J. Austral. Math. Soc. (*Series A*) **35** (1983), 143–161

ON REPRESENTING INTEGERS AS PRODUCTS OF INTEGERS OF A PRESCRIBED TYPE

P. D. T. A. ELLIOTT

(Received 25 May 1982)

Communicated by A. J. van der Poorten

Abstract

A general group-theoretic procedure is indicated for representing rational integers as products of other integers. A detailed example is given.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 K 20, 10 L 10, 10 M 99, 12 C 99.

THEOREM. *Let*

$$R(x) = \prod_{i=1}^{h} (x + a_i)^{b_i}$$

be a rational function with integer roots $-a_i \leqslant 0$, *and non-zero exponents whose highest common factor* $(b_1, \ldots, b_h)$ *is* 1. *Let an integer* $k \geqslant 3$ *be given.*

Then every positive integer n has a representation of the form

$$n = \prod_j R(n_j)^{\varepsilon_j}$$

where each $\varepsilon_j = \pm 1$, *and the* n_j *lie in an interval* $k \leqslant n_j \leqslant c_0 n$ *for some constant* c_0.

The condition $(b_1, \ldots, b_h) = 1$ is necessary. If, for example, every b_i were even, then products of the $R(m)$ could only represent squares of integers.

We cannot at present give an algorithm to determine the constant c_0.

This theorem illustrates a procedure which may be attempted whenever it is desired to represent one or many integers as products.

Let Q_1 denote the group of positive rational fractions with multiplication as group law. Let $\Gamma(k)$ denote the subgroup generated by the positive $R(m)$. We

https://doi.org/10.1017/S1446788700025635 Published online by Cambridge University Press

form the quotient group $G = Q_1/\Gamma(k)$ and construct a proof in three stages by showing that

(i) G is finitely generated,

(ii) G has bounded order,

(iii) G is trivial.

Steps (i) and (ii) are carried out by considering the homomorphisms of G into the additive group of rational numbers (mod 1), and of the reals, respectively.

If both (i) and (ii) have been obtained then G is finite. We have preserved the above formulation since one can sometimes obtain (ii) without (i), and the method may still proceed. Moreover, our following arguments generalise almost at once to a wide class of modules, and an analogue of (ii) can be readily formulated.

Step (iii) applies the homomorphisms of G into the finite fields which have a prime number of elements. In other problems one could use a function field over a finite field, since these permit (non-archimedean) topologies. In order to obtain an appropriate action on G it is convenient to work with the quotients G/G^p where G^p is the subgroup of G whose elements are pth-powers.

Taken together these three steps form an analogue of the Hardy-Littlewood (circle) method traditionally employed in the additive representation of integers. Our steps (ii) and (iii) correspond to the introduction of the singular integral and singular series of that method, and represent some form of the Hasse "local to global" principle. Step (i) corresponds to the application of algebraic geometry to the study of exponential sums on the so-called minor arcs. For an up-to-date presentation of the classical and some modern applications of the Hardy-Littlewood method see Vaughan (1981). For an example which illustrates the need for auxiliary information from algebraic geometry see Davenport's paper (1963) on cubic forms.

Product representations of the above type play a rôle in the theory of characters. If a Dirichlet character $\chi(\ )$ satisfies

$$\chi(R(n)) = 1 \quad \text{for } k < n \leqslant H$$

then our theorem shows that

$$\chi(n) = 1 \quad \text{for } 1 \leqslant n \leqslant H/c_0.$$

For non-principal characters this puts a limit on the size H may be. In this way we can obtain a small integer n for which $\chi(R(n))$ is not zero or 1. For background results on character sums see Burgess (1962). For an example of an application of this type (with a different function in the rôle of $R(n)$) see Burgess (1967).

Our present method reduces the problem to the consideration of additive arithmetic functions on sequences of various integers. Whilst the study of such

https://doi.org/10.1017/S1446788700025635 Published online by Cambridge University Press

functions lies within the scope of probabilistic number theory (see, for example, Elliott (1979/80)), in many circumstances only partial results are readily available. Some connections between the present method and others used in obtaining related results, together with an example involving shifted prime numbers, are discussed following the proof of the theorem.

Divisible modules

Let G be an abelian group (written additively) which becomes a module under the action of a principal ideal domain R. We write this action on the left side, thus rg is defined for r in R and g in G.

We say that G is a divisible (R-) module if for every element g in G and every non-zero member r of R we can find a further element h in G so that $g = rh$.

LEMMA 1. *Let H be a submodule of the R-module G. Then any homomorphism of H into a divisible R-module D can be extended to a homomorphism of G into D.*

REMARK. In this and what follows the homomorphisms are module homomorphisms.

PROOF. When R is $\mathbf{Z}$, the ring of rational integers, this result appears as exercise 1 in Kaplansky's book (1969) on infinite abelian groups.

We consider the collection of all pairs (K, t) of submodules K containing H which have a homomorphism t into D extending that defined on H. We partially order these pairs by

$$(K, t) \succ (K', t')$$

if K includes K' and t extends t'. It is readily checked that any chain has an upper bound, and by Zorn's lemma the collection contains a maximal pair, (L, τ) say.

Suppose that L is not G, and let g be an element of G not in L. Let Δ be the submodule generated by g and L.

