So

$$B = \tfrac{1}{2}\sum{}'\delta(I) = \tfrac{1}{2}\sum{}'\delta(X).$$

We now look at b. If X is an element of H of order $e = e(X)$ then $\mathscr{X}_X = \prec X(e\,\text{times})\succ$ is an irreducible type with $\Omega_X(\mathscr{X}_X) = e(X)$ and $\Omega_Y(\mathscr{X}_X) = 0$ if $Y\neq X$. So choosing $v(\mathscr{X}_X) = \delta(X)/e(X)$ and $v(\mathscr{X}) = 0$ if $\mathscr{X}$ is not one of the $\mathscr{X}_X$'s gives a solution of (5) with $\sum'v(\mathscr{X}) = \sum'\delta(X)/e(X)$. Hence

$$b\leqslant \sum{}'\delta(X)/e(X).$$

This upper bound is attained when H is a cyclic p-group, as it then coincides with the lower bound (9) to be proved later. It is not attained when H is a homocyclic (but not cyclic) p-group and k is normal of prime degree, as then (9) is attained (by Theorem 5) and is different from it.

A lower bound for b can be got by the same kind of argument that gave an upper bound for B. The *Davenport number* $D = D(H)$ of an Abelian group H is the smallest integer such that every family $\mathscr{F}$ of D elements of H (counted with multiplicities) has a non-empty subfamily (possibly $\mathscr{F}$ itself) whose product is the identity. Equivalently, $D(H)$ is the length of the longest irreducible type of H: omitting one element from an irreducible type gives a family having no subfamily with product the identity, and conversely a family having no subfamily with product the identity can be enlarged to give an irreducible type. Hence

$$\sum_{X} \Omega_X(\mathscr{X}) \leqslant D = D(H),$$

the Davenport number of the class group, for all types $\mathscr{X}$, and adding the equations (5) leads to

$$b \geqslant {\sum}' \delta(X)/D.$$

Theorems 3 and 5 will show that this lower bound is attained when H is cyclic of prime order and when H is an elementary p-group and k is normal of prime degree. It is not attained when H is a non-elementary p-group, since then (9) is stronger.

J. E. Olson [13] has shown that if H is a p-group and $H = \times \boldsymbol{Z}^{(i)}$ is the (essentially unique) decomposition of H into a direct product of cyclic groups then

$$D(H) = \sum (|\boldsymbol{Z}^{(i)}|-1)+1.$$

(It has since been shown that $D(H)$ may be larger than this when H is not a p-group, and is larger when $H = \boldsymbol{Z}_2^4 \times \boldsymbol{Z}_6$.) By using a sharper form of this result (also due to Olson) we can get the improved lower bound (9) for b when H is a p-group.

LEMMA 3. *If H is a p-group, $\mathscr{X}$ is a non-trivial irreducible type of H and $\nu = \nu(X) = p^{a(X)}$ (for any element $X \neq X_0$ of H) is the largest power of p for which X is the ν-th power of an element of H, then*

$$(8) \qquad {\sum}' \nu(X)\,\Omega_X(\mathscr{X}) \leqslant D(H).$$

Proof. Theorem 2 of [13] says that if $\mathscr{F}$ is a family of elements of H such that $\sum_{X\in\mathscr{F}} \nu(X) \geqslant D(H)$ then $\prod_{X\in\mathscr{F}} (X_0 - X) \equiv 0 \pmod{p}$ (where the product is in the group ring $\boldsymbol{Z}[H]$). Considering the coefficient of X_0 then shows (as in the remark following the statement of Theorem 1 of [13]) that at least one non-empty subfamily of $\mathscr{F}$ has product X_0. Let $\mathscr{X}$ be a non-trivial irreducible type of H. If $\nu(Y) = 1$ for some Y in $\mathscr{X}$ then

$${\sum}' \nu(X)\,\Omega_X(\mathscr{X}) = \sum_{X\in\mathscr{X}} \nu(X) = 1 + \sum_{X\in\mathscr{X}\setminus(Y)} \nu(X).$$

But $\mathscr{X}\setminus\{Y\}$ is a family of elements such that no non-empty subfamily has product X_0, and so the sum on the right is less than $D(H)$. Hence ${\sum}' \nu(X)\,\Omega_X(\mathscr{X}) \leqslant D(H)$. If, on the other hand, $\nu(X) > 1$ for all X in $\mathscr{X}$ we work in the subgroup H^ν of νth powers in H, where ν is the smallest value of $\nu(X)$ for X in $\mathscr{X}$. Every X in $\mathscr{X}$ is in H^ν, and $\nu'(X) = \nu(X)/\nu$ for X in H^ν, where ν' is defined on H^ν in the same way as ν is on H. Also if $H = \times \boldsymbol{Z}^{(i)}$, where the $\boldsymbol{Z}^{(i)}$'s are cyclic, then $|\boldsymbol{Z}^{(i)}| > \nu$ for at least one i (since $\mathscr{X} \neq \{X_0\}$). So

$$D(H^\nu) = \sum_{|\boldsymbol{Z}^{(i)}|>\nu} \left(\frac{|\boldsymbol{Z}^{(i)}|}{\nu} - 1\right) + 1 \leqslant \frac{1}{\nu}\left(\sum (|\boldsymbol{Z}^{(i)}|-1)+1\right) = \frac{1}{\nu} D(H).$$

Hence

$${\sum}' \nu(X)\,\Omega_X(\mathscr{X}) = \nu {\sum}' \nu'(X)\,\Omega_X(\mathscr{X}) \leqslant \nu D(H^\nu) \leqslant D(H).$$

We can think of no plausible generalization of this inequality to groups that are not p-groups.

To deduce a lower bound for b when H is a p-group we multiply (5) by $\nu(X)$ and sum over X to get

$$\sum_{\mathscr{X}}{}' \Big(\sum_{X}{}' \nu(X)\,\Omega_X(\mathscr{X}) \Big) v(\mathscr{X}) = \sum_{X}{}' \nu(X)\,\delta(X),$$

and now Lemma 3 shows that

$$(9) \qquad b \geqslant \frac{1}{D} {\sum}' \nu(X)\,\delta(X),$$

with equality if and only if (5) is soluble with $v(\mathscr{X}) = 0$ for all types $\mathscr{X}$ that do not give equality in (8). This is bigger than our previous lower bound when H is non-cyclic, and in Theorem 5 we shall show that it is attained whenever H is homocyclic and k is normal of prime degree.

