PRESENTATIONS OF MATRIX RINGS

MARTIN KASSABOV

Recently, there has been a significant interest in the combinatorial properties the ring of $n \times n$ matrices. The aim of this note is to describe a short (may be the shortest possible) presentation of the matrix ring $\mathrm{Mat}_n(\mathbb{Z})$. This presentation is significantly shorter than the previously known ones, see [7].

Surprisingly, the number of relations in the presentation does not depend on the size of the matrices and all relations have relatively simple form. In contrast, the similar statement for the groups $\mathrm{GL}_n(\mathbb{Z})$ is significantly more difficult to prove and the presentations have more relations, see [5, 4].

Theorem 1. *The ring*[1] *of $n \times n$ matrices over $\mathbb{Z}$, for $n \geq 2$, has a presentation with* 2 *generators and 3 relations*

$$\mathrm{Mat}_n(\mathbb{Z}) = \langle x, y \mid x^n = y^n = 0, xy + y^{n-1}x^{n-1} = 1 \rangle.$$

Proof. Let R denote the ring defined by the above presentation. A homomorphism from the free associative ring to $\mathrm{Mat}_n(\mathbb{Z})$ given by

$$x \to X = \sum e_{i,i+1} \quad y \to Y = \sum e_{i,i-1}$$

factors through the ring R.[2] The first two relations are satisfied because both X and Y are nilpotent matrices and the third follows form a direct computation. Moreover, this homomorphism is surjective because the matrices X and Y generate $\mathrm{Mat}_n(\mathbb{Z})$ as a ring.

Thus, it remains to prove that the ring R is not too big. Our first step is to find other relations, which are satisfied in the ring R.

Lemma 2. *For any non-negative integers $k, l, m \geq 0$, such that $m \geq l$, we have*

$$x^k y^l x^m = \begin{cases} y^{l-k}x^k & \text{if } l \geq k \\ x^{k+m-l} & \text{if } l \leq k \end{cases}$$

and

$$y^m x^l y^k = \begin{cases} y^m x^{l-k} & \text{if } l \geq k \\ y^{k+m-l} & \text{if } l \leq k \end{cases}.$$

The author was supported in part by the NSF grants DMS 0600244 and DMS 0900932.

[1] All rings in this paper are associative and contain a unit element. Also all presentations are in the category of unitial associative rings.

[2] As usual, $e_{i,j}$ denotes the elementary matrix with 1 at i,j-th place and zeroes everywhere else.

Proof. The proof uses induction on l. The base case $l = 0$ is trivial. If $k = 0$ again there is noting to prove. Thus, without loss of generality we can assume that $k, l \geq 1$.

$$x^k y^l x^m = x^{k-1}(xy)y^{l-1}x^m = x^{k-1}(1 - y^{n-1}x^{n-1})y^{l-1}x^m =$$
$$= x^{k-1}y^{l-1}x^m - x^{k-1}y^{n-1}\left(x^{n-1}y^{l-1}x^m\right).$$

By the induction assumption the part of the second term in the brackets is equal to $x^{n+m-l} = 0$, since $m \geq l$. Thus, the second term vanishes. Another application of the induction assumption shows that

$$x^{k-1}y^{l-1}x^m = \begin{cases} y^{l-k}x^m & \text{if } l \geq k \\ x^{k+m-l} & \text{if } l \leq k \end{cases}$$

and completes the proof of the first part of the lemma.