If mg does not lie in L for any non-zero member m of R then Δ is the direct sum of L and the module generated by g. We may define a map $T: \Delta \to D$ by

$$T(mg + \lambda) = \tau(\lambda)$$

for all λ in L.

Otherwise there will be a non-trivial ideal of elements m in R so that mg lies in L. Since R is principal this ideal will be generated by an element, π say.

We now appeal to the divisibility of the module D, and let δ be an element of it for which $\tau(\pi g) = \pi\delta$. We then define

$$T(mg + \lambda) = m\delta + \tau(\lambda).$$

Note that if $m_1 g + \lambda_1 = m_2 g + \lambda_2$ then $(m_1 - m_2)g$ belongs to L, so that in R $m_1 - m_2$ must be a multiple of π, say $k\pi$. Hence

$$\begin{aligned} T(m_1 g + \lambda_1) - T(m_2 g + \lambda_2) &= (m_1 - m_2)\delta + \tau(\lambda_1) - \tau(\lambda_2) \\ &= k\pi\delta + \tau(\lambda_1 - \lambda_2) = k\pi\delta + \tau(\{m_2 - m_1\}g) \\ &= k\pi\delta - k\tau(\pi g) = 0, \end{aligned}$$

so that T is well defined.

In either case we obtain a genuine extension

$$(\Delta, T) \succ (L, \tau),$$

contradicting the maximality of (L, τ).

Thus $L = G$ and the lemma is proved.

We say that a homomorphism is trivial on a set of elements of a module if it takes each of them to zero (the identity).

In what follows D will be a divisible module containing at least two elements.

LEMMA 2. *Let G_1 and G_2 be submodules of an R-module G_1. If every homomorphism of G into D which is trivial on G_1 is also trivial on G_2, then to each element g in G_2 there is a non-zero member r of R so that rg lies in G_1.*

PROOF. Suppose, to the contrary, that no product rg with r in R of the element g of G_2 lies in G_1. Let Δ be the module generated by g and G_1. Since Δ is the direct sum of G_1 and the module generated by g, we may define a homomorphism t of Δ into D by setting $t(g)$ to be any non-zero element in D, and defining

$$t(rg + \mu) = rt(g)$$

for each element μ of G_1.

By Lemma 1 t may be extended to a homomorphism of G into D. Moreover, this new homomorphism is trivial on G_1 but not on G_2, contradicting the hypothesis of the lemma.

Lemma 2 is established.

REMARK. In our applications it will not be assumed that the modules G_1 and G_2 have any non-trivial intersection.

Any abelian group may be considered a $\mathbf{Z}$-module. An abelian group which is divisible as a $\mathbf{Z}$-module we shall call a *divisible abelian group* without mentioning its module structure. In this case we can reformulate Lemma 2 as

LEMMA 3. *Let G_1 and G_2 be subgroups of an abelian group G. Suppose that every homomorphism of G into a (non-trivial) divisible group D which is trivial on G_1, is also trivial on G_2. Then every element in G_2 has a positive multiple in G_1.*

REMARK. In our applications of this lemma it will be convenient to take for D the additive group of the real numbers, which is clearly divisible.

For groups which have torsion better can sometimes be done. Let p be a rational number prime number and let G be a possibly infinite abelian group, each of whose non-trivial elements has order p. Let F_p be a finite field of p elements.

We can make F_p act on G by identifying F_p with the field of integer residue classes (mod p), $\mathbf{Z}/p\mathbf{Z}$, and using the rule

$$(n \pmod p, g) \mapsto ng.$$

In view of the p-torsion this action is well defined. G now becomes a vector space over F_p.

The analogue of Lemma 3 is now

LEMMA 4. *Let G_1 and G_2 be subgroups of an abelian group G with p-torsion. Suppose that every homomorphism of G into a non-trivial vector space over F_p which is trivial on G_1 is also trivial on G_2. Then G_2 is contained in G_1.*

PROOF. Since F_p is a field, any vector space over F_p is F_p-divisible. According to Lemma 2 with $R = F_p$, to each element g of G_2 there is a non-zero member r of F_p so that rg belongs to G_1. Once again using that F_p is a field, there is a member s of F_p so that $sr = 1$, and therefore $g = s(rg)$ itself belongs to G_1.

REMARK. In our application of Lemma 4 groups G arise which need not have p-torsion; so we give them it by considering the factor group G/G^p, where G^p denotes the subgroup of pth-powers of elements in G.

AN EXAMPLE. Let q be a rational prime and let $p_1 < p_2 < \cdots$ run through all the rational primes. Define the integers

$$(1) \qquad a_1 = p_1^{q^2}, \qquad a_{j+1} = (p_1 \cdots p_{j+1})^q (p_1 \cdots p_j)^{-1}, \qquad j = 1, 2, \ldots.$$

Let A be the subgroup Q_1 which is generated by these a_i.

If for any $i \geqslant 2$ and integer m p_i^m belongs to A, then there will be a representation

$$p_i^m = \prod_{l=1}^{s} a_l^{d_l}$$

for integers d_l, and $s \geqslant 1$. Since each p_{j+1} occurs in a_{j+1} and in no a_w with $w \leqslant j$, we see that $s \leqslant i$ must hold. Then $m = qd_i$.