Collecting these results:

THEOREM 2. (i) *For any algebraic number field k with class group H*

$$B_k = \tfrac{1}{2} {\sum}' \delta(X)$$

and

$$\frac{1}{D(H)} {\sum}' \delta(X) \leqslant b_k \leqslant {\sum}' \delta(X)/e(X).$$

Hence

$${\sum}' \left(\frac{1}{2} - \frac{1}{e(X)}\right)\delta(X) \leqslant C_k \leqslant \left(\frac{1}{2} - \frac{1}{D(H)}\right) {\sum}' \delta(X).$$

(ii) *If h is a power of a prime p then*

$$b_k \geqslant \frac{1}{D(H)} \sum{}' \nu(X)\,\delta(X)$$

and hence

$$C_k \leqslant \sum{}' \left(\frac{1}{2} - \frac{\nu(X)}{D(H)}\right)\delta(X).$$

Combining (i) with Lemma 2 gives

$$\frac{1}{2} - \frac{1}{2h} - \frac{1}{h}\sum{}' \frac{1}{e(X)} \leqslant C_k \leqslant \left(\frac{1}{2} - \frac{1}{D}\right)\left\{\left(1 - \frac{1}{n}\right)\left[\frac{n}{2}\right] + 1 - \frac{1}{h}\right\}.$$

The lower bound here is attained when H is a cyclic p-group and k is normal of prime degree q, say, (where p and q may or may not be equal). The upper bound seems unlikely to be attained exactly since the only obvious case of equality for the upper bound in (i) is when H is cyclic of prime order, whereas our example of equality for the upper bound in Lemma 2 had H a direct product of at least two factors. However, for that example we do have $\delta(X) = 2^{-rs}(2^{r-1}+1)$ for all X of exponent 2^s in H, so that

$$C_k \geqslant \sum{}' \left(\frac{1}{2} - \frac{1}{e(X)}\right)\delta(X) \geqslant \left(\frac{1}{2} - \frac{1}{2^s}\right)2^{-rs}(2^{r-1}+1)(2^{rs} - 2^{r(s-1)})$$
$$= \left(\frac{1}{4} - \frac{1}{2^{s+1}}\right)(n+2)\left(1 - \frac{1}{n}\right).$$

Thus there are almost certainly fields k of large degree for which C_k is very close to its upper bound, and, in particular, for which $C_k > \frac{1}{4}n - 1$.

From this lower bound we can derive an absolute lower bound for C_k. If we write the lower bound as

$$L(H) = \frac{1}{|H|}\sum_{X}{}' \left(\frac{1}{2} - \frac{1}{e(X)}\right),$$

then $L(H)$ is an increasing function of H in the sense that if $H_2 = H/H_1$ is a quotient of H then $L(H_2) \leqslant L(H)$. In fact $e(X) \geqslant e_1(X)$, for X in H, where $e_1(X)$ is the order of X in H/H_1, so on letting Y run through H_1 and Z through a set of coset representatives of H_1 in H we have

$$L(H) = \frac{1}{|H|}\sum_{Y}\sum_{Z}{}' \left(\frac{1}{2} - \frac{1}{e(YZ)}\right) + \frac{1}{|H|}\sum_{Y}{}' \left(\frac{1}{2} - \frac{1}{e(Y)}\right)$$
$$\geqslant \frac{|H_1|}{|H_1|\,|H_2|}\sum_{Z}{}' \left(\frac{1}{2} - \frac{1}{e_1(Z)}\right) + \frac{1}{|H_1|\,|H_2|}\sum_{Y}{}' \left(\frac{1}{2} - \frac{1}{e(Y)}\right)$$
$$= L(H_2) + \frac{1}{|H_2|}L(H_1) \geqslant L(H_2).$$

There is equality here only when $L(H_1) = 0$ and $e(X) = e_1(X)$ for all X not in H_1, and this can happen only when $H_1 = \{X_0\}$ (the trivial subgroup of H) or when H is a 2-group and H_1 is an elementary 2-group. Since there is a subgroup H_2' of H isomorphic to H_2 with H/H_2' isomorphic to H_1, we also have

$$L(H) \geqslant L(H_1) + \frac{1}{|H_1|}L(H_2).$$

If H is not a 2-group then it has a subgroup $\boldsymbol{Z}_p$ for some odd prime p, and so

$$L(H) \geqslant L(\boldsymbol{Z}_p) = \frac{1}{2}\left(1 - \frac{1}{p}\right)\left(1 - \frac{2}{p}\right) \geqslant \frac{1}{9}.$$

If H is a non-elementary 2-group then it has a subgroup $\boldsymbol{Z}_4$, and $L(H) \geqslant L(\boldsymbol{Z}_4) = 1/8$. If H is an elementary 2-group then $L(H) = 0$, but Theorem 5 will show that

$$C_k \geqslant \left(\frac{1}{2} - \frac{1}{r+1}\right)\left(1 - \frac{1}{2^r}\right)$$

when $H = \boldsymbol{Z}_2^r$, and since $r \geqslant 2$ (because $h \geqslant 3$) the right hand side here is $\geqslant 1/8$. Hence $C_k \geqslant 1/9$ for all k, and equality is possible only when $h = 3$.

5. C_k when H is a cyclic p-group.

THEOREM 3. *If H is cyclic of prime power order p^s and is generated by Y then*

$$C_k = \sum_{i=1}^{s}\left(\frac{1}{2} - \frac{1}{p^i}\right)\sum_{j(\operatorname{mod} p^i)}{}^{\!*}\, \delta(Y^{jp^{s-i}}),$$

where the inner sum is over a reduced set of residues mod p^i.

Proof. When H is cyclic of order p^s we have $D(H) = p^s$ and $\nu(X) = p^s/e(X)$ for all X in H, and so the lower bound for C_k in (i) of Theorem 2 is the same as the upper bound in (ii). The value of C_k stated in the theorem can then be got by collecting together terms corresponding to X's of the same order in the sum representing the common value of these two bounds. (The fact that $\delta(Y^{(p^i-j)p^{s-i}}) = \delta(Y^{jp^{s-i}})$ means that the inner sum is really only half as long as it looks.)

