JOURNAL OF ALGEBRA **210,** 194–215 (1998)
ARTICLE NO. JA987527

Algebra of Matrix Arithmetic

Gautami Bhowmik* and Olivier Ramaré†

Department of Mathematics, Université Lille 1, Unité associée au CNRS, URA 751, 59655 Villeneuve d'Ascq Cedex, France

Communicated by Walter Feit

Received November 3, 1997

We study the algebra of the arithmetic of integer matrices. A link is established between the divisor classes of matrices and lattices. The algebra of arithmetical functions of integral matrices is then shown to be isomorphic to an extension of the Hecke algebra, also called a Hall algebra in combinatorics. The dictionary helps translate results from one setting to another. One important application is the study of subgroups of a finite abelian group.

I. INTRODUCTION

Although integral matrices have been intensively studied (see, for instance, [H], [Ne], [N4], [T3]) and some arithmetical notions like GCD and divisibility have been introduced, the set of divisor classes of a given matrix still remains unsatisfactorily understood; in this paper we wish to fill this gap. Let $\mathfrak{M}_r$ be the algebra of $r \times r$ matrices with coefficients in $\mathbb{Z}$. We shall pay special attention to nonsingular matrices, i.e., to Inv_r, the subset of $\mathfrak{M}_r$ consisting of those matrices M for which $\det(M) \neq 0$. The set of invertible elements $\mathscr{U}_r$ (some authors use $GL_r(\mathbb{Z})$ instead), which is the subset of $\mathfrak{M}_r$ consisting of matrices M verifying $\det(M) = \pm 1$, will feature prominently in our discussion. Although we do not do so in this paper, we could as well have worked with singular matrices, the arithmetic of which would be adapted on the lines of [BN].

We recall that if M is in Inv_r, a left divisor class of M is an integral matrix A that is a canonical representative of $A \cdot \mathscr{U}_r$ for which there exists an integral matrix B such that $AB = M$. In particular, we take A in

* E-mail: bhowmik@gat.univ-lille1.fr.
† E-mail: ramare@gat.univ-lille1.fr.

0021-8693/98 $25.00

Hermite Normal Form (HNF). We use the notation $A \mid M$ to indicate divisibility. The set containing (left) divisor classes of M is denoted by $LD(M)$ and is known to be of finite cardinality.

The classical way to study the arithmetic of commutative structures is through the description of ideals of $\mathfrak{M}_r$. This approach is not obviously adapted to noncommutative situations, and in this paper we shall derive information from the action of $\mathfrak{M}_r$ over $\mathbb{Z}^r$. To do so, we choose a basis $\mathscr{B}$ of $\mathbb{Z}^r$ and identify a matrix M with the endomorphism φ_M whose matrix in $\mathscr{B}$ is M. We consider the image $M(\mathbb{Z}^r)$, which depends only on the unimodular class of M, i.e., the HNF of M and its cokernel $G(M) = \mathbb{Z}^r/M(\mathbb{Z}^r)$. (If we wished to study singular matrices as well, we would take only the torsion part of the cokernel.) It is known that $G(M)$ is a finite abelian group independent of the chosen basis, and its invariant factors are the same as that of M.

Notwithstanding partial efforts like those of Hua [H, Chap. 14] or Thompson [T2, T3], in the past matrices have been used only as a tool in the study of finite abelian groups (see, e.g., [B], [Ne, II.21.a]) without any formal connection having been established. Here we prove

THEOREM 1.1. *Let $M \in Inv_r$. The arrow*

$$\Delta\colon LD(M) \to \{\textit{subgroups of } G(M)\},$$
$$A \mapsto A(\mathbb{Z}^r)/M(\mathbb{Z}^r)$$

is one-to-one and order-preserving (i.e., if $A_1 \mid_l A_2$ then $\Delta(A_1) \supset \Delta(A_2)$). Furthermore, $G(A^{-1}M) \cong \Delta(A)$.

As an immediate corollary we get

COROLLARY 1.2. *The number of divisor classes of $M \in Inv_r$ is equal to the number of subgroups of $G(M)$.*

The interpretation of divisor classes in terms of lattices and finite groups has other applications. The left GCD D_l and right multiple M_r of A and B in Inv_r can be defined simply as $D_l(\mathbb{Z}^r) = A(\mathbb{Z}^r) + B(\mathbb{Z}^r)$ and $M_r(\mathbb{Z}^r) = A(\mathbb{Z}^r) \cap B(\mathbb{Z}^r)$. This enables us to give another proof of a recent result of Thompson (see [T1] and [N1] for two other proofs) on the classical lines of Grassman's formula.

COROLLARY 1.3. $G(A) \times G(B) \cong G(D_l) \times G(M_r)$.

As another important application, we determine $\mathrm{ind}(S)$, the index of a matrix S, which is the number of Hermite Normal Forms H having a given Smith Normal Form S. We recall that S is a canonical representative of $\mathscr{U}_r \cdot H \cdot \mathscr{U}_r$.

COROLLARY 1.4. *Let p be a prime number and $\lambda = (\lambda_1, \dots, \lambda_r)$ be a partition. The number of Hermite Normal Forms whose Smith Normal Form is* $\mathrm{diag}(p^{\lambda_r}, \dots, p^{\lambda_1})$ *is given by*

$$\left[\begin{matrix} r \\ \lambda'_1 - \lambda'_2, \lambda'_2 - \lambda'_3, \dots, \lambda'_{\lambda_1} \end{matrix} \right]_p p^{\sum_{i=1}^{\lambda_1 - 1} \lambda'_{i+1}(r - \lambda'_i)},$$

where λ' is the conjugate partition of λ and $[\dots]_p$ is the gaussian multinomial.

We shall see that this index function is the classical homomorphism from an abstract Hecke algebra to $\mathbb{C}$.

It is well known that if G is a finite abelian p-group, there exist positive integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s$ such that G is isomorphic to $\prod_i \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$. The partition $\lambda = (\lambda_1, \dots, \lambda_s)$ is called the type of G (also sometimes called its Segre characteristic). A subgroup H of G has a type μ and a cotype ν, which, by definition, is the type of G/H. Klein ([K]) has shown that there exists a polynomial $g^{\lambda}_{\mu,\nu}$ with integer coefficients such that the number of subgroups of G of type μ and cotype ν is $g^{\lambda}_{\mu,\nu}(p)$. These polynomials are called Hall polynomials. The corresponding notion for matrices is the notion of invariant factors. If $M \in Inv_r$ has a determinant that is a power of a prime p, then $\mathscr{U}_r \cdot M \cdot \mathscr{U}_r$ contains a unique diagonal matrix $\mathrm{diag}(p^{\lambda_r}, \dots, p^{\lambda_1})$ with $\lambda_1 \geq \cdots \geq \lambda_r$. This representative is called the Smith Normal Form of M and is denoted by $\mathrm{SNF}(M)$. As a corollary to Theorem 1.1, we get

COROLLARY 1.5. *Let p be a prime number, let $M \in Inv_r$ be of determinant a power of p, and let μ and ν be partitions of length r. We put* $\mathrm{SNF}(M) = \mathrm{diag}(p^{\lambda_r}, \dots, p^{\lambda_1})$. *Then the number of divisors A of M such that* $\mathrm{SNF}(A) = \mathrm{diag}(p^{\mu_r}, \dots, p^{\mu_1})$ *and* $\mathrm{SNF}(A^{-1}M) = \mathrm{diag}(p^{\nu_r}, \dots, p^{\nu_1})$ *is equal to $g^{\lambda}_{\mu,\nu}(p)$.*

In [T3] Thompson established that the two quantities under consideration are simultaneously nonzero. In the same paper Thompson addresses the following important problem: given three finite abelian groups G, H, and K, what would be the necessary and sufficient conditions in terms of divisibility relations between the invariant factors of these three groups for K to be a subgroup of G with $G/K \cong H$. In the same paper Thompson proves some intricate inequalities necessarily verified by these invariant factors. A necessary and sufficient condition is of course given by the nonvanishing of the corresponding Hall polynomial and in turn by the existence of a rather intricate combinatorial object called a Littlewood–Richardson sequence (hereafter abbreviated as LR-sequence). We shall describe LR-sequences in a way that helps us give simpler proofs for some

of Thompson's results. Note that links between the arithmetic of matrices and that of partitions have been shown earlier in some special situations (see [N2], [B0], [B3], [Ne], and [M]).