On the other hand (group theoretically)

$$p_{j+1}^q \equiv (p_1 \cdots p_j)^{q-1} \pmod{A},$$

and an easy inductive proof shows that

$$p_i^{q^{i+1}} \equiv 1 \pmod{A}, \qquad i = 1, 2, \ldots.$$

We see that every element of the group Q_1/A has an order which is a power of q, and which is at least q.

Since every element of Q_1/A has a finite order all homomorphisms of it into the additive group of real numbers are trivial. Likewise it cannot have a non-trivial homomorphism into an F_p with $p \neq q$. Moreover,

$$p_j = \frac{p_2 \cdots p_j}{p_2 \cdots p_{j-1}} \equiv \frac{(p_1 \cdots p_{j+1})^q}{(p_1 \cdots p_j)^q} \equiv p_{j+1}^q \pmod{A}$$

for $j \geqslant 2$, and

$$p_1 = \frac{p_1 p_2}{p_2} \equiv \frac{(p_1 p_2 p_3)^q}{p_2} \pmod{A},$$

so that every element of Q_1/A is the qth-power. Thus it has no non-trivial homomorphisms into F_q.

Since no p_i belongs to A it is clear that the vanishing of the homomorphisms into the additive group of the reals, together with those into the finite fields F_p is not enough to ensure the triviality of Q_1/A, and therefore the representation of integers as products of the a_j.

The reason for this is that the homomorphisms have ranges in groups which do not (necessarily) possess enough structure. By considering maps into more structured groups better may be done.

Let D_1 be a divisible R-module with an identity. Suppose that for each prime element π of R there is a non-zero element g of D_1 so that $\pi g_1 = 0$.

Lemma 5. *Let G_1 and G_2 be sub-modules of an R-module G. Suppose that every homomorphism of G into D_1 which is trivial on G_1 is also trivial on G_2. Then G_2 is contained in G_1.*

https://doi.org/10.1017/S1446788700025635 Published online by Cambridge University Press

PROOF. For each g in G_2, Lemma 2 guarantees that the ideal of elements r in R for which rg belongs to G_1 is not empty.

Suppose that for some g in G_2 this ideal is non-trivial, and is generated by α. Let π be a prime element of R which divides α and set $yu = \pi^{-1}\alpha g$. Then y belongs to G_2 but not to G_1. Moreover, πy lies in G_1.

Let Δ be the module generated by G_1 and y. We define a map T of Δ into D_1 by choosing a non-zero element δ of D_1 which satisfies $\pi\delta = 0$ and setting

$$T(ry + \mu) = r\delta$$

for every r in R and μ in G_1. If $r_1 y + \mu_1 = r_2 y + \mu_2$ then $(r_1 - r_2)y$ belongs to G_1, so that π divides $r_1 - r_2$. Let $r_1 - r_2 = \rho\pi$. Then

$$T(r_1 y + \mu_1) - T(r_2 y + \mu_2) = (r_1 - r_2)\delta = \rho\pi\delta = 0,$$

and T is well defined.

By Lemma 1 we may extend T to a homomorphism of G into D_1, which is then trivial on G_1 but not G_2. This contradicts the hypothesis of the lemma.

Lemma 5 is proved.

A candidate for D_1 is the multiplicative group of complex numbers which are roots of unity, or its isomorphic copy the additive group $Q/\mathbf{Z}$ of rationals (mod 1).

A ring of operators

Let S be an R-module, containing at least two elements, defined over an integral domain R which has an identity. Consider the set of all doubly-infinite sequences $(\ldots, s_{-1}, s_0, s_1, s_2, \ldots)$ of elements of s. We introduce the shift operator E whose action takes a typical sequence $\{s_n\}$ to the new sequence $\{s_{n+1}\}$. If $F(x) = \sum_{j=1}^{r} c_j x^j$ is a polynomial with coefficients in K, we extend this definition by defining

$$F(E)s_n = \sum_{j=1}^{r} c_j s_{n+j}.$$

In this way we define a ring of operators which is isomorphic to the ring of polynomials with coefficients in K. In what follows operator will mean a (polynomial) operator which belongs to this ring.

Let K be the quotient ring of R.

LEMMA 6. *Let $F(x)$ be a polynomial in $R[x]$ which factorises into*

$$a \sum_{i=1}^{r} (x - \theta_i)$$

over some extension field of K. Then for each positive integer d

$$a^{rd}\sum_{i=1}^{r}(x-\theta_i^d)$$

also belongs to $R[x]$.

If, furthermore, R is integrally closed, then the polynomial

$$a^{rd}\prod_{i=1}^{r}(x^d-\theta_i^d)$$

is divisible by $F(x)$ *in* $R[x]$.

Remark. For the properties of integral closure see Zariski and Samuel (1962) Chapter V.

Proof. Consider the polynomial

$$\prod_{i=1}^{r}(x-y_i^d)$$

with the y_i distinct indeterminates over K. The coefficients b_j of s^j, $0 < j < r$, is a symmetric function of the y_i, of total degree $(r-j)d$. If σ_ν, $\nu = 0,\ldots,r$, denotes the elementary symmetric functions of the y_i, then b_j is a polynomial in these σ_ν, of degree at most rd. (See, for example, van der Waerden (1953) Volume 1, Chapter 26.)

Specialising the y_i to θ_i, we see from our first hypothesis that every $a\sigma_\nu$ belongs to R. Hence $a^{rd}b_j$ belongs to R for every j, which justifies the first assertion of the lemma.