The proof of the second part uses similar induction. Alternatively, one can use that the transformation $x \to y$ and $y \to x$ extends to an anti-automorphism σ of R and apply σ to the identities from the first part. □

Lemma 3. *The ring R is generated, as an additive group, by the elements $y^i x^j$ for $0 \leq i, j < n$.*

Proof. Let T denote the additive subgroup of R generated by the elements $y^i x^j$. It suffices to show that T is closed under, both left and right, multiplication by x and y, because $1 = x^0 y^0 \in T$. The two relations $x^n = y^n = 0$ imply that T is closed under left multiplication by y and right multiplication by x. Thus, it remains to show that $xT, Ty \subseteq T$. The element $x.y^i x^j$ is clearly in T if $i = 0$. If $i \geq 1$ we have

$$xy^i x^j = (xy)y^{i-1}x^j = \left(1 - y^{n-1}x^{n-1}\right) y^{i-1}x^j =$$
$$= y^{i-1}x^j - \left(y^{n-1}x^{n-1}y^{i-1}\right) x^j = y^{i-1}x^j - y^{n-1}x^{n-i}x^j \in T,$$

where the last equality uses Lemma 2.

Similarly, $y^i x^j.y$ is in T if $j = 0$ and if $j \geq 1$ we have

$$y^i x^j y = y^i x^{j-1}(xy) = y^i x^{j-1}\left(1 - y^{n-1}x^{n-1}\right) =$$
$$= y^i x^{j-1} - y^i\left(x^{j-1}y^{n-1}x^{n-1}\right) = y^{i-1}x^j - y^i y^{n-j}x^{n-1} \in T.$$

□

Lemma 3 together with the surjection for R to $\mathrm{Mat}_n(\mathbb{Z})$ is sufficient to show to R is isomorphic to the matrix ring, but one can build the isomorphism directly:

Definition 4. Let $a_{i,j}$, for $0 \leq i, j < n$, denote the elements

$$a_{i,j} = y^i x^j - y^{i+1}x^{j+1}.$$

Lemma 5. *We have that*

$$a_{i,j}x = a_{i,j+1} \quad a_{i,j}y = a_{i,j-1} \quad xa_{i,j} = a_{i-1,j} \quad ya_{i,j} = a_{i+1,j}.$$

Here, we assume that $a_{i,j} = 0$ if either i or j is outside the interval $[0, n-1]$.

Proof. Two of the identities follow directly from the definition of the elements $a_{i,j}$. The only non-trivial ones are $a_{i,j}y = a_{i,j-1}$ and $xa_{i,j} = a_{i-1,j}$. By the definition of the element $a_{i,j}$ we have

$$a_{i,j}y = y^i x^j y - y^{i+1}x^{j+1}y$$

If $j = 0$ the right side is equal to $y^{i+1} - y^{i+1}xy = y^{i+1}y^{n-1}x^{n-1} = 0$. Otherwise, we can use the proof of Lemma 3:

$$= \left(y^i x^{j-1} - y^{n+i-j}x^{n-1}\right) - \left(y^{i+1}x^j - y^{n+i-j}x^{n-1}\right) =$$

$$= y^i x^{j-1} - y^{i+1}x^j = a_{i,j-1}.$$

The proof of the second relation $xa_{i,j} = a_{i-1,j}$ is similar. □

Lemma 6. *The product $a_{i,j}a_{p,q}$ is equal to 0 if $j \neq p$ and is equal to $a_{i,q}$ if $j = p$. Moreover we have*

$$1 = \sum a_{i,i} \quad x = \sum a_{i,i+1} \quad y = \sum a_{i+1,i}.$$

Proof. These equalities follows directly from Lemma 5 and the definition of the elements a_{ij}. □

Thus, the map $a_{i,j} \to e_{i,j}$ extends to an isomorphism between the ring R and $\mathrm{Mat}_n(\mathbb{Z})$, which completes the proof of Theorem 1. □

Remark 7. From the isomorphism between R and $\mathrm{Mat}_n(\mathbb{Z})$ it follows that the elements x and y also satisfy the relation

$$yx + x^{n-1}y^{n-1} = 1,$$

i.e., the map $x \to y$ and $y \to x$ can be extended to an automorphism of R.