In the final part of this paper we interpret arithmetical functions of matrices in the context of divisibility in terms of lattices. A function f: $Inv_r \to \mathbb{C}$ is said to be arithmetical whenever $f(A)$ depends only on the Smith Normal Form of A. This formalization helps us determine the pointwise value of arithmetical functions that are given as a convolution of two simpler functions (for instance, the number of divisors of a given matrix). Pointwise evaluations have been treated in [C] (for the symmetric Euler-ϕ function), in [N2] (for the norm, the t-norms, Euler-ϕ_t functions, and Möbius function), in [RS] and [N3] (for Ramanujan sums), and more recently in [B3] (for the divisor function). A unified account of these results will be found in [BN]. Since these quantities are often difficult to evaluate, it is of interest to have a description that enables us to compare them or to have an idea of their forms. With this aim we shall give formulas for the Dirichlet series of a convolution product of two functions in the context of the Hall algebra (generalizing the result of [BR]).

We shall finally use the divisor class–sublattice correspondence to deal with the algebra of arithmetical functions as defined in [N4]. Note, however, that unlike in [N4], we restrict our attention to $r \times r$ integral matrices with nonzero determinant to get a more complete description. We shall identify in a natural way the "p-component" of this algebra as the completion of the abstract Hecke algebra built over $Inv_{r,p}$ and the unimodular group (see [Kr]), where $Inv_{r,p}$ is the set of $r \times r$ integer matrices whose determinant is a power of p. From this we shall deduce that this p-component is isomorphic to the algebra of formal power series with r indeterminates over $\mathbb{C}$. As a further consequence we shall get

THEOREM 1.6. *The ring of arithmetical functions is isomorphic as a $\mathbb{C}$-algebra to the ring of formal power series in countably many unknowns over $\mathbb{C}$.*

From the above we infer that this ring does not have any zero divisors and that it is factorial (a property shown by Cashwell and Everett (cf. [CE]) while studying the case $r = 1$).

II. NOTATIONS

Let $r \geq 1$ be the dimension.

$$\mathfrak{M}_r = \{\text{integer } r \times r \text{ matrices with coefficients in } \mathbb{Z}\},$$

$$Inv_r = \{M \in \mathfrak{M}_r / \det(M) \neq 0\}, \qquad \mathscr{U}_r = \{M \in \mathfrak{M}_r / \det(M) = \pm 1\}.$$

We need similar notations for the p-primary components when p is a prime number. We will use $\mathfrak{M}_{r,p}$ to denote the set of matrices of determinant $\pm p^\nu$, $\nu \in \mathbb{N}$, and

$$Inv_{r,p} = \{M \in \mathfrak{M}_{r,p} / \det(M) \neq 0\}.$$

We finally put $|M| = |\det M|$.

Any $M \in Inv_r$ is equivalent over $\mathbb{Z}$ to a unique diagonal matrix $\mathrm{diag}(a_i)$, where a_i is a positive integer, and $a_i \mid a_{i+1}$, which we call its Smith Normal form or SNF. We shall also write $\mathrm{SNF}(M) = (a_i)$. If $\mathscr{R}$ is a free $\mathbb{Z}$-module of rank r and $(e_1, \dots, e_r)$ is a basis of $\mathscr{R}$, then $M \in Inv_r$ can be considered as a mapping. If $M(\mathbb{Z}^r) = M(\mathscr{R})$, then the cokernel $G(M) = \mathscr{R}/M(\mathbb{Z}^r)$ is a finite abelian group. It has a unique decomposition of the form $\prod_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$ with $a_i \mid a_{i+1}$. We shall call $\mathrm{diag}(a_i)$ its Smith Normal Form or, when required, we shall call it the SNF of $M(\mathbb{Z}^r)$. It is of course equal to $\mathrm{SNF}(M)$ and does not depend either on $\mathscr{R}$ or on $(e_1, \dots, e_r)$. Where only p-groups are concerned, we have $a_i = p^{\lambda_i}$, and we shall call (λ_{r-i+1}) the type of M (or of $G(M)$ or of $M(\mathbb{Z}^r)$).

A partition is a sequence $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_t, 0, 0, \dots)$ with $\lambda_i \geq \lambda_{i+1}$, $\lambda_i \in \mathbb{N}$. For a partition λ we let λ' denote its conjugate partition and define $n(\lambda) = \sum_i (i-1)\lambda_i$. We associate the following diagram with a partition: build a vertical line (i.e., a column) of λ_1 squares; to the right of this column put a column of λ_2 squares with its upper end level with that of the previous column, and so on. We thus get a triangular shape containing $|\lambda| = \lambda_1 + \lambda_2 + \cdots$ squares.

III. AN INTERPRETATION IN TERMS OF LATTICES

In this section we interpret the divisibility of matrices in terms of lattices and define the left GCD and right LCM in this context.

We denote the category of our objects by $\mathscr{V}(\mathbb{Z}^r)$, the set of all lattices ($:=$ submodules of rank r) of $\mathbb{Z}^r$. If V_1 and V_2 are two elements of $\mathscr{V}(\mathbb{Z}^r)$, then the *morphisms* between V_1 and V_2 are defined as the $\mathbb{Z}$-linear mappings from $\mathbb{Z}^r$ to $\mathbb{Z}^r$ of rank r such that $\varphi(V_1) \subset V_2$. We let Ab_r denote the category of abelian torsion groups that are free products of r cyclic groups equipped with the usual morphisms.

We consider the functor $\mathscr{V}(\mathbb{Z}^r) \to Ab_r$, which associates $\mathbb{Z}^r/V$ with every module V of $\mathscr{V}(\mathbb{Z}^r)$ and transforms a morphism γ from V_1 to V_2 into

$$\gamma^* : \mathbb{Z}^r/V_1 \to \mathbb{Z}^r/V_2$$
$$\bar{x} \mapsto \overline{\gamma(x)}.$$

We have

LEMMA 3.1. *Every morphism* $f: \mathbb{Z}^r/V_1 \to \mathbb{Z}^r/V_2$ *can be written as* $f = \gamma^*$ *with* $\gamma \in Inv_r$ *and* $\gamma(V_1) \subset V_2$. *Moreover,* f *is injective if and only if* $\gamma(V_1) = V_2 \cap \gamma(\mathbb{Z}^r)$.

Proof. Let $(e_1, e_2, \ldots, e_r)$ be a basis of $\mathbb{Z}^r$ such that $(a_1 e_1, \ldots, a_r e_r)$ is a basis of V_1, and let $(\epsilon_1, \epsilon_2, \ldots, \epsilon_r)$ be a basis of $\mathbb{Z}^r$ such that $(b_1 \epsilon_1, \ldots, b_r \epsilon_r)$ is a basis of V_2. We can write

$$f(e_i) = \sum_{j=1}^{r} (m_{ij} + b_j \mathbb{Z}) \epsilon_j \qquad (j = 1, \ldots r)$$

for some choice of m_{ij}. Let N be a large integer parameter. We modify the m_{ij} into m'_{ij} by $m'_{ii} = m_{ii} + b_i N$. If N is taken large enough, the determinant of the map $\gamma(e_i) = \sum_{j=1}^{r} m'_{ij} \epsilon_j$ for $i = 1, \ldots r$ is asymptotic to $N^r b_1 \cdots b_r$ and thus is nonzero if $N \geq N_0$, say. We take $N = N_0$, and verify further that $\overline{\gamma(x)} = f(\bar{x})$. Moreover, $f(0) = 0$, so that $\gamma(V_1) \subset V_2$. ∎

To describe $\mathrm{Hom}(\mathbb{Z}^r, V_1)$ we define $\mathrm{Epi}(V_1, V_2)$ as the subset of $\mathrm{Hom}(V_1, V_2)$ consisting of elements γ such that $\gamma(V_1) = V_2$. We also let $\mathrm{Iso}(V) = \mathrm{Epi}(V, V)$. Every element of $\mathrm{Iso}(V)$ induces an isomorphism on V (since its determinant is ± 1). We have

LEMMA 3.2. *If* $\gamma \in \mathrm{Epi}(\mathbb{Z}^r, V)$ *and* $\psi \in \mathrm{Hom}(\mathbb{Z}^r, V)$ *then there exists* $\kappa \in \mathrm{Hom}(\mathbb{Z}^r, \mathbb{Z}^r)$ *such that* $\psi = \gamma\kappa$.