6. The number $C(H)$ and its evaluation for homocyclic p-groups.

THEOREM 4. *For every Abelian group H there is a number $C(H)$ such that $C(H) \leqslant C_k$ for every field k with class group H and $C(H) = C_k$ whenever k is normal of prime degree.*

Proof. By Lemma 2, $\delta(X) = 1/h$ for all $X \neq X_0$ when k is normal of prime degree, so we define $C(H)$ to be $B(H)-b(H)$, where $B(H)$ and $b(H)$ are the maximum and minimum values of $\sum' v(\mathscr{X})$ among solutions of

$$\sum_{\mathscr{X}}{}' \Omega_X(\mathscr{X}) v(\mathscr{X}) = 1/h \quad (X \neq X_0) \tag{10}$$

in non-negative real variables.

Also by Lemma 2, for general k $\delta(X) \geqslant 1/h$ for all X. Take any fixed solution in non-negative real numbers of

$$\sum_{\mathscr{X}}{}' \Omega_X(\mathscr{X}) v(\mathscr{X}) = \delta(X) - 1/h.$$

(For example, $v(\mathscr{X}_X) = \big(\delta(X)-1/h\big)/e(X)$ and $v(\mathscr{X}) = 0$ if $\mathscr{X}$ is not an $\mathscr{X}_X$ would do.) Then adding this solution to each of two non-negative solutions of (10) with their values of $\sum' v(\mathscr{X})$ differing by $C(H)$ gives two non-negative solutions of (5) with their values of $\sum' v(\mathscr{X})$ differing by $C(H)$. Hence $C_k \geqslant C(H)$.

We saw in §2 that it is likely that there are fields k with

$$\delta(X) = 1/h \quad \text{whenever } X \neq X_0 \tag{11}$$

that are not cyclic of prime degree, and $C_k = C(H)$ for these fields too. It is also possible that $C_k = C(H)$ for some fields k that do not satisfy (11). For example, suppose that k is a normal quartic field with class group $\boldsymbol{Z}_4$ generated by Y and that the group G of § 2 is the direct product of the class group with $\mathrm{Gal}(k/\boldsymbol{Q})$. Then $\tau Y = Y$ for every τ in $\mathrm{Gal}(k/\boldsymbol{Q})$ and norm $X = X^4 = X_0$ for every class X. It is easy to check that every prime in Y or Y^3 has degree 1 and that $\delta(Y) = \delta(Y^3) = 1/4$ but $\delta(Y^2) = 1/2$ if $\mathrm{Gal}(k/\boldsymbol{Q}) = \boldsymbol{Z}_4$ and $\delta(Y^2) = 1$ if $\mathrm{Gal}(k/\boldsymbol{Q}) = \boldsymbol{Z}_2^2$. However, $\delta(Y^2)$ has coefficient zero in the expression for C_k given by Theorem 3, and so $C_k = C(H) = 1/8$. This example asks rather a lot of the field k, though, and we do not know whether there are any such fields.

We now evaluate $C(H)$ when H is a homocyclic p-group. (A group is *homocyclic* if it is a direct product of cyclic groups of the same order.)

By an *automorphism class* A of H (an arbitrary Abelian group for the moment) we shall mean an orbit of H under the action of its group of automorphisms. So X and Y are in the same automorphism class if and only if $Y = aX$ for some automorphism a of H. If $\mathscr{X} = \prec X_1, X_2, \ldots$ $\ldots, X_l \succ$ is an irreducible type and a is an automorphism of H we write

$$a\mathscr{X} = \prec aX_1, aX_2, \ldots, aX_l \succ.$$

This gives an action of the group of automorphisms of H on the set of types, and consequently the types too fall into automorphism classes $\mathscr{A}$. We shall say that two objects (group elements or types) are *automorphic* to each other if they belong to the same automorphism class. For any automorphism a we have $\Omega_{aX}(a\mathscr{X}) = \Omega_X(\mathscr{X})$, and consequently, for each class X,

$$\sum_{\mathscr{X}\in\mathscr{A}} \Omega_X(\mathscr{X}) = \sum_{\mathscr{X}\in\mathscr{A}} \Omega_{aX}(\mathscr{X}). \tag{12}$$

If A is an automorphism class of H and $\mathscr{A}$ is the automorphism class of types automorphic to a given type $\mathscr{X}$ we define

$$\Omega_A(\mathscr{A}) = \sum_{X\in A} \Omega_X(\mathscr{X}).$$

Then $\Omega_A(\mathscr{A})$ is the number of elements of the automorphism class A in $\mathscr{X}$ (with multiplicities) and is clearly independent of which $\mathscr{X}$ in $\mathscr{A}$ is chosen. Also we have

$$\Omega_A(\mathscr{A}) = \frac{1}{|\mathscr{A}|} \sum_{X\in A} \sum_{\mathscr{X}\in\mathscr{A}} \Omega_X(\mathscr{X}) = \frac{|A|}{|\mathscr{A}|} \sum_{\mathscr{X}\in\mathscr{A}} \Omega_X(\mathscr{X}), \tag{13}$$

by (12), where X is any element of A. Adding together the equations in (5) corresponding to X's in the same automorphism class now gives

$$\sum_{\mathscr{A}}{}' \Omega_A(\mathscr{A}) w(\mathscr{A}) = \delta(A) \tag{14}$$

for each automorphism class A except the 'identity' $A_0 = \{X_0\}$, where

$$\delta(A) = \sum_{X\in A} \delta(X), \quad w(\mathscr{A}) = \sum_{\mathscr{X}\in\mathscr{A}} v(\mathscr{X})$$

and the sum is over all automorphism classes of types except $\prec\mathscr{X}_0\succ$. Thus each non-negative solution of (5) gives rise to a non-negative solution of (14) with $\sum' w(\mathscr{A}) = \sum' v(\mathscr{X})$. Conversely, if $\delta(X) = \delta(Y)$ whenever X and Y are automorphic, then, in view of (13), every non-negative solution of (14) gives rise to a non-negative solution of (5) by taking $v(\mathscr{X}) = w(\mathscr{A})/|\mathscr{A}|$ for $\mathscr{X}$ in $\mathscr{A}$, and $\sum' v(\mathscr{X}) = \sum' w(\mathscr{A})$. If, in addition, H is a p-group, then

$$b \geqslant \frac{1}{D} \sum{}' \nu(A)\,\delta(A), \tag{15}$$

by (9), where $\nu(A)$ is the common value of $\nu(X)$ for X in A, and there is equality here if we can find a set of $\mathscr{A}$'s such that each $\boldsymbol{\Omega}(\mathscr{A})$ (the vector with components $\Omega_A(\mathscr{A})$) lies on the hyperplane

$$\sum{}' \nu(A)\,\Omega_A(\mathscr{A}) = D \tag{16}$$

and Δ (the vector with components $\delta(A)$) is a linear combination of these $\boldsymbol{\Omega}(\mathscr{A})$'s with non-negative coefficients. This reduces the original $(h-1)$-dimensional problem to one of lower dimension.