Consider next the polynomial

$$W(x) = a^{rd}\prod_{i=1}^{r}(s^d-\theta_i^d).$$

Clearly each factor $x^d-\theta_i^d$ is divisible by $x-\theta_i$ in some algebraic extension of K. By working in a large enough extension $F(x)$ will divide $W(x)$. Since K is a field $F(x)$ then divides $W(x)$ in $K[x]$.

For each root θ_i of $F(x) = 0$, $a\theta_i$ is integral over R. The coefficients of the polynomial

$$a^{d-1}\frac{x^d-\theta_i^d}{x-\theta_i}$$

are thus integral over R, and so are those of the polynomial $W(x)R(x)^{-1}$.

Since R is integrally closed in its quotient field, this last polynomial actually belongs to $R[x]$.

The lemma is proved.

In our next two lemmas and in their application, R will be a unique factorisation integral domain with identity.

A function $f(n)$ is said to be *arithmetic* if it is defined on the positive natural integers. We shall say that it is *additive* if it takes values in S and satisfies the relation

$$f(ab) = f(a) + f(b)$$

for all positive integers a and b. In the theory of numbers one traditionally requires this relation only to hold if a and b have no common factor other than 1. We shall not need this limitation. Thus our additive arithmetic functions are restrictions, to the integers, of homomorphisms of the group of positive rational fractions.

We extend the sequence $f(1), f(2), \ldots,$ of values of an arithmetic function to a doubly infinite sequence by setting $f(n) = 0$ if $n \leqslant 0$.

Note that if $f(\ )$ is an arithmetic function

$$Ef(2n) = f(2n+1).$$

If, however, we define a new arithmetic function $g(\ )$ by $g(n) = f(2n)$ then

$$Eg(n) = g(n+1) = f(2n+2).$$

LEMMA 7. *In the above notation suppose that the additive arithmetic function $f(\ )$ satisfies*

$$\psi(E)f(n) = \textit{constant}, \qquad k \leqslant n \leqslant H,$$

for some operator $\psi(E)$. Let

$$\psi(x) = a\sum_{i=1}^{s}(x-\omega_i)^{r_i},$$

with distinct ω_i, hold over some extension field of K. Let $t = r_1 + \cdots + r_s$ denote the degree of $\psi(x)$. Let a positive integer d be given.

Then either there is a permutation σ of the ω_i with

(2) $$\sigma(\omega_i) = \omega_i^d, \qquad i = 1, \ldots, s,$$

or there is a further non-zero polynomial $\psi_1(x)$, defined over R and with degree less than that of $\psi(x)$, so that

(3) $$\psi_1(E)f(n) = (\textit{another})\ \textit{constant}$$

holds over the interval $k \leqslant n \leqslant (H/d) - t$.

PROOF. Consider the polynomial $G(x) = a^{td}\prod_{i=1}^{s}(x-\omega_i^d)^{r_i}$. By Lemma 6 $\psi(x)$ divides $G(x^d)$ in $R[x]$. Therefore

$$G(E^d)f(n) = \text{constant}$$

for $k \leqslant n \leqslant H - m_1$ where $m_1 = \deg(G(x^d)/\psi(x)) \leqslant t(d-1)$.

Let $G(x) = \sum_{j=0}^{t} c_j x^j$. Then $G(E^d)f(n) = \sum_{j=0}^{t} c_j f(n + dj)$, so that for $k \leqslant nd \leqslant H - m_1$

$$\sum_{j=0}^{t} c_j f(n+j) = \sum_{j=0}^{t} c_j [f(d\{n+j\}) - f(d)]$$
$$= G(E^d)f(nd) - G(1)f(d) = \text{constant}.$$

In particular

$$G(E)f(n) = \text{constant}$$

over the range $k \leqslant n \leqslant (H/d) - t$.

If the roots of G are a permutation of the ω_i (in both cases neglecting the multiplicities r_i) we obtain the first of the two possibilities appearing in the statement of Lemma 7. Otherwise $G(x)$ and $a^{td-1}\psi(x)$ have the same leading terms, but are distinct. With $\psi_1(x) = a^{td-1}\psi(x) - G(x)$ we then have the second of the possibilities.

Lemma 7 is proved.

Lemma 8. *Let*

$$\psi(E)f(n) = \textit{constant}, \qquad k \leqslant n \leqslant H,$$

where $\psi(x)$ is a polynomial over R of degree t. Let d be an integer, $d \geqslant 2$.

Then there are integers q, $0 \leqslant q \leqslant t$, and a non-zero element δ of R, such that

$$\delta(E-1)^q f(n) = 0 \quad \textit{for } k + t \leqslant n \leqslant Hd^{-t^2(t+1)} - 2t.$$

Moreover, if $H \geqslant 2^{11t^3}k^2$ and S is a field, then

$$f(n) = 0 \quad \textit{for } k + t \leqslant n \leqslant 2^{-6t^3}H.$$

Remark. The same value of δ may serve for all the H which satisfy the hypothesis of the lemma.

Proof. The hypotheses of Lemma 7 are satisfied. Suppose that a permutation σ with the property (2) of that lemma exists. Consider a cycle in the permutation, say,

$$z_1 \to z_2 \to \cdots \to z_h \to z_1,$$

so that $z_j = \sigma z_{j-1}$, $j = 1, \ldots, h$. Then by (2)

$$z_1 = \sigma z_h = z_h^d = (\sigma z_{h-1})^d = \cdots = z_1^{d^h},$$

giving $z_1^{d^h - 1} = 1$. In this way every root ω_i of $\psi(x)$ is seen to be a root of unity, $\omega_i^{d_i} = 1$ say, and each d_i is a divisor of one of the numbers $d^w - 1$, $1 \leqslant w \leqslant s$.