Proof. For any x in $\mathbb{Z}^r$, $\psi(x)$ is in V. Thus there exists a unique y in $\mathbb{Z}^r$ such that $\gamma(y) = \psi(x)$. ∎

LEMMA 3.3. *Let* $\gamma_0 \in \mathrm{Epi}(\mathbb{Z}^r, V)$. *Then* $\mathrm{Hom}(\mathbb{Z}^r, V) = \gamma_0 \circ \mathrm{Hom}(\mathbb{Z}^r, \mathbb{Z}^r)$.

Proof. One inclusion is clear. For the other let $\mathscr{B}$ be a basis of $\mathbb{Z}^r$ and $\gamma \in \mathrm{Hom}(\mathbb{Z}^r, V)$. Then $\gamma(\mathscr{B})$ can be expressed in terms of $\gamma_0(\mathscr{B})$. Hence the result. ∎

Let us fix a basis $\mathscr{B} = (e_1, e_2, \ldots, e_r)$ of $\mathbb{Z}^r$. With any $M \in \mathfrak{M}_r$ we associate the linear mapping φ_M of $\mathbb{Z}^r$, whose matrix is M in $\mathscr{B}$ and $M(\mathbb{Z}^r) = \varphi_M(\mathbb{Z}^r)$. Whenever convenient, we shall write M instead of φ_M. We also define $G(M) = \mathbb{Z}^r/M(\mathbb{Z}^r)$. It is well known that $G(M)$ is in one-to-one correspondence with the SNF of M.

We now define divisors:

Left Divisors: V_1 is a left divisor of V_2 iff $V_2 \subset V_1$. The set of left divisors of V will be denoted by $\mathrm{LD}(V)$. Note that $\mathrm{LD}(V)$ is naturally ordered by inclusion.

Weak Complementary Divisors: Let V_1 and V_2 be two submodules of $\mathbb{Z}^r$. We say that $\mathscr{U}_r \cdot V_1$ is a weak complementary divisor of V_2 if there exists $\gamma \in \mathrm{Epi}(V_1, V_2)$. Such a definition would make sense only if $V_1 = u(V_1')$ for $u \in \mathscr{U}_r$, and if for a morphism γ of $\mathrm{Epi}(V_1, V_2)$ the map belongs to $\mathrm{Epi}(V_1', V_2)$. The set of weak complementary divisors of V will be denoted by $\mathrm{WCD}(V)$.

Furthermore, for $M \in Inv_r$, we let $\mathrm{LD}(M)$ be the set of left divisor classes of M. This set is naturally ordered by divisibility. We now describe the links between these three sets of "divisors." To this end we define the three following arrows:

$$\Theta: (\mathrm{LD}(M), |) \to (\mathrm{LD}(M(\mathbb{Z}^r)), \supset),$$
$$M_1 \cdot \mathscr{U}_r \mapsto M_1 \mathbb{Z}^r,$$
$$\tilde{\Theta}: (\mathrm{LD}(M(\mathbb{Z}^r)), \supset) \to (\mathrm{LD}(M), |),$$
$$V_1 \mapsto M_1 \cdot \mathscr{U}_r,$$

and

$$\Psi: \mathrm{LD}(M) \to \mathrm{WCD}(M(\mathbb{Z}^r)),$$
$$M_1 \cdot \mathscr{U}_r \mapsto \mathscr{U}_r \cdot M_1^{-1} M(\mathbb{Z}^r),$$

where M_1 is the matrix in $\mathscr{B}$ of any $u \in \mathrm{Epi}(\mathbb{Z}^r, V_1)$. We show that these arrows are well defined. This is clearly so for Θ and Ψ. We note also that Ψ depends only on the HNF of M and that $\tilde{\Theta}$ is well defined by Lemma 3.3.

We check that $\Theta \circ \tilde{\Theta} = \mathrm{Id}_{\mathrm{LD}(M)}$ and $\tilde{\Theta} \circ \Theta = \mathrm{Id}_{\mathrm{LD}(M(\mathbb{Z}^r))}$, so that $\tilde{\Theta} = \Theta^{-1}$. We show that Ψ is a surjection by taking an element of $\mathrm{WCD}(M(\mathbb{Z}^r))$, $\mathscr{U}_r \cdot V_2$, and one of $\mathrm{Epi}(V_2, M(\mathbb{Z}^r))$ and then letting $V_1 = \gamma(\mathbb{Z}^r) \supset M(\mathbb{Z}^r)$. We then have $\gamma^{-1}\varphi_M \mathbb{Z}^r = V_2$, as required.

Finally, we prove that Θ and $\tilde{\Theta}$ are order-preserving. Let $M_1 | M_2 | M$. Then $M_2 = M_1 N$ for some $N \in Inv_r$, which implies $M_2(\mathbb{Z}^r) \subset M_1(\mathbb{Z}^r)$, as required. Conversely, if $M_1(\mathbb{Z}^r) \supset M_2(\mathbb{Z}^r)$, then $M_1 \mid M_2$ by the sheer fact that the mapping $\tilde{\Theta}$ associated with M_2 is well defined.

We have thus proved a sharper form of Theorem 1.1, i.e., *Θ and $\tilde{\Theta}$ are one-to-one and order-preserving and are inverses of one another. Furthermore, Ψ is a surjection.*

We will henceforth use Θ^{-1} instead of $\tilde{\Theta}$. In fact, a bit more can be said, since Ψ actually identifies the SNF of the complementary divisor.

THEOREM 3.4. *Let V_1 be a left divisor of V and choose V_2 so that $\Psi\Theta^{-1}(V_1) = \mathscr{U}_r \cdot V_2$. Then there exists $\gamma \in \mathrm{Epi}(V_2, V) \cap \mathrm{Epi}(\mathbb{Z}^r, V_1)$. For any such choice (V_2, γ), we have an exact sequence,*

$$0 \to \mathbb{Z}^r / V_2 \xrightarrow{\gamma^*} \mathbb{Z}^r / V \to \mathbb{Z}^r / V_1 \to 0.$$

Proof. With obvious notations we have $\mathscr{U}_r \cdot V_2 = \mathscr{U}_r \cdot M_1^{-1} M \mathbb{Z}^r$. Thus $V_2 = u \circ M_1^{-1} M \mathbb{Z}^r$ and $\gamma = M_1 \circ u^{-1}$ is a point of $\mathrm{Epi}(V_2, V)$ such that $\gamma(\mathbb{Z}^r) = V_1$. Thus γ^* is injective and $\gamma^*(\mathbb{Z}^r/V_2) = V_1/V$, which proves the exactness of the above sequence. ∎

Theorem 3.4 tells us that V_1/V is isomorphic to the SNF of the complementary divisor.

COROLLARY 3.5. *The number of divisor classes M_1 of M such that* $\mathrm{SNF}(M_1) = S_1$ *and* $\mathrm{SNF}(M_1^{-1}M) = S_2$ *is equal to the number of subgroups* Γ *of* $G(M)$ *such that* $\Gamma \cong G(S_2)$ *and* $G(M)/\Gamma \cong G(S_1)$.

Furthermore, we have Corollary 1.2.