From now on we take H to be the homocyclic p-group $\boldsymbol{Z}_{p^s}^r$ with generators $X_1, \ldots, X_r$ each of order p^s. Then the automorphism classes are precisely the classes of elements of equal order. Indeed if X has order p^s then $X = \prod X_i^{a_i}$, where a_j, say, is not divisible by p, and $aX_j = X$, $aX_i = X_i$ $(i \neq j)$ defines an automorphism a of H that takes X_j to X. Clearly the generators X_i are all automorphic, any permutation of them defining an automorphism. If X has order p^t $(t < s)$ then X is the p^{s-t}th power of some element of order p^s and so is automorphic to $X_1^{p^{s-t}}$. (The property that elements of the same order are automorphic is true of homocyclic groups generally, in fact, since every homocyclic group is the direct product of one homocyclic p-group for each p dividing its order. Conversely, it is clear that every finite Abelian group with this property is a direct product of homocyclic p-groups for distinct primes p — but such a group need not be homocyclic.)

Now assume that the $\delta(X)$'s with $X \neq X_0$ are all equal, with common value δ, say. The number of elements of order p^{s-t} in H is $(p^{s-t})^r-(p^{s-t-1})^r$ $= p^{r(s-t)}(1-p^{-r})$, so $\Delta = (|A|)\,\delta$ is proportional to $(p^r, p^{2r}, \ldots, p^{rs})$, where we have arranged the automorphism classes in order of increasing order. For each t with $0 \leqslant t \leqslant s-1$

$$\prec \underset{p^{s-t}-1}{X_1^{p^t}}, \ldots, \underset{p^{s-t}-1}{X_r^{p^t}}, \underset{p-1}{X_1^{p^{t-1}}}, \ldots, \underset{p-1}{X_r^{p^{t-1}}}, \ldots, \underset{p-1}{X_1}, \ldots, \underset{p-1}{X_r}, X_1 \ldots X_r \succ,$$

is clearly an irreducible type, where the numbers underneath are multiplicities. (To get the exponent of one X_i up to p^s the last element must be used, and consequently the exponents of all the X_i's will have to be p^s, which can only be done by using every term.) The vector $\boldsymbol{\Omega}(\mathscr{A})$ corresponding to this type is

$$\big(\underbrace{0, \ldots, 0}_{s-t-1 \text{ times}}, r(p^{s-t}-1), \underbrace{r(p-1), \ldots, r(p-1)}_{t-1 \text{ times}}, r(p-1)+1\big)$$

if $t \neq 0$ and $\big(0, \ldots, 0, r(p^s-1)+1\big)$ if $t = 0$, and these vectors satisfy (16) since $D(H) = r(p^s-1)+1$. Since this set of vectors (for $t = s-1, \ldots, 0$) is in echelon form and for each of them the ratio of consecutive non-zero terms is $\geqslant p^{-r}$ (in fact all but the last of these ratios is $\geqslant 1$, and the last is $\geqslant 1/2$) the vector $(p^r, p^{2r}, \ldots, p^{sr})$ can be expressed as a linear combination of them with non-negative coefficients. Hence

$$b = \frac{1}{D}\sum{}' \nu(A)\,\delta(A) = \frac{1}{r(p^s-1)+1}\sum_{t=0}^{s-1} p^t\,\delta p^{r(s-t)}\Big(1-\frac{1}{p^r}\Big)$$
$$= \frac{\delta p^{rs}(1-p^{-r})(1-p^{-(r-1)s})}{\big(r(p^s-1)+1\big)(1-p^{-(r-1)})}$$

(where $(1-p^{-(r-1)s})/(1-p^{-(r-1)})$ is to be interpreted as s when $r = 1$). When $\delta = 1/h$ $(= p^{-rs})$ this gives

THEOREM 5.

$$C(\boldsymbol{Z}_{p^s}^r) = \frac{1}{2} - \frac{1}{2p^{rs}} - \frac{(1-p^{-r})(1-p^{-(r-1)s})}{\big(r(p^s-1)+1\big)(1-p^{-(r-1)})},$$

with the gloss just described.

Having all the $\delta(X)$'s equal for $X \neq X_0$ is not a vital part of the proof that $b = \sum' \nu(X)\,\delta(X)$. Thinking of our vectors as homogeneous coordinates of points in $(h-2)$-dimensional space, all that is needed is that δ is in the convex hull of those $\boldsymbol{\Omega}(\mathscr{X})$'s that give equality in (8). A small change in the $\delta(X)$'s does not affect this, and there is plenty of leeway when H is homocyclic. For a general p-group $b = \sum' \nu(X)\,\delta(X)$ if and only if the types $\mathscr{X}$ that give equality in (8) are widely enough spread for the corresponding points $\boldsymbol{\Omega}(\mathscr{X})$ to have δ in their convex hull. We shall see in the next section that for the smallest non-homocyclic group, $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$, these $\boldsymbol{\Omega}(\mathscr{X})$'s all lie in a proper subspace and $b < \sum' \nu(X)\,\delta(X)$ when the $\delta(X)$'s with non-principal X are all equal. When H is not a p-group we do not even have a target to aim at. What is needed is a vector $\boldsymbol{\nu}$ such that $\boldsymbol{\nu} \cdot \boldsymbol{\Omega}(\mathscr{X})$ attains its maximum value for a wide variety of types $\mathscr{X}$.

