Algebra & Number Theory

Volume 6
2012
No. 2

On the smallest number of generators and the probability of generating an algebra

Rostyslav V. Kravchenko, Marcin Mazur and Bogdan V. Petrenko

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 6:2(2012)

msp

On the smallest number of generators and the probability of generating an algebra

Rostyslav V. Kravchenko, Marcin Mazur and Bogdan V. Petrenko

In this paper we study algebraic and asymptotic properties of generating sets of algebras over orders in number fields. Let A be an associative algebra over an order R in an algebraic number field. We assume that A is a free R-module of finite rank. We develop a technique to compute the smallest number of generators of A. For example, we prove that the ring $\mathrm{M}_3(\mathbb{Z})^k$ admits two generators if and only if $k \leq 768$. For a given positive integer m, we define the density of the set of all ordered m-tuples of elements of A which generate it as an R-algebra. We express this density as a certain infinite product over the maximal ideals of R, and we interpret the resulting formula probabilistically. For example, we show that the probability that 2 random 3×3 matrices generate the ring $\mathrm{M}_3(\mathbb{Z})$ is equal to $(\zeta(2)^2\zeta(3))^{-1}$, where ζ is the Riemann zeta function.

1. Introduction

Let R be a commutative ring with 1. Recall that a set S generates an associative unital R-algebra A if the set of all monomials in the elements of S (including the

MSC2000: primary 16S15, 11R45, 11R99, 15A33, 15B36, 11C20, 11C08; secondary 16P10, 16H05.

Keywords: density, smallest number of generators, probability of generating.

degree-zero monomial 1) spans A as an R-module. This paper lays a foundation for our program to investigate properties of the sets of generators of R-algebras A whose additive group is a finitely generated R-module. A substantial part of our results grew out of the following question: given a ring A whose additive group is a free abelian group of finite rank and a positive integer k, what is the probability that k random elements of A generate it as a $\mathbb{Z}$-algebra? We will show that this question can be stated in a rigorous way and that it has a very interesting answer. The following formulas, in which ζ denotes the Riemann zeta function, are special cases of our results (see Theorem 8.1):

- The probability that m random 2×2 matrices generate the ring $\mathrm{M}_2(\mathbb{Z})$ is equal to $1/(\zeta(m-1)\zeta(m))$.
- The probability that 2 random 3×3 matrices generate the ring $\mathrm{M}_3(\mathbb{Z})$ is equal to $1/(\zeta(2)^2\zeta(3))$.
- The probability that 3 random 3×3 matrices generate the ring $\mathrm{M}_3(\mathbb{Z})$ is equal to
$$\frac{1}{\zeta(2)\zeta(3)\zeta(4)}\prod_p\left(1+\frac{1}{p^2}+\frac{1}{p^3}-\frac{1}{p^5}\right),$$
where the product is taken over all prime numbers.

Our main results are obtained for algebras A over an order R in some number field such that A is a free R-module of finite rank. It is not hard though to extend the results to the case when R is an order in a global field of positive characteristic (we will address this in a follow-up paper). Roughly speaking, a choice of an integral basis of R and of a basis of A over R allows us to introduce integral coordinates on all Cartesian powers A^k, $k\in\mathbb{N}$. For any subset S of A^k and any N we consider the finite set $S(N)$ of all points whose coordinates are in the interval $[-N, N]$. We define the density $\mathrm{den}(S)$ of S as the limit
$$\lim_{N\to\infty}\frac{|S(N)|}{|A^k(N)|}$$
(we do not claim that it always exists). Our goal is to calculate the density of the set of generators of A.

Definition 1.1. Let A be an algebra over a commutative ring R, and let k be a positive integer. We define the set $\mathrm{Gen}_k(A, R)$ as follows:

$$\mathrm{Gen}_k(A, R)=\{(a_1,\dots,a_k)\in A^k : a_1,\dots,a_k \text{ generate } A \text{ as an } R\text{-algebra}\}.$$

For the rest of the introduction, we assume that R is an order in a number field K and A is an R-algebra which is free of finite rank m as an R-module (unless stated otherwise).

In Theorem 3.2 we prove that the set $\mathrm{Gen}_k(A, R)$ has density, which we denote by $\mathrm{den}_k(A)$, and that it can be computed locally as follows:

$$\mathrm{den}_k(A) = \prod_{\mathfrak{p}\in \text{m-Spec } R} \frac{|\mathrm{Gen}_k(A/\mathfrak{p}A, R/\mathfrak{p})|}{|R/\mathfrak{p}|^{mk}}, \tag{1}$$

where m-Spec R denotes the set of all maximal ideals of R. In order to prove Theorem 3.2 we had to extend this local-to-global formula for density to a substantially larger class of sets. This led us to Theorem 3.3, which is of independent interest and has potential applications to various other questions. Theorem 3.3 deals with a finite set $f_1, \ldots, f_s$ of polynomials in $R[x_1, \ldots, x_n]$ and the set S of all $a \in R^n$ such that the ideal generated by $f_1(a), \ldots, f_s(a)$ is R. It asserts that the set S has density $\mathrm{den}(S)$ given by the formula

$$\mathrm{den}(S) = \prod_{\mathfrak{p}\in \text{m-Spec } R} \left(1 - \frac{t_{\mathfrak{p}}}{|R/\mathfrak{p}|^n}\right),$$

where $t_{\mathfrak{p}}$ is the number of common zeros in $(R/\mathfrak{p})^n$ of the polynomials $f_1 \ldots, f_s$ considered as polynomials over the field $R/\mathfrak{p}$.