We now consider lattices V verifying $\varphi(V) \subset V$ for every $\varphi \in \mathrm{Hom}(\mathbb{Z}^r, \mathbb{Z}^r)$. It is easily seen that the lattices $m\mathbb{Z}^r$ verify this property and that they are the only ones to do so. Furthermore, given any lattice V, we have $V \supset \det(V)\mathbb{Z}^r$ (corresponding to the fact that any algebraic extension of $\mathbb{Q}$ is contained in a Galois extension). This property extends to several lattices, so that the intersection of two lattices is yet another lattice. We shall call such lattices diagonal lattices whose mere existence is enough to prove Corollary 1.4.

Proof of Corollary 1.4. For this proof we need the material presented in Section IV. Let $m = \gamma_1 + \cdots + \gamma_r$. The HNF's we are looking for are the lattices L contained in $p^m\mathbb{Z}^r$ whose cotypes are $\nu = (\gamma_r, \ldots, \gamma_1)$. It is thus the sum over all possible types α of $g_{\alpha,\nu}^{(m,\ldots,m)}(p)$ (cf. Section IV). The first part of the theorem follows readily. To get the precise expression, we first use the fact that $g_{\mu,\nu}^{\lambda} = g_{\nu,\mu}^{\lambda}$, and then use Birkhoff's result (Proposition 4.5). ∎

We note, finally, that this index is an important quantity in Hecke algebras. Following Krieg [Kr], it would already have been possible to show that the index is a polynomial in p.

One obtains that the index is a homomorphism from $\mathscr{H}_r$ to $\mathbb{Z}$, and that $\mathscr{H}_r$ is a polynomial algebra generated by some $T_{r,0}, \ldots, T_{r,r}$ for which we know that $\mathrm{ind}(T_{r,j}) = \begin{bmatrix} r \\ j \end{bmatrix}_p$. (See Remark 7.3.b, Proposition 7.2 and Theorem 8.1 of Chapter 5 as well as Corollary 4.5 of Chapter 1 of [Kr].) Obtaining the degree of the polynomial by this approach does not seem to be easy.

We shall give definitions of left GCD and right LCM in terms of lattices.

- Given A and B in Inv_r, there exists a D_l, unique up to multiplication on the right by a unimodular matrix, such that $A(\mathbb{Z}^r) + B(\mathbb{Z}^r) = D_l(\mathbb{Z}^r)$ (which is, by the way, the analogue of the definition given in [H, Theorem 9.7, Chap. 14]).

• Similarly, $A(\mathbb{Z}^r) \cap B(\mathbb{Z}^r) = M_r(\mathbb{Z}^r)$, where M_r is a right common multiple (this intersection is yet another lattice by virtue of the remark following Corollary 3.5). Note that we have the exact sequence

$$\begin{array}{ccccccc} 0 & \to & G(M_r) & \to & G(A) \times G(B) & \to & G(D_l) \to 0 \\ & & x & \mapsto & (x, -x) & & \\ & & & & (x, y) & \mapsto & x + y, \end{array}$$

which finally yields Corollary 1.3; although first we need two auxiliary results on the ranks of finite abelian groups.

LEMMA 3.6. *If H is a subgroup of a finite abelian group G, there exists H_0, a direct factor of G, of the same rank as H, such that $H \subset H_0 \subset G$.*

Proof. We lift the situation in $\mathbb{Z}^r$ where the rank of G is r. We take $V \subset \mathbb{Z}^r$ such that $\mathbb{Z}^r/V \cong G$ and denote this surjection by s. Now there exists a submodule W of $\mathbb{Z}^r$ such that $V \subset W \subset \mathbb{Z}^r$ and $s(W) = H$ with $\operatorname{rank}(W) = \operatorname{rank}(H)$. We can find a basis $(e_1, \ldots, e_r)$ of $\mathbb{Z}^r$ for which there exist integers $a_1, \ldots, a_r$ such that $W = \sum_{i=1}^r \mathbb{Z} \cdot a_i e_i$. With a suitable reordering of the e_i-s we could assume that for $i \le t$, t being the rank of H, $a_i \neq 0$ and that $a_{t+1} = \cdots = a_r = 0$. We set $W_0 = \sum_{i=1}^t \mathbb{Z} \cdot e_i$ and $W_1 = \sum_{i=t+1}^r \mathbb{Z} \cdot e_i$, so that $\mathbb{Z}^r = W_1 \oplus W_0$ and $W \subset W_0$. From this we infer that $G = s(W_1) + s(W_0)$. To prove that this sum is direct, we simply show that $(W_1 + V) \cap (W_0 + V) = V$. Let $w_1 = w_0 + v$. Then $v = v_1 + v_0$. This gives $w_1 - v_1 = w_0 + v_0 = 0$. Hence $w_1 = v_1 \in V$. Now $H_0 = s(W_0)$ satisfies our requirement. ∎

LEMMA 3.7. *Let G, H, K be finite abelian groups with* $\operatorname{rank}(G) \ge \operatorname{rank}(H) + \operatorname{rank}(K)$. *If there exists an exact sequence*

$$0 \to H \xrightarrow{f} G \xrightarrow{g} K \to 0,$$

then $G \cong H \times K$.

Proof. By Lemma 3.6 we can write $G = H_0 \oplus H$, where $H_0 \supset f(H)$ and is of the same rank as H. With obvious notations, let $(g(k_1^1 + k_0^1), \ldots, g(k_1^s + k_0^s))$ be a basis of K. But $(k_1^1, \ldots, k_1^s)$ generates H_1, for the cardinality of the subgroup of H_1 generated by the above elements is the cardinality of K and hence of H_1. Let H_2 be generated by $\langle k_1^1 + k_0^1, \ldots, k_1^s + k_0^s \rangle$. We check that $H_2 + H_0 = G$.

To prove that the above sum is direct, we use the fact that

$$\dim(H_2/pG) + \dim(H_0/pG) \le \dim(G/pG),$$

which gives $H_2 \cap H_0 = \{0\}$. Thus $H_2 \oplus H_0 = G$. By definition $H_2 \cong K$. Hence $g(H_0) = 0$, i.e., $H_0 = \operatorname{Ker} g = f(H)$. ∎

Proof of Corollary 1.3. We notice that D_l is a GCD of A and B if and only if pD_l is a GCD of pA and pB. The same is true for LCM. We can thus assume the ranks of both $G(A)$ and $G(B)$ to be equal to r. Since the ranks of $G(D_l)$ and $G(M_r)$ are at most r, the conclusion follows. ∎

We note that other proofs of Corollary 1.3 can be found in [T1] and [N1], and that by duality we also obtain $G(A) \times G(B) \cong G(D_r) \times G(M_l)$.

IV. PARTITIONS AND MATRICES

Throughout this section p is a fixed prime number. We study some links between partitions and matrices and start with a description of the LR-sequence of a subgroup H of an abelian p-group G. By the structure theorem of finite abelian groups (which can easily be derived from the study above), G is isomorphic to a group.

$$\mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_r}\mathbb{Z} \qquad (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r).$$

Following [K] and [M], we define the *type* of G as being the partition $\lambda(G) = (\lambda_1, \ldots, \lambda_r)$. Given a subgroup H of G, we have access to its type $\lambda(H)$ and to its cotype $\lambda(G/H)$. Further invariants are obtained by taking $\lambda(G/p^iH)$ for $i \geq 0$.

We now need to recall the definition of a LR-sequence. A LR-sequence of type $(\mu, \nu; \lambda)$ is an increasing sequence $(\lambda^{(1)}, \ldots, \lambda^{(s)})$ of partitions with $\lambda^{(1)} = \mu$ and $\lambda^{(s)} = \lambda$. A third batch of properties involving ν is also imposed. To explain it we build the diagram associated with $\lambda^{(1)}$ (cf. Section II) and write 0 over all of the squares. On top of this diagram, put the one for $\lambda^{(2)}$, with the upper left corners of the two diagrams coinciding. Write 1 over the new squares created. Continue in this way with $\lambda^{(3)}, \ldots, \lambda^{(s)}$. We end up with a diagram representing $\lambda = \lambda^{(s)}$, where the squares are numbered 0 to $s - 1$. We assume the following properties to hold true:

(i) When a horizontal line (i.e., a row) is read from left to right, the symbols are weakly increasing.