We end this section by proving

THEOREM 6. *$C(H) \to \frac{1}{2}$ as $h \to \infty$.*

Proof. Every large finite Abelian group has a large homocyclic p-subgroup, for some p, so this theorem would follow from the previous one if we could show that $C(H)$ was an increasing function of H. We have not been able to do this. We do know that the lower bound $L(H)$ for $C(H)$ is an increasing function of H, but $L(H)$ does not tend to $1/2$ as h tends to infinity ($L(H) < 1/2 - 1/p$ for every elementary p-group, for example). Taking an intermediate course, we shall define an auxiliary function $C_2(H)$ that is a lower bound for $C(H)$, that is close to $C(H)$ when H is a homocyclic p-group and that is an increasing function of H in the sense (weaker than before) that $C_2(H_1) \leqslant C_2(H_1 \times H_2)$. This function is defined in the same way as $C(H)$ except that only types of even length are used. So $C_2(H)$ is the difference between the maximum and minimum values of $\sum' v(\mathscr{X})$ ($B_2(H)$ and $b_2(H)$, say) among solutions of (10) in non-negative real variables $v(\mathscr{X})$ with $v(\mathscr{X}) = 0$ for all types $\mathscr{X}$ of odd length. Clearly $C_2(H) \leqslant C(H)$ for every H. Also $B_2(H) = B(H)$, since types $\prec X, X^{-1} \succ$ only, of length 2, were used to achieve $\sum' v(\mathscr{X})$ $= \frac{1}{2}\sum' \delta(X) = B$ at the beginning of §4. (This also shows that $C_2(H)$ exists for non-trivial H.) For homocyclic p-groups the proof of Theorem 5 can be modified to show that $C_2(H) \geqslant C(H) - \big(D(H)\big)^{-1}$. The types of odd length that are used in the proof can be made one element shorter by replacing the last two elements by their product. The new types are still irreducible and the corresponding vectors $\Omega(\mathscr{A})$ are still in echelon form and have the ratio of consecutive non-zero terms $\geqslant p^{-r}$. (The only one of these ratios that can decrease is the next to last when H is a cyclic 2-group, and it then becomes $1/2$.) For the altered types we have

$$\sum{}' \nu(X)\,\Omega_X(\mathscr{X}) \geqslant D(H)-1, \tag{17}$$

and so the proof of Theorem 5 shows that (10) can be satisfied with $v(\mathscr{X}) \neq 0$ only for types $\mathscr{X}$ of even length that satisfy (17). Multiplying (10) by $\nu(X)$ and summing over X (as in the proof of Theorem 2 (ii)) now shows that

$$\big(D(H)-1\big)\, b_2(H) \leqslant \sum{}' \nu(X)/h = D(H)\,b(H).$$

Hence

$$C_2(H) \geqslant B(H) - \frac{D(H)}{D(H)-1}\, b(H) = C(H) - \frac{1}{D(H)-1}\, b(H) \geqslant C(H) - \frac{1}{D(H)},$$

since $b(H) \leqslant 1/2$ and $D(H) \geqslant 2$ for non-trivial H.

We now show that $C_2(H_1) \leqslant C_2(H_1\times H_2)$ for any finite Abelian groups H_1 and H_2. To avoid the argument's splitting into several cases it is convenient to consider the subgroup of the automorphism group of $H_1\times H_2$ generated by the inversion automorphisms on the individual factors H_1 and H_2. We shall call the orbits of $H_1\times H_2$ and its set of types under the action of this subgroup *automorphism classes* (each one has at most four elements). These restricted automorphism classes can be used to reduce the number of variables and equations in (5) in the same way that the full automorphism classes can. There is a one-one correspondence between automorphism classes of elements of $H_1\times H_2$ and pairs $\{I^{(1)}, I^{(2)}\}$ of inverse pairs of elements of H_1 and H_2 given by

$$\{I^{(1)}, I^{(2)}\} = \big\{\{Y, Y^{-1}\}, \{Z, Z^{-1}\}\big\} \leftrightarrow I^{(1)}I^{(2)} = \{YZ, YZ^{-1}, Y^{-1}Z, Y^{-1}Z^{-1}\},$$

and

$$|I^{(1)}I^{(2)}| = |I^{(1)}|\,|I^{(2)}|.$$

Let $\mathscr{I}^{(1)}$ be any inverse pair of types of even length of H_1 and $I^{(2)} = \{Z, Z^{-1}\}$ any inverse pair of elements of H_2. If $\prec Y_1, \ldots, Y_{2\lambda} \succ$ is one of the types in $\mathscr{I}^{(1)}$ (with its elements arranged in some arbitrarily determined order) then $\prec Y_1Z, \ldots, Y_\lambda Z, Y_{\lambda+1}Z^{-1}, \ldots, Y_{2\lambda}Z^{-1} \succ$ is an irreducible type of $H_1\times H_2$ belonging to an automorphism class $\mathscr{A}$, say, and $\Omega_A(\mathscr{A})$ is $\Omega_{I^{(1)}}(\mathscr{I}^{(1)})$ if $A = I^{(1)}I^{(2)}$ for some inverse pair $I^{(1)}$ of H_1 and is zero otherwise. Hence any solution of

$$\sum_{\mathscr{I}^{(1)}}{}' w_1(\mathscr{I}^{(1)})\,\Omega_{I^{(1)}}(\mathscr{I}^{(1)}) = |I^{(1)}|/|H_1| \qquad (I^{(1)} \neq I_0^{(1)}),$$

using types of even length only, gives rise to a solution of

$$\sum_{\mathscr{A}}{}' w(\mathscr{A})\,\Omega_A(\mathscr{A}) = \begin{cases} |A|/|H_1\times H_2| & \text{if } A = I^{(1)}I^{(2)} \text{ with } I^{(1)} \neq I_0^{(1)}, \\ 0 & \text{if } A = I_0^{(1)}I^{(2)}, \end{cases} \tag{18}$$

by taking

$$w(\mathscr{A}) = \frac{|A|\,|H_1|}{|I^{(1)}|\,|H_1\times H_2|}\, w_1(\mathscr{I}^{(1)}) = \frac{|I^{(2)}|}{|H_2|}\, w_1(\mathscr{I}^{(1)}),$$

where $\mathscr{A}$ is obtained from $\mathscr{I}^{(1)}$ and $I^{(2)}$ as above (and all other variables zero). Also, since H_2 is a subgroup of $H_1\times H_2$, every irreducible type $\mathscr{I}^{(2)}$ of H_2 is an irreducible type of $H_1\times H_2$, and $\Omega_A(\mathscr{I}^{(2)})$ is $\Omega_{I^{(2)}}(\mathscr{I}^{(2)})$ if $A = I_0^{(1)}I^{(2)}$ $(= I^{(2)})$ and is zero otherwise. Hence any solution of

$$\sum_{\mathscr{I}^{(2)}}{}' w_2(\mathscr{I}^{(2)})\,\Omega_{I^{(2)}}(\mathscr{I}^{(2)}) = |I^{(2)}|/|H_2| \qquad (I^{(2)} \neq I_0^{(2)}),$$

using types of even length only, gives rise to a solution of

$$\sum_{\mathscr{I}^{(2)}}{}' w(\mathscr{I}^{(2)})\,\Omega_A(\mathscr{I}^{(2)}) = \begin{cases} |A|/|H_1\times H_2| & \text{if } A = I_0^{(1)}I^{(2)} \\ & \text{for some } I^{(2)} \neq I_0^{(2)}, \\ 0 & \text{if } A = I^{(1)}I^{(2)} \\ & \text{with } I^{(1)} \neq I_0^{(1)}, \end{cases} \tag{19}$$

by taking

$$w(\mathscr{I}^{(2)}) = \frac{|A|\,|H_2|}{|I^{(2)}|\,|H_1\times H_2|}\, w_2(\mathscr{I}^{(2)}) = \frac{1}{|H_1|}\, w_2(\mathscr{I}^{(2)}).$$