As a first application of our results we answer in Section 3A the following question posed by Ilya Kapovich: what is the probability that m random elements of a free abelian group of rank $n \le m$ generate the group? Our results provide a rigorous proof of the following answer: the probability in question is equal to $\left(\prod_{k=m-n+1}^{m} \zeta(k)\right)^{-1}$, where ζ is the Riemann zeta function (when $m = n$ this product should be interpreted as 0).

In Section 5 we show how (1) can be used to get information about the smallest number of generators of an R-algebra A.

Definition 1.2. Let A be a finitely generated R-algebra. By $r(A, R)$ we denote the smallest number of generators of A as an R-algebra.

In Theorem 5.2 we prove that if k is an integer such that $k - 1 \ge r_0 := r(A \otimes_R K, K)$ and $k \ge r_{\mathfrak{p}} := r(A/\mathfrak{p}A, R/\mathfrak{p}R)$ for every maximal ideal $\mathfrak{p}$ of R then $\mathrm{den}_k(A) > 0$. Let r_f be the largest among the numbers $r_{\mathfrak{p}}$. Clearly, if $\mathrm{den}_k(A) > 0$ then A can be generated by k elements. Using this remark and Theorem 5.2 we show in Theorem 5.5 that the smallest number of generators of A coincides with r_f if $r_f > r_0$ and is either r_0 or r_0+1 otherwise. A special case of this result, when $R = \mathbb{Z}$, was kindly communicated to us by H. W. Lenstra (private communication, 2007). Note that when $r_f = r_0$, we only know that r is either r_0 or $r_0 + 1$. Nevertheless, it is often possible to prove that $\mathrm{den}_{r_0}(A) > 0$ and conclude that $r = r_0$. For example, we have been unable for a long time to find the largest integer n such that the product $\mathrm{M}_3(\mathbb{Z})^n$ of n copies of the matrix ring $\mathrm{M}_3(\mathbb{Z})$ admits two generators as a $\mathbb{Z}$-algebra. We knew that $n \le 768$, but any attempts to construct explicitly two

generators for such large values of n have been beyond our computational ability. It turns out, though, that we can prove that $\mathrm{den}_2(\mathrm{M}_3(\mathbb{Z})^{768}) > 0$, hence we get a (nonconstructive) proof that $n = 768$ (see Theorem 8.2).

In Theorem 5.7 we extend Lenstra's original approach to obtain a similar formula for the smallest number of generators of algebras over any commutative ring R of dimension at most 1. This formula is reminiscent of the Forster–Swan theorem on the number of generators of modules over Noetherian commutative rings [Matsumura 1986, Theorem 5.8]. By analogy with this result, in Conjecture 5.8 we propose an extension of our formula to algebras over general Noetherian rings.

In order to use (1) in concrete cases one needs to be able to compute the numbers $|\mathrm{Gen}_k(A/\mathfrak{p}A, R/\mathfrak{p})|$. This leads us to the results of Sections 6 and 7, where we study these numbers under the assumption that $A/\mathfrak{p}A$ is a product of matrix algebras. After various reductions in Section 6 we derive explicit formulas for $|\mathrm{Gen}_k(\mathrm{M}_n(\mathbb{F}), \mathbb{F})|$, where $\mathbb{F}$ is a finite field and $n = 2, 3$. Furthermore, we get a lower bound when $n > 3$ (Proposition 7.9). As a corollary, we prove that if $m \geq 2$ then the probability that m matrices in $\mathrm{M}_n(\mathbb{F}_q)$, chosen under the uniform distribution, generate the $\mathbb{F}_q$-algebra $\mathrm{M}_n(\mathbb{F}_q)$ tends to 1 as $q+m+n \to \infty$ (see Corollary 7.10). This result proves and vastly generalizes the conjectural formula [Petrenko and Sidki 2007, (17), p. 27]. The case of $n = 2$ and some of the results of Section 6 have been discussed earlier in [Kravchenko and Petrenko 2006], which was the starting point for the present work. This part of our paper has been influenced by ideas of Philip Hall [1936].

In Section 8 the results of Sections 6 and 7 are applied to finite products of matrix algebras over the ring of integers in a number field.

To state some of our remaining results, we need the following notation.

Definition 1.3. Let $m, n \geq 1$ be integers and let A be an R-algebra. We introduce the following notation:

(i) $\mathrm{gen}_m(A, R)$ is the largest $k \in \mathbb{Z} \cup \{\infty\}$ such that $r(A^k, R) \leq m$;

(ii) $\mathrm{gen}_{m,n}(q) = \mathrm{gen}_m(\mathrm{M}_n(\mathbb{F}_q), \mathbb{F}_q)$;

(iii) $\mathrm{g}_{m,n}(q) = |\mathrm{Gen}_m(\mathrm{M}_n(\mathbb{F}_q), \mathbb{F}_q)|$.