Let

$$D = \prod_{w=1}^{s} (d^w - 1) < d^{s^2} \leqslant d^{t^2}.$$

Then $\omega_i^D = 1$ for every i. Clearly $\psi(x)$ divides the polynomial

$$a^{tD} \prod_{i=1}^{s} \left(x^D - \omega_i^D\right)^{r_i},$$

giving

$$a^{tD}(E^D - 1)^t f(n) = \text{constant}$$

over the interval $k \leqslant n \leqslant H - t(D - 1)$. Arguing as in the proof of Lemma 7 we replace n by Dn and reach

$$a^{tD}(E - 1)^t f(n) = \text{constant}$$

for $k \leqslant n < (H/D) - t$.

It is convenient at this point to consider the alternative (3) presented in Lemma 7. This has the form of the hypothesis of the present lemma save that the degree of $\psi_1(x)$ is less than that of $\psi(x)$, and the range $[k, H]$ is reduced to $[k, (H/D) - t]$.

Assume that $t \geqslant 1$. We may argue inductively to reach an integer q, $0 \leqslant q \leqslant t$, a non-zero element δ, such that

$$\delta(E - 1)^q f(n) = \text{constant}$$

holds for

$$k + t \leqslant n \leqslant \frac{H}{d^{t^2(t-q+1)}} - t\left(1 + \frac{1}{d^{t^2}} + \cdots + \frac{1}{d^{t^2(t-q)}}\right),$$

and certainly over the range $k \leqslant n \leqslant Hd^{-t^2(t+1)} - 2t$.

If now S is a field, and $q \geqslant 1$, we set $s(n) = (E - 1)^{q-1} f(n)$ and over this same range have $s(n + 1) - s(n) = c_0$, say, giving $s(n) = c_0 n + c_1$ for certain constants c_0, c_1. Proceeding inductively in this manner we obtain a polynomial $g(y)$, of degree at most t, such that

$$f(n) = g(n) \quad \text{for } k + t \leqslant n \leqslant Hd^{-t^2(t+1)} - 2t.$$

We next note that so long as $k^2 \leqslant n^2 \leqslant Hd^{-t^2(t+1)} - 2t$ we have

$$g(n^2) - 2g(n) = f(n^2) - 2f(n) = 0.$$

If now $H > 2t(4t + k)^2 d^{t^2(t+1)}$, $t \geqslant 1$, and S has characteristic zero, the polynomial $g(x^2) - 2g(x)$, which is of degree at most $2t$, will have more than $2t$ distinct (integer) roots. It must therefore be identically zero, that is to say $g(x)$ must be a constant.

The same argument may still be made unless S is a field of finite characteristic $p \leqslant 2t$. For such fields we have

$$f(p) + f(n) = f(pn) = g(0) \quad \text{for } k + t \leqslant pn \leqslant Hd^{-t^2(t+1)} - 2t.$$

Thus in every case

$$f(n) = \text{constant}, \qquad k + t \leqslant n \leqslant (2t)^{-1} Hd^{-t^2(t+1)} - 1.$$

Denoting this constant by c we have $2c = 2f(k+t) = f((k+t)^2) = c$, giving $c = 0$.

The proof of the lemma is now completed by setting $d = 2$ and treating the simple case $t = 0$ directly.

Proof of the theorem

As in the introduction let Q_1 denote the multiplicative group of positive rational numbers.

Let G_1 denote its subgroup generated by the fractions

$$R(l) \quad \text{with } k \leqslant l \leqslant H,$$

and let G_2 be the subgroup generated by the integers in the interval $k + t \leqslant n \leqslant 2^{-6t^3}H$.

Let W be the group G_2/G_1, viewed as the subgroup of Q_1/G_1 which is generated by the cosets $g \pmod{G_1}$ as g runs through the elements of G_2.

Suppose that f^* is a homomorphism of W into an R-divisible group Γ, where R is a principal ideal domain which acts upon W and Q_1/G_1. Then by Lemma 1 there is an extension of f^* which maps the whole of Q_1/G_1 into Γ. Thus there is an additive function

$$f: Q_1 \to \Gamma$$

which is trivial on the subgroup G_1, and which is consistent with f^* when suitably restricted.

For a homomorphism $f(\ )$ of Q_1 into Γ to be trivial on G_1 we must have $f(R(l)) = 0$, that is

$$\sum_{i=1}^{h} b_i f(l + a_i) = 0 \tag{4}$$

for each integer l in $[k, H]$. Here we have assumed that the rational integers can be given a suitable interpretation in R.

(i) If now $H \geqslant 2^{11t^3}k^2$ and $\Gamma = S$ is the additive group $Q/\mathbf{Z}$, regarded as a $\mathbf{Z}$-module, then we may apply Lemma 8 with

$$\psi(x) = \sum_{i=1}^{h} b_i x^{a_i}, \qquad t = \max a_i,$$

to obtain integers $m > 0$ and q, $0 \leqslant q \leqslant t$, so that

$$m(E-1)^q f(n) = 0, \qquad k + t \leqslant n \leqslant H2^{-t^2(t+1)} - 2t.$$

Note that S is not a field, so we are not permitted to appeal to the second assertion of that lemma.