Taken together, (18) and (19) amount to

$$\sum_{\mathscr{A}}{}' w(\mathscr{A})\,\Omega_A(\mathscr{A}) = |A|/|H_1\times H_2| \qquad (A \neq A_0),$$

where each $\mathscr{A}$ with $w(\mathscr{A}) \neq 0$ consists of types of even length, and

$$\begin{aligned} \sum{}' w(\mathscr{A}) &= \sum_{\mathscr{I}^{(1)}}{}' \sum_{I^{(2)}} \frac{|I^{(2)}|}{|H_2|}\, w_1(\mathscr{I}^{(1)}) + \sum_{\mathscr{I}^{(2)}}{}' \frac{1}{|H_1|}\, w_2(\mathscr{I}^{(2)}) \\ &= \sum_{\mathscr{I}^{(1)}}{}' w_1(\mathscr{I}^{(1)}) + \frac{1}{|H_1|} \sum_{\mathscr{I}^{(2)}}{}' w_2(\mathscr{I}^{(2)}). \end{aligned}$$

It follows that

$$B_2(H_1\times H_2) \geqslant B_2(H_1) + |H_1|^{-1} B_2(H_2)$$

and

$$b_2(H_1\times H_2) \leqslant b_2(H_1) + |H_1|^{-1} b_2(H_2),$$

and hence

$$C_2(H_1\times H_2) \geqslant C_2(H_1) + |H_1|^{-1} C_2(H_2).$$

Every finite Abelian group can be written as a direct product of distinct homocyclic p-groups (although the primes p need not be distinct). Since there are only finitely many homocyclic p-groups of any given order, a large finite Abelian group must have a large homocyclic p-group as a direct factor. Theorem 6 now follows from the facts that C_2 is an increasing function of H, that $D(H)$ tends to infinity with h and that $C(H)$ tends to $1/2$ as h tends to infinity when H is restricted to homocyclic p-groups (by Theorem 5).

It would be interesting to know whether $C(H)$ itself is an increasing function of H in any sense, and if so whether it satisfies an inequality of the kind that $L(H)$ and $C_2(H)$ do. An argument very like the one used at the end of §4 shows that if

$$U(H) = \frac{1}{|H|}\sum{}'\left(\frac{1}{2}-\frac{\nu(H)}{D(H)}\right)$$

(by Theorem 2 (ii) this is an upper bound for $C(H)$ when H is a p-group) then $U(H) \geqslant U(H/H_1)+U(H_1)|H_1|/|H|$ for every subgroup H_1 of H. (The corresponding inequality for the general upper bound $(\frac{1}{2}-D(H)^{-1})\times$ $\times(1-|H|^{-1})$ given by Lemma 2 (i) is also true and follows trivially from the fact that $D(H)$ is, by its definition, an increasing function of H.) Since Theorem 5 shows that $C(H) = U(H)$ when H is a homocyclic p-group we have $C(H) \geqslant C(H/H_1)+C(H_1)|H_1|/|H|$ whenever H is a homocyclic p-group.

7. C_k and $C(H)$ for certain small class groups. In this section we evaluate C_k and $C(H)$ for some small class groups not covered by Theorems 3 or 5.

We start with $H = \boldsymbol{Z}_2\times\boldsymbol{Z}_2 = \langle Y, Z\rangle$, where $Y^2 = Z^2 = X_0$. The irreducible types of H are $\prec Y, Y\succ$, $\prec Z, Z\succ$, $\prec YZ, YZ\succ$ and $\prec Y, Z, YZ\succ$, and so the equations (5) are

$$\begin{aligned}2v_1+v_4 &= \delta(Y),\\ 2v_2+v_4 &= \delta(Z),\\ 2v_3+v_4 &= \delta(YZ),\end{aligned}$$

where the numbering of the variables corresponds to the order we have listed the types in. In any solution $v_1 = \frac{1}{2}(\delta(Y)-v_4)$, $v_2 = \frac{1}{2}(\delta(Z)-v_4)$ and $v_3 = \frac{1}{2}(\delta(YZ)-v_4)$, so

$$\sum_{i=1}^{4} v_i = \tfrac{1}{2}(\delta(Y)+\delta(Z)+\delta(YZ)-v_4).$$

This is minimal when v_4 is as large as possible (subject to the variables being non-negative), that is, $v_4 = \min(\delta(Y), \delta(Z), \delta(YZ))$. Hence

$$b = \tfrac{1}{2}\Big(\sum_{X\neq X_0}\delta(X)-\min_{X\neq X_0}\delta(X)\Big) \quad\text{and}\quad C = \tfrac{1}{2}\min_{X\neq X_0}\delta(X).$$

Next take $H = \boldsymbol{Z}_6 = \langle Y\rangle$, where $Y^6 = X_0$. The irreducible types of H (taking only one from each inverse pair) are

$$\prec \underset{6}{Y}\succ,\quad \prec \underset{3}{Y^2}\succ,\quad \prec \underset{2}{Y^3}\succ,\quad \prec \underset{4}{Y}, Y^2\succ,\quad \prec \underset{3}{Y}, Y^3\succ,\quad \prec \underset{2}{Y}, Y^4\succ,$$
$$\prec \underset{2}{Y}, \underset{2}{Y^2}\succ,\quad \prec Y, Y^5\succ,\quad \prec Y, Y^2, Y^3\succ,\quad \prec Y^2, Y^4\succ,\quad \prec Y, Y^3, \underset{2}{Y^4}\succ,$$

and so the equations (7) are

$$\begin{array}{lllllllllllll} 6w_1 & & & +4w_4 & +3w_5 & +2w_6 & +2w_7 & +2w_8 & +w_9 & & +w_{11} & = 2\delta(Y), \\ & 3w_2 & & +w_4 & & +w_6 & +2w_7 & & +w_9 & +2w_{10} & +2w_{11} & = 2\delta(Y^2) \\ & & +2w_3 & & +w_5 & & & & +w_9 & & +w_{11} & = \delta(Y^3). \end{array}$$