(ii) When a vertical line (i.e., a column) is read from top to bottom, starting after the last 0, the symbols (if any) are strictly increasing.

(iii) For any $i \geq 1$ and any $k \geq 1$, the number of symbols in the last k columns (starting from the left) is not less than the number of symbols $i + 1$.

(iv) For any $i \geq 1$, the number of symbols i in the whole diagram is ν'_i.

As a useful additional property, one checks that

(v) The kth row (starting from the top) contains some or all of the symbols $0, 1, \dots, k$.

Given such a diagram, its north is the top of the page, its east is the right-hand side of the page, and so on. Here is an example of an LR-sequence of type $((3,2,1),(6,4,3,1);(7,6,6,2))$:

0	0	0	1
0	0	1	2
0	0	2	
1	1	3	
2	3	4	
3	4	5	
6			

The LR-sequence itself is the sequence of partitions

$$((3,3,1),(4,4,2,1),(5,4,3,2),(6,5,4,2),$$
$$(6,6,5,2),(6,6,6,2),(7,6,6,2)).$$

We define a *string* of length k as being a line linking symbols $k, k-1, \dots, 1$, with exactly one of these symbols, each segment of this line being oriented between north and northeast. We now have

LEMMA 4.1. *Given a LR-sequence of type* $(\mu, \nu; \lambda)$, *it is possible to build* ν_1' *strings such that each symbol* ≥ 1 *belongs to a string and that two distinct strings do not intersect*.

Proof. We prove this lemma by recursion on the highest symbol k. For $k = 1$, it is trivial. Let us suppose our strings to be built until the symbol k, and let us add the symbol $k+1$. Take the symbol $k+1$, which is the most east, say square S. Then there exists a symbol k north and east of S by property (iii). Such a symbol is forcibly north of S by (i) and (ii). We take the easternmost of such symbols. We continue in a similar fashion. ∎

Green (cf. [G]) has shown that the sequence

$$S(H) = (\lambda(G/H), \lambda(G/pH), \dots, \lambda(G/p^sH) = \lambda(G))$$

for a large enough s is a LR-sequence of type $(\lambda(H), \lambda(G/H); \lambda(G))$. We shall count subgroups according to their LR-sequence. It would be interesting to describe such classes. In this direction we have

CONJECTURE 4.2. Let p be a prime number. Let G be a finite abelian p-group and H and K be two of its subgroups. Then there exists an automorphism σ of G such that $\sigma(H) = K$ if and only if H and K have the same LR-sequence.

(Note that in the Appendix we prove this conjecture for some special cases.)

We recall the following theorem announced by P. Hall in the 1950s (it was probably already stated by Frobenius in the beginning of the century) and proved by T. Klein in 1969 [K].

THEOREM 4.3 (T. Klein). *Let p be a prime number. Let G be a finite abelian p-group of type λ. The number of subgroups of G having a given LR-sequence and being of type μ and cotype ν is a monic polynomial in p with integer coefficients and of degree $n(\lambda) - n(\mu) - n(\nu)$.*

Summing over all possible LR-sequences having a fixed type μ and a fixed cotype ν tells us that the number of subgroups of G having type μ and cotype ν is a polynomial in p, which we denote by $g^{\lambda}_{\mu,\nu}(p)$ of degree $n(\lambda) - n(\mu) - n(\nu)$, and the leading coefficient of which is $c^{\lambda}_{\mu,\nu}$, the number of LR-sequences of type μ and cotype ν. Summing over all possible types and cotypes and recalling Corollary 3.5, we get that the number of divisors of a matrix $\in Inv_{r,p}$ is a polynomial in p, a fact that is proved in a very short way in [B3].

Note: In [T3] Thompson also considers LR-sequences. However, the reader should be aware of the fact that his definition is not compatible with McDonald's or with ours; what Thompson calls an LR-sequence is what we call the type of an LR-sequence, i.e., the triple (λ, μ, ν) up to some reordering. There might be several LR-sequences having the same type.

Having described LR-sequences and their relations with subgroups, we turn toward their use. The concept of strings will turn out to be helpful. We present a very simple proof of an inequality relating the invariant factors of A, B, and $C = AB$ [T2]. We denote these factors by $s_r(M) \mid s_{r-1}(M) \mid \cdots \mid s_1(M)$.

PROPOSITION 4.4. *Let $C = AB$, where A and B are $r \times r$ integer nonsingular matrices. Then*

$$s_{l_1}(C)s_{l_2}(C)\cdots s_{l_t}(C) \mid s_{i_1}(A)s_{i_2}(A)\cdots s_{i_t}(A)s_{j_1}(B)s_{j_2}(B)\cdots s_{j_t}(B)$$

whenever

$$i_1 < \cdots < i_t, \quad j_1 < \cdots < j_t, \quad l_m = i_m + j_m - m, \quad 1 \le m \le t.$$

Proof. It is enough to assume that the determinant of C is a power of a prime p. Let $\lambda = \lambda(G(C))$, $\mu = \lambda(G(B))$, and $\nu = \lambda(G(C))$ be the associated partitions. Let $\theta_m = \lambda_{i_m + j_m - m} - \mu_m$. We will prove

$$\sum_{m=1}^{t} \nu_{j_m} \ge \sum_{m=1}^{t} \theta_m.$$

The case $t = 1$ is obvious. For $t = 2$, we consider the θ_1th nonzero element in column λ_{i_1} and the $(j_1 - 1)$ elements to the right of it in the same row. Let these j_1 elements comprise what we call sr_1 (subrow 1). We similarly construct sr_2 with $(j_2 - 1)$ elements.

Let k_1 elements of sr_2 be included in the strings passing through the elements of sr_1. By definition, the elements of sr_1 are at least equal to θ_1. We let the minimum value be $\theta_1 + u_1$. Thus $\nu_{j_1} = \theta_1 + u_1$, $u_1 \ge 0$. Now there are $(j_2 - 1 - k_1)$ elements of sr_2 that have not been counted in these strings and which, therefore, give at least $(j_2 - 1 - k_1)$ strings of length at least θ_2. For $0 \le k_1 < j_1$, we already have $j_2 - j_1$ strings of length at least θ_2, and hence $\nu_{j_2} \ge \theta_2$.

For $k_1 = j_1$, we consider the column representing λ_{i_1}. Since a string passing through the λ_{i_1}th column into sr_2 can utilize at most $(\theta_1 + u_1) - \theta_2$ elements of the column, there is an element at least $\theta_2 - u_1$ on this column, which makes up for the missing string, and we have

$$\nu_{j_2} \ge \theta_2 - u_1.$$

We now use induction on t. Let $\nu_{j_n} = \theta_n - u_{n-1} + u_n$ for $1 \le n \le t$. For $n = t + 1$, we use the same reasoning as above to find, in the worst case (i.e., when $k_t = j_t - t$), one additional string of length $\theta_{t+1} - u_t$, given by an element of at least this value, which can be found on the column representing λ_{i_t}. Thus

$$\nu_{j_{t+1}} \ge \theta_{t+1} - u_t,$$

which concludes the recursion. ∎

In fact, the condition satisfied by the indices in Proposition 4.4 can be generalized, as was done by Thompson [T3]. We need the concept of a *row LR-sequence*, to be differentiated from the (column) LR that we have used up to now. To the best of our understanding, the definition of a row LR-sequence can be drastically simplified from that of Thompson's [T3] which we do here.

DEFINITION. The sequence of increasing partitions $(a^{(0)}, a^{(1)}, \ldots, a^{(s)})$ is a row LR-sequence of type $(\tilde{a}, \tilde{b}, \tilde{c})$ if and only if the sequence of conjugate partitions $(a^{(0)'}, a^{(1)'}, \ldots, a^{(s)'})$ is a column LR-sequence of type (a', b', c'), where $\tilde{n}$ denotes the conjugate partition of n written in increasing order.

Note that the diagram of a row LR-sequence $(a^{(0)}, a^{(1)}, \ldots, a^{(s)})$ and a column LR-sequence $(a^{(0)'}, a^{(1)'}, \ldots, a^{(s)'})$ are the same; their types are mutual conjugates.