The following variation of Theorem 1 gives presentation of the ring of matrices over $\mathbb{Z}/N\mathbb{Z}$:

Theorem 8. *For any integer N the matrix ring $\mathrm{Mat}_n(\mathbb{Z}/N\mathbb{Z})$ has presentation*

$$\langle x, y \mid x^n = y^n = 0, xy + (N+1)y^{n-1}x^{n-1} = 1\rangle.$$

Proof. The argument is a slight modification of the proof of Theorem 1. The map $x \to X$ and $y \to Y$ is a homomorphism onto $\mathrm{Mat}_n(\mathbb{Z}/N\mathbb{Z})$. The proof of injectivity follows the same outline — Lemmas 2, 3, 5 and 6 still hold. Finally one observes that $a_{n-1,n-1} = y^{n-1}x^{n-1}$ and $xy = \sum_{i=0}^{n-2} a_{i,i}$. Thus the last relation in the presentation is equivalent to

$$\sum_{i=0}^{n-1} a_{i,i} = 1 = xy + (N+1)y^{n-1}x^{n-1} =$$

$$= \sum_{i=0}^{n-2} a_{i,i} + (N+1)a_{n-1,n-1}$$

therefore $Na_{n-1,n-1} = 0$, which implies that $Na_{i,j} = 0$ for all i, j, i.e., the additive group of R has exponent N. □

Remark 9. In the case $N = p$ is a prime number, one can use that the matrix algebra $\mathrm{Mat}_n(\mathbb{F}_p)$ is a cyclic algebra, thus it is possible to obtain a presentation (as an algebra over $\mathbb{F}_p$) with 2 generators and 3 relations. This leads to a presentation of the ring $\mathrm{Mat}_n(\mathbb{F}_p)$ with 2 generators and 4 relations. The presentation obtained using this approach uses a presentation of the finite field $\mathbb{F}_{p^n}$, which involves an irreducible polynomial of degree n over $\mathbb{F}_p$. Thus, the relations in this presentation will be more "complicated" than the ones Theorem 8. In some cases, one can modify the presentation of the cyclic algebra and save one relation:[3]

$$\mathrm{Mat}_p(\mathbb{F}_p) = \langle x, y \mid y^p = 1, x^p = x, xy = y(x+1)\rangle.$$

Remark 10. In some sense the presentation in Theorem 1 is a variant of the presentation of cyclic algebra, where one uses the nilpotent ring $\mathbb{Z}[x]/(x^n)$ instead of the maximal subfield, however it is not completely clear what is the analog of the "field" automorphism in this picture.

One would like to say that the presentations in Theorems 1 and 8 are the simplest possible. Unfortunately, we were not able to prove that presentations of the matrix rings with 2 generators and only 2 relations do not exist. The following result shows that there isn't any presentation of the matrix ring $\mathrm{Mat}_n(\mathbb{Z})$ with a single relation:

Theorem 11. *The number of relations in any presentation of the matrix ring* $\mathrm{Mat}_n(\mathbb{Z})$ *is at least equal to the number of generators.*

Proof. The main idea of the proof is to "translate" the notion of the "relation module" from groups rings and use it to obtain a lower bound for the number of relations in a presentation of ring, see [6].

Let $0 \to I \to \mathbb{Z}\langle S\rangle \to R \to 0$ be a presentation of the ring R. The quotient I/I^2 is called *relation module associated to this presentation* and is naturally a R bi-module. It is clear that the projection of any generating set of the ideal I to I/I^2 is a generating set of this bi-module. Thus, the minimal number of generators of relation module gives a lower bound for the number of generators of the ideal I and the number of relations in a presentation of the ring R.

One way to construct a big quotient of the relation module is the following: Let d be the size of the generating set $\bar{S}$ and let M be the free R bi-module on d generators m_i, i.e., $M \simeq (R \otimes R)^{\oplus d}$. We can define a ring structure on the abelian group $R \oplus M$, where the multiplication between elements of R and M is defined using left and right actions of R on M and the product of any two elements in M is equal to zero.