Every column except the last, of the coefficient matrix on the left, can be expressed as a linear combination of the first three columns with non-negative coefficients whose sum is $\leqslant 1$. Hence any solution of the equations can be modified to make $w_4, \ldots, w_{10}$ zero at the expense of increasing w_1, w_2 and w_3, and $\sum w_i$ will be no larger for the new solution than for the original one. So in looking for a solution with $\sum w_i$ minimal we can assume that $w_4 = \ldots = w_{10} = 0$, and the equations become

$$\begin{aligned}6w_1+w_{11} &= 2\delta(Y),\\ 3w_2+2w_{11} &= 2\delta(Y^2),\\ 2w_3+w_{11} &= \delta(Y^3).\end{aligned}$$

In any solution $w_1 = \frac{1}{3}\delta(Y)-\frac{1}{6}w_{11}$, $w_2 = \frac{2}{3}\delta(Y^2)-\frac{2}{3}w_{11}$ and $w_3 = \frac{1}{2}\delta(Y^3)-$ $-\frac{1}{2}w_{11}$, so

$$\sum w_i = \tfrac{1}{3}\delta(Y)+\tfrac{2}{3}\delta(Y^2)+\tfrac{1}{2}\delta(Y^3)-\tfrac{1}{3}w_{11}.$$

This is minimal when w_{11} is as large as possible, namely $\min(2\delta(Y),$ $\delta(Y^2), \delta(Y^3))$. Hence

$$b = \tfrac{1}{3}\delta(Y)+\tfrac{2}{3}\delta(Y^2)+\tfrac{1}{2}\delta(Y^3)-\min\left(\tfrac{2}{3}\delta(Y), \tfrac{1}{3}\delta(Y^2), \tfrac{1}{3}\delta(Y^3)\right)$$

and

$$C = \tfrac{2}{3}\delta(Y)+\tfrac{1}{3}\delta(Y^2)+\min\left(\tfrac{2}{3}\delta(Y), \tfrac{1}{3}\delta(Y^2), \tfrac{1}{3}\delta(Y^3)\right).$$

Finally we evaluate $C(\boldsymbol{Z}_2\times\boldsymbol{Z}_4)$. Let Y and Z be generators of $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ with $Y^2 = Z^4 = X_0$. Apart from $\{X_0\}$ this group has the three automorphism classes $\{Z^2\}$, $\{Y, YZ^2\}$, and $\{Z, Z^3, YZ, YZ^3\}$, the first having $\nu = 2$ and the other two having $\nu = 1$. Also $D(\boldsymbol{Z}_2\times\boldsymbol{Z}_4) = 5$. Any irreducible type other than $\prec Z^2, Z^2 \succ$, can have at most one element from the first of these classes and at most two from the second, and it must have an even number of elements from the third class for the total power of Z in the product of its elements to be even. Consequently the only possible vectors $\boldsymbol{\Omega}(\mathscr{A})$ that satisfy (16) are $\boldsymbol{\Omega}_1 = (1, 1, 2)$ and $\boldsymbol{\Omega}_2 = (0, 1, 4)$. However, when $\delta(X) = h^{-1} = 1/8$ for all non-principal X, $\Delta = h^{-1}(|\mathscr{A}|) = (\frac{1}{8}, \frac{1}{4}, \frac{1}{2})$, which is not a linear combination of $\boldsymbol{\Omega}_1$ and $\boldsymbol{\Omega}_2$ at all, let alone a linear combination with non-negative coefficients. Consequently

$$b(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4) > \frac{1}{D} \sum{}' \nu(A) \frac{|A|}{h} = \tfrac{1}{5}.$$

To find the exact value of $b(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4)$ we start by listing all the possible vectors $\boldsymbol{\Omega}(\mathscr{A})$ with $\sum{}' \nu(A)\Omega_A(\mathscr{A}) < D$. These are

$$\boldsymbol{\Omega}_3 = (2, 0, 0), \quad \boldsymbol{\Omega}_4 = (1, 2, 0), \quad \boldsymbol{\Omega}_5 = (1, 0, 2), \quad \boldsymbol{\Omega}_6 = (0, 2, 2),$$
$$\boldsymbol{\Omega}_7 = (0, 0, 4), \quad \boldsymbol{\Omega}_8 = (0, 1, 2), \quad \boldsymbol{\Omega}_9 = (0, 2, 0), \quad \boldsymbol{\Omega}_{10} = (0, 0, 2).$$

It is possible to find a non-negative solution of

$$\sum_{i=1}^{10} w_i \boldsymbol{\Omega}_i = (\tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}) \tag{20}$$

with $\sum w_i = 5/24$ (for example, $w_1 = 1/12$, $w_2 = 1/12$, $w_4 = 1/24$, the other w_i's zero, or $w_1 = 1/8$, $w_2 = 1/24$, $w_6 = 1/24$, the other w_i's zero) and we shall show that no smaller value of $\sum w_i$ is possible. First, the minimum value of $\sum w_i$ can be attained with all but three of the w_i's zero, since any four or more $\boldsymbol{\Omega}_i$'s are linearly dependent, and the linear dependence relation can be used to reduce one of the corresponding w_i's to zero while keeping the others non-negative and not decreasing the sum of the w_i's. Next, put $w_1 + w_2 = W_5$, $w_3 + w_4 + w_5 + w_6 + w_7 = W_4$, $w_8 = W_3$ and $w_9 + w_{10} = W_2$ (the new suffixes referring to the value of the left-hand side of (16) for the corresponding $\boldsymbol{\Omega}_i$'s). Then multiplying (14) by $\nu(A)$ and summing over A gives

$$5W_5 + 4W_4 + 3W_3 + 2W_2 = 2 \cdot \tfrac{1}{8} + 1 \cdot \tfrac{1}{4} + 1 \cdot \tfrac{1}{2} = 1.$$