EXAMPLE. The column LR-sequence of the last example is a row LR-sequence of type (a, b, c), with $a = (2, 2, 3)$, $b = (1, 1, 2, 3, 3, 4)$, and $c = (1, 3, 3, 3, 3, 4, 4)$.

Thompson's proof for the condition of divisibility in terms of row and column LR-sequences is very long, and we believe that it can be simplified along the lines of the proof of Proposition 4.4.

In 1933 G. Birkhoff had already established a partial result in the direction of Theorem 4.3, and his result (cf. [B]) has the advantage that the involved polynomials are more explicit. His formulation is rather complicated, and we state his result in the form given in [Bu].

PROPOSITION 4.5 (G. Birkhoff). *Let G be a finite abelian p-group of type λ, and let ν be the type of a subgroup of G. The number of subgroups of G having type ν is given by*

$$\prod_{i \geq 1} p^{\nu'_{i+1}(\lambda'_i - \nu'_i)} \begin{bmatrix} \lambda'_i - \nu'_{i+1} \\ \nu'_i - \nu'_{i+1} \end{bmatrix}_p,$$

where $[\ldots]_p$ is the gaussian polynomial.

Using Corollary 1.2 together with the above proposition, we get an explicit expression for the number of divisors of an integer matrix. In [B3], the first named author has given another way of evaluating this function. The proof is short and thus gives a simple method of obtaining the total number of subgroups of a finite abelian group (in fact, the number of subgroups having a given cardinality is also obtained).

V. THE STRUCTURE OF THE ALGEBRA OF ARITHMETICAL FUNCTIONS

The value of an arithmetical function is invariant on matrices A,

$$\begin{pmatrix} 0 & 0 \\ 0 & A \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}.$$

Furthermore, this value is the same on all matrices equivalent to A. Thus we can confine our attention to nonsingular matrices. We consider the set of functions that depend only on the double cosets, i.e.,

$$\hat{\mathscr{H}}_r = \{f : \mathscr{U}_r \backslash Inv_r / \mathscr{U}_r \to \mathbb{C}\}.$$

Alternatively, $\hat{\mathscr{H}}_r$ can be seen as the set of functions $Inv_r \to \mathbb{C}$ that depend only on the SNF or as the set of formal infinite linear combinations of double cosets. $(\hat{\mathscr{H}}_r, +, \cdot)$ is, of course, a vector space over $\mathbb{C}$.

The convolution product [N4] over all divisor classes H of S is given by

$$(f \star g)(S) = \sum_{H \mid S} f(H) g(SH^{-1}),$$

which we write as

$$(f \star g)(S) = \sum_{S_1, S_2 \text{ in SNF}} f(S_1) g(S_2) \alpha(S_1, S_2; S),$$

where the "weight" $\alpha(S_1, S_2; S)$ is the number of H in HNF that divide S and whose SNF is S_1, and such that the SNF of $H^{-1}S$ is S_2. With this product $(\hat{\mathscr{H}}_r, +, \star, \cdot)$ is a commutative $\mathbb{C}$-algebra.

We retrace the definition of this product in the context of an abstract Hecke algebra $\mathscr{H}_r$. Since $(GL_r(\mathbb{Q}), \mathscr{U}_r)$ is a Hecke pair (see [Kr]), we simply have a product over the set

$$\mathscr{H}_r = \left\{ f \in \hat{\mathscr{H}}_r / f(S) = 0 \text{ except in finitely many points} \right\}.$$

The product is defined as follows. Let

$$\mathscr{U}_r S \mathscr{U}_r = \bigcup_{\mu=1}^{d_l(S)} \mathscr{U}_r H_\mu \qquad \text{disjoint with } d_l(S) = \#\mathscr{U}_r \backslash \mathscr{U}_r S \mathscr{U}_r$$

and

$$\mathscr{U}_r T \mathscr{U}_r = \bigcup_{\nu=1}^{d_r(T)} L_\nu \mathscr{U}_r \qquad \text{disjoint with } d_r(T) = \#\mathscr{U}_r T \mathscr{U}_r / \mathscr{U}_r.$$

Note that $d_r(S) = d_l(S)$ because of the transposition. It is the number of HNF of SNF S and is denoted by $\mathrm{ind}(S)$ ([Kr], p. 11). We have

$$(\mathscr{U}_r S \mathscr{U}_r) \cdot (\mathscr{U}_r T \mathscr{U}_r) = \sum_{R \in \mathscr{U}_r \backslash \mathscr{U}_r S \mathscr{U}_r T \mathscr{U}_r / \mathscr{U}_r} \alpha(S, T; R) \mathscr{U}_r R \mathscr{U}_r,$$

where

$$\begin{aligned} \alpha(S, T; R) &= \#\{(\mu, \nu) / H_\mu L_\nu \in \mathscr{U}_r R\} \\ &= \#\left\{\mathscr{U}_r \tilde{L} / \mathscr{U}_r \tilde{L} \subset \mathscr{U}_r T \mathscr{U}_r, R\tilde{L}^{-1} \in \mathscr{U}_r S \mathscr{U}_r\right\}, \end{aligned}$$

and this last expression is exactly how we have defined α earlier, so that $\mathscr{H}_r$ is a subalgebra of $\hat{\mathscr{H}}_r$.

The convolution product of arithmetical functions then gives a *natural definition* for the Hecke product on $\mathscr{H}_r$. We could use this definition to prove, for example, the associativity of the Hecke product, an otherwise difficult exercise. On the other hand, this correspondence helps us to prove below that $\hat{\mathscr{H}}_r$ is factorial.

When p is a prime number, we define the primary component $\mathscr{H}_{r,p}$ by

$$\mathscr{H}_{r,p} = \{f: \mathscr{U}_r \setminus Inv_{r,p} / \mathscr{U}_r \to \mathbb{C}, / f(S) = 0 \text{ except in finitely many points}\}.$$

In [Kr], it is shown that $\mathscr{H}_{r,p}$ is isomorphic as a $\mathbb{C}$-algebra to $\mathbb{C}[X_1, \ldots, X_r]$ and that $\mathscr{H}_r$ is isomorphic to the tensor product of the $\mathscr{H}_{r,p}$'s. Defining $\hat{\mathscr{H}}_{r,p}$ in a similar way, we thus see that $\hat{\mathscr{H}}_{r,p}$ is isomorphic as a $\mathbb{C}$-algebra to the algebra of formal power series in r variables, which we denote by $\mathbb{C}[[X_1, \ldots, X_r]]$, from which we deduce that $\hat{\mathscr{H}}_{r,p}$ is a local noetherian factorial ring with no zero divisors. As for $\hat{\mathscr{H}}_r$, we see that it is isomorphic to the ring of formal power series in countably many unknowns $\mathbb{C}[[X_{i,p}$, $1 \le i \le r$, p prime]]. The factoriality of this latter ring has been shown by Cashwell and Everett in 1959 (cf. [CE]).

To prove Theorem 1.6 it is useful to introduce a norm over $\hat{\mathscr{H}}_r$. For any nonzero f in $\hat{\mathscr{H}}_r$, put

$$\|f\| = \sup\{|M|^{-1}, \text{ for } M \in Inv_r, f(M) \neq 0\}$$

and extend it by $\|0\| = 0$. We then verify that

$$\|f + g\| \le \max(\|f\|, \|g\|), \quad \|f \star g\| \le \|f\| \, \|g\|, \quad \|f\| < 1 \text{ iff } f(Id) = 0.$$

It is then a routine matter to identify the invertible elements: denoting by η the function defined by $\eta(Id) = 1$ and $\eta(M) = 0$ whenever $|M| > 1$, we check that $\eta - g$ is invertible if and only if $\|g\| < 1$, which is obtained in another way in [N4, Theorem 3.12].