For any generating set $\bar{S}$ of R with d elements one can define a subring $\tilde{R}$ of $R \oplus M$ generated by "extensions" of the generators in $\bar{S}$ by generators of the module M, i.e., $\tilde{s}_i = \bar{s}_i + m_i$. It is easy to see that the relation module

[3]This presentation was found by Robert Guralnick [3].

corresponding to this presentation maps surjectively onto the intersection of $\tilde{R}$ with M.

In the special case of the matrix ring $\mathrm{Mat}_n(\mathbb{Z})$, we have the module isomorphism $M \simeq \mathrm{Mat}_n(L)$, where L is free abelian group on $n^2 d$ generators (this follows form the isomorphism of the bi-modules $\mathrm{Mat}_n(\mathbb{Z}) \otimes \mathrm{Mat}_n(\mathbb{Z}) \simeq \mathrm{Mat}_n(\mathbb{Z}^{\oplus n^2})$). A long computation shows that the intersection of $\tilde{R}$ with M is isomorphic to $\mathrm{Mat}_n(\tilde{L})$, where $\tilde{L} \subset L$ is a subgroup of rank at least $n^2(d-1)+n > n^2(d-1)$ — this bound does not depend on the images of the generators S in $\mathrm{Mat}_n(\mathbb{Z})$. This completes the proof of the Theorem, since the relation module can not be generated by than $d-1$ elements. □

Remark 12. A more carefully computation shows that the relation module, corresponding to the map $\mathbb{Z}\langle x, y\rangle \to \mathrm{Mat}_n(\mathbb{Z})$ given by $x \to X$ and $y \to Y$, can be generated by only two elements as an bi-module (for example the elements $xy + y^{n-1}x^{n-1} - 1$ and $xy^n + yx^n$ generate the relation module). This suggests that it might be possible to "combine" the two relations $x^n = y^n = 0$ into a single one and obtain a presentation of $\mathrm{Mat}_n(\mathbb{Z})$ with 2 generators and only 2 relations. Unfortunately, the usual trick of combining such relations — replacing them with $x^n = y^n$ does not work, because the presentation

$$\langle x, y \mid x^n = y^n, xy + y^{n-1}x^{n-1} = 1\rangle$$

defines a ring which surjects onto $\mathrm{Mat}_n\left(\mathbb{Z}[t]/(t^2)\right)$.

Remark 13. One can view the proof of Theprem 11 as an analog of Gaschütz' result [1, 2], which says that the tensor product of the relation module for a finite group G with $\mathbb{Q}$ is isomorphic as G-module to $\mathbb{Q}[G]^{\oplus d-1} \oplus \mathbb{Q}$, therefore the relation module can not be generated by less than d elements.

Acknowledgment: The presentations in this paper arise as a side-result of a project about presentations of finite groups. The author wish to thank his collaborators in that project Robert Guralnick, William Kantor and Alex Lubotzky for useful discussions.

References

[1] Wolfgang Gaschütz. Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden. *Math. Z.*, 60:274–286, 1954.

[2] Karl W. Gruenberg. *Relation modules of finite groups*. American Mathematical Society, Providence, R.I., 1976. Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 25.

[3] R. M. Guralnick. private communacation.

[4] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky. Presentations of finite simple groups: a computational approach. *J. European Math. Soc., to appear.*

[5] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky. Presentations of finite simple groups: a quantitative approach. *J. Amer. Math. Soc.*, 21(3):711–774, 2008.

[6] S. V. Ivanov. Relation modules and relation bimodules of groups, semigroups and associative algebras. *Internat. J. Algebra Comput.*, 1(1):89–114, 1991.

[7] B. V. Petrenko and S. N. Sidki. On pairs of matrices generating matrix rings and their presentations. *J. Algebra*, 310(1):15–40, 2007.

Martin Kassabov, Department of Mathematics, Cornell University, Malott Hall, Ithaca, NY 14853-4201, USA

email: kassabov@math.cornell.edu