If $W_5 + W_4 + W_3 + W_2 \leqslant 5/24$ then $W_5 - W_3 - 2W_2 \geqslant 1 - 4 \cdot (5/24) = 1/6$. Hence $W_5 = w_1 + w_2 \geqslant 1/6$ when $\sum w_i$ attains its minimum. Considering the first and last components on each side of (20) shows that neither w_1 nor w_2 can be as large as $1/6$, so w_1 and w_2 are both non-zero when $\sum w_i$ attains its minimum. For each $i = 3, \ldots, 10$ there is a unique solution of

$$w_1 \boldsymbol{\Omega}_1 + w_2 \boldsymbol{\Omega}_2 + w_i \boldsymbol{\Omega}_i = (\tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}),$$

and all that now remains is to pick, from among these eight sets of w's, the one with the w's all positive that has the smallest sum. There are in fact two such sets (those mentioned above) and their common sum is $5/24$. Finally, we need to check that there actually are irreducible types $\mathscr{A}$ with $\boldsymbol{\Omega}(\mathscr{A})$ equal to $\boldsymbol{\Omega}_1$, $\boldsymbol{\Omega}_2$ and $\boldsymbol{\Omega}_4$ (or $\boldsymbol{\Omega}_6$), and these are given by $\prec Z^2, Y, Z, YZ \succ$, $\prec Y, Z, Z, Z, YZ \succ$ and $\prec Z^2, Y, YZ^2 \succ$ (or $\prec Y, YZ^2, Z, Z \succ$). Hence

$$b(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4) = \frac{5}{24} \quad \text{and} \quad C(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4) = \frac{1}{2} \cdot \frac{7}{8} - \frac{5}{24} = \frac{11}{48}.$$

THEOREM 7. (i) *If k has class group $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ then*

$$C_k = \tfrac{1}{2} \min_{X \neq X_0} \delta(X).$$

(ii) *If k has class group $\boldsymbol{Z}_6$ and Y is a generator of it then*

$$C_k = \tfrac{2}{3}\delta(Y) + \tfrac{1}{3}\delta(Y^2) + \min\left(\tfrac{2}{3}\delta(Y), \tfrac{1}{3}\delta(Y^2), \tfrac{1}{3}\delta(Y^3)\right).$$

(iii) $C(\boldsymbol{Z}_2 \times \boldsymbol{Z}_4) = 11/48$.

References

[1] S. Allen, *On the factorisations of natural numbers in an algebraic number field*, J. London Math. Soc. (2) 11 (1975), pp. 294–300.

[2] E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ. Hamburg 3 (1924), pp. 89–108; *Collected papers*, Addison-Wesley, 1965, pp. 105–124.

[3] — *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Sem. Univ. Hamburg 5 (1927), pp. 353–363; *Collected papers*, pp. 131–141.

[4] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391–392.

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

[6] J. Kubilius, *Probabilistic methods in the theory of numbers*, Vilnius 1962. English translation, Amer. Math. Soc., Providence, Rhode Island 1964.

[7] W. Narkiewicz, *Factorization of natural numbers in some quadratic number fields*, Colloq. Math. 16 (1967), pp. 257–268.

[8] — *Numbers with unique factorization in an algebraic number field*, Acta Arith. 21 (1972), pp. 313–322.

[9] — *Elementary and analytic theory of algebraic numbers*, PWN, Warszawa 1974.

[10] — *Normal order for a function associated with factorization into irreducibles* (to appear in Acta Arith. 37).

[11] — and J. Śliwa, *Normal orders for certain functions associated with factorizations in number fields*, Colloq. Math. 38 (1978), pp. 323–328.

[12] R. W. K. Odoni, *On a problem of Narkiewicz*, J. Reine Angew. Math. 288 (1976), pp. 160–167.

[13] J. E. Olson, *A combinatorial problem on finite Abelian groups, I*, J. Number Theory 1 (1969), pp. 8–10.

[14] J. Rosiński and J. Śliwa, *The number of factorizations in an algebraic number field*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 24 (1976), pp. 821–826.

[15] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), pp. 274–276.

[16] – *Über einige Verallgemeinerungen eines Satzes von Hardy und Ramanujan*, ibid. 11 (1936), pp. 125–133.

SCICON COMPUTER SERVICES
Brick Close, Kiln Farm
Milton Keynes, England

DEPARTMENT OF PURE MATHEMATICS
UNIVERSITY COLLEGE, CARDIFF
Cardiff, Wales

Received on 30. 5. 1977
and in revised form on 21. 6. 1977 (948)

ACTA ARITHMETICA
XXXVI (1980)

A note on some polynomial identities

by

L. Carlitz (Durham, N. C.)

1. Hirschhorn [2] has proved the polynomial identities

$$\prod_{r=1}^{3n}(1-x^r) = (1-x^{3n+3})\ldots(1-x^{6n})+\sum_{r=1}^{n}(-1)^r(x^{r(3r-1)/2}+x^{r(3r+1)/2}\times \tag{1.1}$$

$$\times(1-x^{3n-3r+3})\ldots(1-x^{3n})(1-x^{3n-3r+3})\ldots(1-x^{6n})$$

and

$$\prod_{r=1}^{n}(1-x^r)^3 = \sum_{r=0}^{n}(-1)^r(2r+1)x^{(r+1)/2}\times \tag{1.2}$$

$$\times(1-x^{n-r+1})\ldots(1-x^n)(1-x^{n+r+2})\ldots(1-x^{2n+1}).$$

He showed also that (1.1) and (1.2) imply

$$\prod_{r=1}^{\infty}(1-x^r) = 1+\sum_{r=1}^{\infty}(-1)^r(x^{r(3r-1)/2}+x^{r(3r+1)/2}) \tag{1.3}$$

and

$$\prod_{r=1}^{\infty}(1-x^r)^3 = \sum_{r=0}^{\infty}(-1)^r(2r+1)x^{r(r+1)/2}, \tag{1.4}$$

the identities of Euler and Jacobi, respectively.

In this note we show that

$$\prod_{r=1}^{3n}(1-x^{r/3}) = (x)_n\sum_{r=-n}^{n}(-1)^r\begin{bmatrix}2n\\ n-r\end{bmatrix}x^{r(r-1)/2+r/3} \tag{1.5}$$

and

$$\prod_{r=1}^{n}(1-x^r)^2 = \sum_{r=0}^{n}(-1)^r(2r+1)\begin{bmatrix}2n+1\\ n-r\end{bmatrix}x^{r(r+1)/2}, \tag{1.6}$$

where

$$(x)_n = (1-x)(1-x^2)\ldots(1-x^n)$$