VI. APPLICATION: ZETA FUNCTION OF THE CONVOLUTION PRODUCT

The interpretation of divisor classes in terms of lattices has another important corollary, which is that the primary component $\mathscr{H}_{r,p}$ of $\mathscr{H}_r$ is isomorphic to the Hall algebra (see [M]). It is interesting to realize that when studied from an algebraical point of view this algebra is called a Hecke algebra, and when studied from a combinatorial viewpoint it is called a Hall algebra, although often there is not much interaction between researchers in these two areas. Here we indicate an application of the isomorphism of algebras.

If we wish to associate a zeta function with the convolution product of arithmetical functions mentioned in Section V, we realize that the zeta function is not a simple product of those of the components of the convolution. Because of the sublattices involved, there is a weight attached that is the sum of $g^{\lambda}_{\mu,\nu}(p)$, the Hall polynomials mentioned in Section IV. From the foregoing discussions we find that this weight is exactly the sum of coefficients of the Hecke product of Section V, $\alpha(S_1, S_2; S)$, where S_1 is of type μ, S_2 is of type ν, and S is of type λ. More precisely, we have

$$\begin{aligned} Z^{(r)}(\chi_1 \star \chi_2, s) &= \sum_{SSNF} \frac{\chi_1 \star \chi_2(S)}{|S|^s} \\ &= \sum_{S_1, S_2\ SNF} \frac{\chi_1(S_1)\chi_2(S_2)}{|S_1|^s |S_2|^s} \sum_{S\ SNF} \alpha(S_1, S_2; S) \\ &= \sum_{S_1, S_2\ SNF} \frac{\chi_1(S_1)\chi_2(S_2)}{|S_1|^s |S_2|^s} \sum g^{\lambda}_{\mu,\nu}(p). \end{aligned}$$

To determine $Z^{(r)}(\chi_1 \star \chi_2, s)$ in the two-dimensional case, we have computed the constant $\alpha(S_1, S_2; S)$. Thus $g^{\lambda}_{\mu,\nu}(p)$ for $\mu = (m+k, k)$, $\nu = (n+l, l)$, and $\lambda = (t+m+k+l, k+l+n-t)$ is known, and we have

$$g^{\lambda}_{\mu,\nu}(p) = \begin{cases} p^n(1+1/p) & \text{if } t = 0,\ m = n, \\ p^n & \text{if } t = 0,\ m \neq n, \\ p^{n-t}(1-1/p) & \text{if } 0 < t < n-m, \\ p^m & \text{if } t = n-m \neq 0, \end{cases}$$

[BR, Proposition 1]. However, a general result of this kind is not yet accessible.

The understanding of this zeta function should throw light on the Hall algebra. In particular, if we consider both χ_1 and χ_2 to be the constant function $\mathbb{1}$ ($\mathbb{1}(M) = 1$ for all M), then the zeta function associated has the easier formulation,

$$Z^{(r)}(\mathbb{1} \star \mathbb{1}, s) = \sum \frac{g^{\lambda}_{\mu,\nu}(p)}{|S|^s},$$

about which some information is already available (for example, in [BW]).

APPENDIX: ENDOMORPHISMS OF $G(M)$

This appendix provides some evidence in support of our belief that for two subgroups H and K of a finite abelian p-group, there exists an automorphism σ such that $\sigma(H) = K$ if and only if H and K have the same LR-sequence (Conjecture 4.2). A step toward understanding this situation is the study of the automorphisms of G. We define an invariant $\rho(y)$ of an element y of G such that $\rho(y) = \rho(z)$ if and only if there exists an automorphism f of G such that $f(y) = z$. This characterization, in turn, reveals part of the structure of G as a module over $HG(M)$, its ring of endomorphisms, and enables us to prove the above conjecture when H is an $HG(M)$-submodule of G (in this case the proof of the conjecture reduces to showing that no two distinct $HG(M)$-submodules of G have the same LR-sequence).

Consider the set of classes of matrices T such that $TM\mathbb{Z}^r = MH\mathbb{Z}^r$ for some $H \in \mathfrak{M}_r$, i.e., such that $M^{-1}TM \in \mathfrak{M}_r$. If T_1 and T_2 are congruent modulo M and if T_1 is a homomorphism, then so is T_2. Note that we have a multiplication over $HG(M)$ induced by composition, so that $HG(M)$ is a ring with unity. We first describe it through coordinates. Let us take M in the form $\operatorname{diag}(p^{\bar{\lambda}_i})$, where $\bar{\lambda}_1 \le \bar{\lambda}_2 \cdots \le \bar{\lambda}_r$. Then $T = (t_{i,j})$ is a homomorphism if and only if

$$t_{i,j} \equiv 0 \left[p^{\bar{\lambda}_j - \bar{\lambda}_i} \right] \qquad (j < i).$$

Note also that $t_{i,j}$ is to be taken modulo $p^{\bar{\lambda}_j}$. In this way we easily get the type of the abelian group $HG(M)$ to be $(\min(\lambda_i, \lambda_j))_{i,j}$. Note further that for any subgroup $H \subset G$ there exists a homomorphism T such that $T(G) = H$ (obtained by taking a divisor class).

Let us see a counterexample. The condition $\operatorname{Im}(f) = \operatorname{Im}(g)$ does not ensure that there exists $h/f = gh$. For example, assume $p^2 e_1 = pe_2 = 0$ and define f by $f(e_1) = e_2$ and $f(e_2) = pe_1 + e_2$ and $g(e_1) = pe_1$ and $g(e_2) = e_2$. We verify that h does not exist.

On applying standard results we see the following.

THEOREM A.1. *Let* $y \in G(M)$. *Then* $HG(M) \cdot y = \{z = \sum z_i e_i / p^{\rho_i(y)} \mid z_i\}$. *Furthermore, the type of this subgroup is* $(\lambda_k - \rho_k(y))_k$ *and its cotype is* $(\rho_k(y))_k$.

We present another interesting counterexample: it is false to say that if y and z have the same order and the depth of y is equal to that of z (the depth being defined as the largest h such that $\exists x$ with $y = p^h x$), then there exists $f \in HG(M)$ such that $f(y) = z$. To see this, take $p^3 e_1 = p^2 e_2 = pe_1 = 0$, $y = pe_1 + pe_2 + e_3$, and $z = pe_1 + e_2 + pe_3$. We verify that this "property" can be violated only if $r \geq 3$.

Before going any further, we study this sequence $\rho(y) = (\rho_k(y))_k$ associated with y.

THEOREM A.2. *The sequence* $\rho(y)$ *verifies* $\lambda_k - \lambda_{k+1} \geq \rho_k(y) - \rho_{k+1}(y) \geq 0$ *for* $1 \leq k \leq r-1$, *or equivalently, the sequences* $\rho(y)$ *and* $\lambda - \rho(y)$ *are decreasing. Reciprocally, for any sequence* θ *verifying these properties there exists a* y *with* $\theta = \rho(y)$.

Note that as a corollary of this theorem, we have that $\rho_k(y) = \rho_{k+1}(y)$ as soon as $\lambda_k = \lambda_{k+1}$.

Proof. All of that follows from the definition. It is worth mentioning that $\rho(y)$ is a fixed point for

$$R\colon (\mu_k) \mapsto \Big(\min_{1 \leq i \leq r} \big(\max(0, \lambda_k - \lambda_i) + \mu_i\big)\Big).$$

∎

We now give another characterization of the $\rho_k(y)$'s.

LEMMA A.3. $\mathrm{Hom}(G(M), \mathbb{Z}/p^{\lambda_k}\mathbb{Z}) \cdot y = p^{\rho_k(y)}\mathbb{Z}/p^{\lambda_k}\mathbb{Z}$.

Proof. Since $\exists f \in HG(M)$ with $f(y) = p^{\rho_k(y)} e_k$, we get one inclusion. For the reverse assume that there exists $F \in \mathrm{Hom}(G(M), \mathbb{Z}/p^{\lambda_k}\mathbb{Z})$ such that $F(y) = p^{\rho_k(y)-1}$. Then $f(z) = F(z)e_k$ is in $HG(M)$—hence the contradiction. ∎

Using the invariant $\rho(y)$, we can be even more precise.

THEOREM A.4. *There exists an automorphism* f *such that* $f(y) = z$ *if and only if* $\rho(y) = \rho(z)$.