However, if $q \geqslant 1$ the function $m(E-1)^{q-1}f(n)$ is constant on the interval $[k+t, 2^{-6t^3}H]$ and, if $f(j) = 0$, $k + t \leqslant j \leqslant k + 2t$, will be zero there.

Arguing inductively we see that the assumption (4) now forces $mf(n)$ to be zero over the whole range $[k, 2^{-6t^3}H]$.

In our above notation: if f^* is trivial on the subgroup of W generated by the cosets $j \pmod{G_1}$, $j = k, \ldots, k + t$, then f^* is trivial on W^m the group of mth-powers of the elements in W.

By Lemma 5 the group W^m is finitely generated, with the $j \pmod{G_1}$ as generators. Moreover, the value of m does not depend upon the value of H.

(ii) We now apply the above argument with $\Gamma = S$ the additive group of the real numbers, regarded as a $\mathbf{Z}$-module. In fact we can apply Lemma 2 directly. In this case the hypothesis (4) leads to the conclusion

$$f(n) = 0 \quad \text{on } \left[k + t, 2^{-6t^3}H\right],$$

for the reals are a field and we may apply the full force of Lemma 8.

Since each of the above integers j lies in the interval $[k + t, 2^{-6t^3}H]$, there are positive integers μ_j so that

$$j^{\mu_j} \equiv 1 \pmod{G_1}.$$

Let μ denote their product. Then each g in W satisfies $g^m \equiv \prod_{j=k+t}^{k+2t} j^{s_j} \pmod{G_1}$ for some s_j, and so

$$g^{m\mu} \equiv 1 \pmod{G_1}.$$

Thus W has bounded order.

This brings us to the end of stage (ii) of the proof. We have shown that for each integer $n > k + t$ there is a representation

$$n^{m\mu} = \prod_i R(n_i)^{\varepsilon_i}$$

with $k \leqslant n_i \leqslant 4^{6t^3}(n + k^2)$. Moreover, the value of the exponent $m\mu$ does not depend upon H. However, we cannot give bounds for the μ_j and so for μ. As we tighten our grip upon the exponent of n, the constant c_0 which appears in the statement of the theorem begins to slip away from us.

(iii) To complete our proof we apply this argument with $\Gamma = S = F_p$, a finite field of p elements, but with Q_1 replaced by Q_1/Q_1^p, G_j by G_j/Q_1^p.

Once again S is a field, and for an f which takes values in F_p to vanish on G_1/Q_1^p we must have

$$\psi(E)f(n) = 0 \quad \text{for } k \leqslant n \leqslant H.$$

Here the polynomial $\psi(x)$ is interpreted by considering the coefficients as in the residue class field $\mathbf{Z}/p\mathbf{Z}$. Since as rational integers the b_i have highest common factor 1, $\psi(x)$ will not then vanish identically.

We conclude from Lemma 8 that

$$f(n) = 0 \quad \text{on } \left[0, 2^{-6t^3}H\right].$$

Thus $G_2 \subseteq G_1Q_1^p$ for every prime p.

In particular each integer $n \geqslant k + t$ has a representation

$$n = z^p \prod_j R(r_j)^{\nu_j}$$

with $\nu_j = \pm 1$ and $k \leqslant r_j \leqslant 4^{6t^3}(n + k^2)$. Clearly the primes which appear in a canonical factorization of the fraction z do not exceed

$$\max_{1 \leqslant i \leqslant h} 4^{6t^3}\left(n + k^2 + a_i\right) < c_1 n.$$

If now $m\mu > 1$ and p divides $m\mu$, then

$$n^{p^{-1}m\mu} = z^{m\mu} \prod_j R(r_j)^{\nu_j} = \prod_i R(n_i)^{\varepsilon_i},$$

this time with $k \leqslant n_i \leqslant 4^{6t^3}(c_1 n + k^2)$. Note that if z has a prime factor t which is less than k, then we consider it as a ratio $(k + t)s/(k + t)$.

Arguing inductively we strip off the primes in $m\mu$ to reach

$$n = \prod_i R(n_i)^{\varepsilon_i}$$

with $k \leqslant n_i \leqslant c_1^{\upsilon + 1}$, where υ denotes the total number of prime divisors of $m\mu$. With $c_0 = c_1^{\upsilon + 1}$ the theorem is proved.

Since we do not have a bound for υ, c_0 cannot be computed.

Sets of uniqueness

Let us now adopt the less restrictive condition that an arithmetic function $f(\ )$ be called *additive* if

$$f(ab) = f(a) + f(b)$$

whenever the (positive) integers a and b are coprime, and *completely additive* if this relation holds for all pairs of integers. The homomorphisms which were applied in the earlier part of this paper were thus defined by completely additive arithmetic functions.

A sequence

$$A: a_1 < a_2 < \cdots$$

of positive integers with the property that every real additive arithmetic function which vanished on them also vanished identically, was said by Kátai (1968a) to be a *set of uniqueness*. In particular, he proved (1968b) that if to the sequence

$$P: 3 < 4 < 6 < \cdots < p + 1 < \cdots,$$

where the p are primes, we adjoin finitely many integers then we obtain a set of uniqueness. He conjectured that P itself was a set of uniqueness. This was established to be true by the author, Elliott (1974).