Proof. It is, of course, a necessary condition. To prove that it is sufficient, we shall send y by an automorphism to $z = \sum p^{\rho_k(y)} e_k$. Let $y = \sum_{i=1}^{r} x_i e_i$. By using mappings of the type

$$e_k \mapsto e_k + t_k p^{\max(0, \lambda_h - \lambda_k)} e_h, \qquad e_i \mapsto e_i \ (i \neq k)$$

for $k \neq h$, we can change x_h modulo $\gcd(x_k p^{\max(0,\,\lambda_h-\lambda_k)}, k \neq h)$. Putting $x_i = p^{\mu_i}\alpha_i$ with $0 \leq \mu_i \leq \lambda_i$ and $(\alpha_i, p) = 1$, we see that x_i can be taken modulo p^t with $t = \min(\mu_k + \max(0, \lambda_h - \lambda_k), k \neq h)$. Now, if $\mu_h = \rho_h(y)$, we do not move it, else $t = \rho_h(y)$, and we get $\mu_h \leq \rho_h(y)$ (i.e., equality) without changing the other μ_k's. Using this process repeatedly, we reach a point

$$y' = \sum \alpha_k p^{\rho_k(y)} e_k, \qquad (\alpha_k, p) = 1.$$

Note that we have only used transforms of determinant 1. It is then easy to conclude the proof. ∎

We say that a subgroup $H \subset G(M)$ is characteristic if $f(H) \subset H$ for any $f \in HG(M)$. Such subgroups are the submodules of $G(M)$ for its structure of the $HG(M)$-module. The smallest of these subgroups are the $HG(M) \cdot y$, and any characteristic subgroup is a sum of such subgroups. Since $(p^{\min(\rho_1(y),\,\rho_1(z))}e_1, \ldots, p^{\min(\rho_r(y),\,\rho_r(z))}e_r)$ is a basis of $HG(M) \cdot y + HG(M) \cdot z$, we see that such a sum is yet another $HG(M) \cdot x$, so that any characteristic subgroup H is in fact a $HG(M) \cdot x$, and that we can define $\rho(H)$ to be $\rho(x)$. We easily prove that a characteristic subgroup is characterized by its function $\rho(H)$.

From the above we see that in case $f(H) = K$, H is a characteristic subgroup if and only if K is one. Furthermore, $f(H) = K$ implies that $\rho(H) = \rho(K)$, which in turn gives that the cotypes of H and K are equal (Theorem A.4). Thus a necessary and sufficient condition for H and K to be equal is that $\rho(H) = \rho(K)$, and we have proved the conjecture for our restricted H.

We are now in a position to characterize ideals of $HG(M)$.

THEOREM A.5. *The correspondences between ideals of $HG(M)$ and characteristic subgroups of $G(M)$ given by*

$$I = \{f / f(H) = 0\}, \qquad H = \{x / I \cdot x = 0\}$$

are one to one and are reciprocals of one another.

Proof. The set $I(H) = \{f / f(H) = 0\}$ is, of course, an ideal (i.e., a left and right ideal). Reciprocally, let I be an ideal of $HG(M)$, and let H be the intersection of the kernels of points of I. It is a characteristic subgroup since if $y \in H$, $g \in HG(M)$, and $f \in I$, then $fg(y) = 0$, since $fg \in I$. Thus $HG(M) \cdot H \subset H$. Then $I \subset I(H)$. Moreover, for any $y \notin H$, there exists $f \in I$ with $f(y) \neq 0$. Take $y = p^{\max(0,\,\rho_k(H)-1)}e_k$. Then composing with a projector, we can find $f_k \in I$ such that $f_k(\sum x_i e_i) = f_k(x_k e_k)$ and $f_k(x_k e_k) = 0$ if and only if $p^{\rho_k(H)} \mid x_k$ (since there exists an f with $f(p^{\max(0,\,\rho_k(H)-1)}e_k) \neq 0$). Furthermore, we can take $f_{k,h}(\sum x_i e_i) =$

$x_k p^{\max(0,\, \lambda_h - \rho_k(H))} e_h$. Then any f in $I(H)$ is a linear combination of these $f_{k,h}$; we get the inclusion $I(H) \subset I$ as required. ∎

COROLLARY A.6. *Ideals of $HG(M)$ are principal.*

Proof. Put $f(e_k) = p^{\lambda_k - \rho_k(H)} e_k$ and look at the ideal $J = HG(M) \cdot f \cdot HG(M)$. We have $f(H) = 0$ and thus $hfg(H) = 0$, which means that $J \subset I(H)$. Since $\mathrm{Ker}(f) = H$, we get the reverse inclusion and hence the result. ∎

REFERENCES

[B0] G. Bhowmik, Completely multiplicative arithmetical functions of matrices and certain partition identities, *J. Ind. Math. Soc.* **56** (1991), 73–83.

[B1] G. Bhowmik, Divisor functions of integer matrices: evaluations, average orders and applications, *Astérisque* **209** (1992), 169–177.

[B2] G. Bhowmik, Average orders of certain functions connected with arithmetic of matrices, *J. Ind. Math. Soc.* **59** (1993), 97–106.

[B3] G. Bhowmik, Evaluation of the divisor function of matrices, *Acta Arith.* **74** (1996), 155–159.

[BN] G. Bhowmik and V. C. Nanda, Arithmetic of matrices, manuscript.

[BR] G. Bhowmik and O. Ramaré, Average orders of multiplicative arithmetical functions of integer matrices, *Acta Arith.* **66** (1994), 45–62.

[BW] G. Bhowmik and J. Wu, Zeta functions of subgroups of abelian groups, preprint, 1997.

[B] G. Birkhoff, Subgroups of abelian groups, *Proc. London Math. Soc.* **38**(2) (1933), 385–401.

[Bu] L. M. Butler, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc.* **101** (1987), 771–775.

[CE] E. D. Cashwell and C. J. Everett, The ring of number-theoretic functions, *Pacific J. Math.* **9** (1959), 975–985.

[C] U. Christian, Über teilerfremde symmetrische Matrizenpaare, *J. Reine Angew. Math.* **229** (1968), 43–49.

[G] J. A. Green, "Symmetric Functions and p-Modules," Lecture Notes, Manchester Univ. Press, Manchester, 1961.

[H] L. K. Hua, "Introduction to Number Theory," Springer-Verlag, Berlin/New York, 1982.

[K] T. Klein, The Hall polynomial, *J. Algebra* **12** (1969), 61–78.

[Kr] A. Krieg, "Hecke Algebras," *Mem. Amer. Math. Soc.* **87** (1990).

[M] I. G. Macdonald, "Symmetric Functions and Hall Polynomials," Oxford Univ. Press, Oxford, 1979.

[N1] V. C. Nanda, On GCD and LCM of matrices, *J. Ind. Math. Soc.*, to appear.

[N2] V. C. Nanda, Arithmetic functions of matrices and polynomial identities, *Colloq. Math. Soc. János Bolyai* **34** (1982), 1107–1126.

[N3] V. C. Nanda, Generalizations of Ramanujan's sum to matrices, *J. Ind. Math. Soc.* **48** (1984), 177–187.

[N4] V. C. Nanda, On arithmetical functions of integral matrices, *J. Ind. Math. Soc.* **55** (1990), 175–188.

[Ne] M. Newman, "Integral Matrices," Academic Press, New York/London, 1972.

[RS] K. G. Ramanathan and M. V. Subbarao, Some generalizations of Ramanujan's sum, *Canad. J. Math.* **32** (1980), 1250–1260.

[T1] R. C. Thompson, Left multiples and right divisors of integral matrices, *Linear and Multilinear Algebra* **19** (1986), 287–295.

[T2] R. C. Thompson, Smith invariants of a product of integral matrices, *in* "Linear Algebra and Its Role in System Theory," Brunswick, Maine, 1984, *Contemp. Math* **47** (1985), 401–435.

[T3] R. C. Thompson, An inequality for invariant factors, *Proc. Amer. Math. Soc.* **86** (1982), 9–11.