It was proved by Wolke (1978) and Dress and Volkmann (1978) that if a sequence A is a set of uniqueness for an additive arithmetic function then every positive integer has a representation

$$n^h = \prod a_{j_i}^{\varepsilon(j_i)}$$

with $\varepsilon(j_i) = \pm 1$. The h may vary with n. This amounts to a form of Lemma 3 with the additive group of the real numbers as D. Our present method differs in the following regard:

We deal with modules, rather than vector spaces over the rationals as they did, and we localise the integers used in the product representation.

It followed from the author's proof of Kátai's conjecture that (as Wolke, and Dress and Volkmann mentioned) there is a representation

$$n^h = \prod (p_i + 1)^{\varepsilon_i} \tag{5}$$

with the p_i prime and $\varepsilon_i = \pm 1$.

Let

$$M(x) = \max_{1 \leqslant n \leqslant x} |f(x)|, \qquad E(x) = \max_{p \leqslant x} |f(p + 1)|.$$

In a later paper the author (Elliott (1976)) proved that for completely additive functions $f(n)$ there are positive (absolute) constants so that

$$M(x) \leqslant AE(x^B) \tag{6}$$

holds for $x \geqslant 2$. In view of our present Lemma 3 this now shows that the primes in the representation (5) may be restricted to the range $p \leqslant n^B$. Assuming only that $f(\ )$ be additive I established only the weaker result

$$M(x) \leqslant AE(x^B) + AM\big((\log x)^C\big)$$

for some $C > 0$.

That (6) holds for all additive function $f(\ )$ was proved by Wirsing (1980), and he strengthened the representation (5) by restricting the primes p_i to lie in an interval $n < p_i \leqslant n^B$, and having both h and the total number of factors in the product bounded above independently of n.

If P_1 denotes the subgroup of Q_1 which is generated by the $(p_i + 1)$ in particular Wirsing's result shows that Q_1/P_1 has bounded order. For the sequence P this brings us to the end of stage (ii) of the general procedure discussed at the beginning of the present paper.

In order to prove that every integer n has a representation

$$n = \prod_i (p_i + 1)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,$$

it is sufficient (and also necessary) that for each prime q, a completely additive arithmetic function $f(\ )$ with values in the integers $(\bmod q)$ which satisfies $f(p+1) \equiv 0 \pmod q$ for all primes p must also satisfy $f(n) \equiv 0 \pmod q$ for every positive integer n.

Multiplicative functions

An arithmetic function $\phi(n)$ is said to be multiplicative if it satisfies

$$\phi(ab) = \phi(a)\phi(b)$$

for all pairs of positive coprime integers a, b and to be *completely multiplicative* if this relation holds for all positive integers a and b.

We can now state

LEMMA 9. *Let $a_1, a_2, \ldots,$ be a sequence of positive integers. In order that every positive integer may have a representation of the form*

$$n = \prod_{j=1}^{s} a_j^{d_j}$$

for some integers d_j, positive negative or zero, it is necessary and sufficient that every completely multiplicative arithmetic function which is 1 *on the a_j and whose values are roots of unity, be identically* 1.

https://doi.org/10.1017/S1446788700025635 Published online by Cambridge University Press

PROOF. We apply Lemma 5 with $G_2 = G = Q_1$, G_1, the subgroup of Q_1 generated by the a_n, and consider maps into the multiplicative group of roots of unity.

A form of this result would be implicit in Theorem 2 of Dress and Volkmann (1978). There they were interested in what properties a sequence a_j must have in order that one could reconstruct a complex-valued completely multiplicative function $\phi(\ )$ from its values $\phi(a_j)$. In particular $\phi(n)$ was allowed to be sometimes zero. However, the proof which they give is not complete.

Translated into our present circumstances, let V be the subgroups of Q_1 generated by the a_j in Lemma 9. They aim to prove that Q_1/V is trivial by showing that otherwise one can construct a complex-valued multiplicative $\phi(\ )$ which is 1 on the a_j, but not identically 1.

Employing a form of Lemma 3 (see our earlier comments on their method) they prove that every element of Q_1/V has a finite order. By adjoining rational primes to V a larger group V_1 is obtained so that the order of each element in Q_1/V_1 is divisible by some particular prime q. A further group V_2 is now formed by adjoining to V_1 the qth-powers of the rational primes needed to generate Q_1/V_1, and (as they maintain) one obtains a group Q_1/V_2 each of whose non-trivial elements has order q.

Their aim is now to obtain a non-trivial map of Q_1/V_1 into some vector space over the field F_q, and for that they need Q_1/V_2 to be non-trivial. This, however, need not be the case. If, for example, V is generated by the integers at (1) then in the above argument $V = V_1$, with every element of Q_1/V_1 being a qth-power. The construction of V_2 by Dress and Volkmann now gives $Q_1 = V_2$.

One may instead argue as follows. Let G be the group Q_1/V. If for some prime p the group G/G^p is non-trivial then (regarded as vector spaces over F_p) there exists a non-trivial homomorphism of G/G^p into $\mathbf{C}_p$, the multiplicative group of pth roots of unity. We have

$$Q_1 \to Q_1/V \to G/G^p \to \mathbf{C}_p$$

where the first two maps are the natural projections. This defines a non-trivial completely multiplicative function $\phi(n)$ on Q_1 which has the value 1 on V.

Otherwise $G = G^p$ for every prime p. The group G is thus a torsion group which is divisible. Such groups are the direct sum for varying rational primes p, of isomorphic copies of the group $\mathbf{Z}(p^\infty)$ (Kaplansky (1969) Theorem 4). This last is the group of rational numbers (mod 1) which are generated by the fractions whose denominators are powers of the prime p. In particular $\mathbf{Z}(p^\infty)$ is isomorphic to the multiplicative group $\mathbf{C}_p^*$ of roots of unity whose orders are powers of p. This gives

$$Q_1 \to Q_1/V \to \mathbf{Z}(p^\infty) \to \mathbf{C}_p^*$$

where the first map is the natural projection, the second is by means of a projection onto one of the direct summands isomorphic to $\mathbf{Z}(p^\infty)$, and the last is an isomorphism. Once again we obtain a non-trivial multiplicative $\phi(n)$ which is one on V.

Since no such $\phi(\,)$ exists Q_1/V must be trivial, as asserted.

This method of proof is interesting in that it illustrates how much of the structure of Q_1/V is determined by homomorphisms into the additive reals or the finite fields F_p.

In our proof of the (main) theorem maps into the additive real rather than the multiplicative complex numbers were employed, since addition is generally more familiar than multiplication. The steps (i)–(iii) are practical in other examples.

Simultaneous representation

Let $Q_2 = Q_1 \oplus Q_1$ be the direct sum of two copies of the multiplicative group of positive rationals. Let a_n, $n = 1, 2, \ldots$, and b_m, $m = 1, 2, \ldots$, be two infinite sequences of integers, and let G be the subgroup generated by the pairs $a_n \oplus b_n$.

If $f(\,)$ is a homomorphism of Q_2 into (for example) the additive group of the real numbers, then we can decompose it as

$$f(\,) = f_1(\,) + f_2(\,)$$

where

$$f_1(r \oplus s) = f(r \oplus 0), \qquad f_2(r \oplus s) = f(0 \oplus r)$$

for all r and s in Q_1. This naturally defines two maps of Q_1 into $\mathbf{R}$.

The group Q_2/G is now studied by considering those additive functions $f_i(n)$, $i = 1, 2$, which satisfy

$$f_1(a_n) + f_2(b_n) = 0$$

for all n. If these must vanish identically, then to each pair of positive integers m_1, m_2 we can find further integers $k > 0$, $n_i > 0$, $\varepsilon_i = \pm 1$, $i = 1, \ldots, s$, so that (simultaneously)

$$m_1^k = \prod_{i=1}^{s} a_{n_i}^{\varepsilon_i}, \qquad m_2^k = \prod_{i=1}^{s} b_{n_i}^{\varepsilon_i}.$$

The preceding theory may thus be adapted to deal with the simultaneous representation of integers. For example, let $(m_1, 3) = 1$, $(m_2, 5) = 1$ hold. Then we can obtain the representation

$$m_1^k = \prod_{i=1}^{s} (3n_i + 1)^{\varepsilon_i}, \qquad m_2^k = \prod_{i=1}^{s} (5n_i + 2)^{\varepsilon_i}.$$

Since the complications increase, however, we shall furnish the details of such an application on another occasion.

References

D. A. Burgess (1962), 'On character sums and primitive roots', *Proc. London Math. Soc.* **12**, 179–192.
D. A. Burgess (1967), 'On the quadratic character of a polynomial', *J. London Math. Soc.* **42**, 73–80.
H. Davenport (1963), 'Cubic forms in 16 variables', *Proc. Roy. Soc. Ser. A* **272**, 285–303.
F. Dress and B. Volkmann, 'Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives', *C. R. Acad. Sci. Paris Ser. A* **287**, 43–46.
P. D. T. A. Elliott (1979/80), *Probabilistic number theory* I, II (Springer, New York, Heidelberg, Berlin).
P. D. T. A. Elliott (1974), 'A conjecture of Kátai', *Acta Arith.* **26**, 11–20.
P. D. T. A. Elliott (1976), 'On two conjectures of Kátai', *Acta Arith.* **30**, 35–59.
I. Kaplansky (1969), *Infinite abelian groups*, revised edition (University of Michigan Press, Ann Arbor).
I. Kátai (1968a), 'On sets characterising number-theoretical functions', *Acta Arith.* **13** 315–320.
I. Kátai (1968b), 'On sets characterising number-theoretical functions (II), (The set of "prime plus one"*s* is a set of quasi-uniqueness)', *Acta Arith.* **16**, 1–4.
R. C. Vaughan (1981), *The Hardy Littlewood method* (Cambridge University Tract No. 80).
B. van der Waerden (1953), *Modern algebra* (Ungar, New York, 1931).
E. Wirsing (1980), 'Additive functions with restrictive growth on the numbers of the form $p + 1$', *Acta Arith.* **37**, 345–357.
D. Wolke (1978), 'Bemerkungen über Eindeutigkeitsmengen additiver Funktionen', *Elem. Math.* **33**, 14–16.
O. Zariski and P. Samuel, *Commutative algebra* (Van Nostrand, Toronto, London, New York, 1958).

Department of Mathematics
University of Colorado
Boulder, Colorado 80309
U.S.A.