We show in Proposition 6.2 that

$$\mathrm{gen}_{m,n}(q) = \frac{\mathrm{g}_{m,n}(q)}{|\mathrm{PGL}_n(\mathbb{F}_q)|}$$

and $r(\mathrm{M}_n(\mathbb{F}_q)^{1+\mathrm{gen}_{m,n}(q)}, \mathbb{F}_q) = m+1$ by Corollary 2.15.

Here are some special cases of our results in Section 8:

(1) $\mathrm{gen}_{m,2}(q) = \dfrac{q^{2m-1}(q^m-1)(q^m-q)}{q^2-1}$.

(2) $\operatorname{gen}_m(\mathrm{M}_2(\mathbb{Z}), \mathbb{Z}) = \operatorname{gen}_{m,2}(2) = \dfrac{2^{2m-1}(2^m-2)(2^m-1)}{3}$.

(3) $\operatorname{gen}_{m,3}(q) = \dfrac{q^{3m-3}(q^m-1)(q^m-q)(q^m+q)}{(q-1)^2(q+1)(q^2+q+1)}$
$\times(q^{3m}-q^{m+2}+q^{2m}-2q^{m+1}-q^m+q^3+q^2)$.

(4) $\operatorname{gen}_m(\mathrm{M}_3(\mathbb{Z}), \mathbb{Z}) = \operatorname{gen}_{m,3}(2)$
$= \dfrac{(2^m-2)(2^m-1)(2^m+2)(2^{3m}+2^{2m}-2^{m+3}-2^m+12)2^{3m-3}}{21}$.

The techniques we have developed so far can be applied to any finitely generated $\mathbb{Z}$-algebra whose reduction modulo every prime is a direct sum of matrix rings over finite fields. However, among maximal orders in semisimple algebras over $\mathbb{Q}$ the only such algebras are the maximal orders in matrix rings by the Hasse–Brauer–Noether–Albert theorem. In order to extend our results to maximal orders in other semisimple algebras we need to obtain formulas for the number of generators of algebras over finite fields which have nontrivial Jacobson radical. This will be done in a subsequent paper. Let us just mention here a special case, when A is a maximal order in the quaternion algebra $\mathbb{Q}(i, j)$ ($i^2 = -1 = j^2$). For any odd prime p we have $A/pA \cong \mathrm{M}_2(\mathbb{F}_p)$, so A and $\mathrm{M}_2(\mathbb{Z})$ differ only at the prime 2 and at infinity. Note that $A/2A$ is a commutative algebra over $\mathbb{F}_2$ whose quotient modulo the Jacobson radical is the field $\mathbb{F}_4$. Since $\mathbb{F}_4^{16}$ cannot be generated by two elements, we see that A^{16} requires at least three generators. It can be verified that A^{15} admits two generators. So A can be distinguished from $\mathrm{M}_2(\mathbb{Z})$ by counting the smallest number of generators of powers of these two algebras. Note that for the integral quaternions $\mathbb{Z}[i, j]$ already $\mathbb{Z}[i, j]^4$ requires at least three generators. In a subsequent paper we will extend these observations to a much larger class of orders.

In another work in progress we apply the techniques developed in the present paper to study generators of various nonassociative algebras. Our technique applies to any finitely generated R-module equipped with an R-bilinear form, but we focus mainly on Lie algebras and Jordan algebras. For example, we show that the probability that m random elements generate the Lie ring $\mathrm{sl}_2(\mathbb{Z})$ of 2×2 integer matrices with zero trace is equal to

$$\frac{1}{\zeta(m-1)\zeta(m)}.$$

2. Preliminary results

Let R be a commutative ring with 1. *Unless stated otherwise, all R-algebras are assumed to be associative, unital, and finitely generated as an R-module.*

In this section we collect several fairly straightforward observations which are used through the paper. Let A be an R-algebra. Recall that elements $a_1, \ldots, a_k$ generate A as an R-algebra if all the (noncommutative) monomials in $a_1, \ldots, a_k$, including the degree-zero monomial 1, generate A as an R-module. We say that $a_1, \ldots, a_k$ *strongly generate* A as an R-algebra if already all the (noncommutative) monomials in $a_1, \ldots, a_k$ of positive degree generate A as an R-module.

Lemma 2.1. *Suppose that there exists no R-algebra homomorphism $A \to R/I$ for any proper ideal I of R. Then any set that generates A as an R-algebra also strongly generates A.*

Proof. Suppose that $a_1, \ldots, a_k$ generate A as an R algebra and let J be the R submodule of A generated by all the (noncommutative) monomials in $a_1, \ldots, a_k$ of positive degree. Then $R \cdot 1 + J = A$. Since J is closed under multiplication, it is a two-sided ideal of A and $A/J \cong R/(R \cap J)$. By our assumption, $R \cap J$ cannot be a proper ideal of R, so $R \cdot 1 \subset J$ and $J = A$. □

Example 2.2. Let the algebra $A = \prod_{i=1}^{n} \mathrm{M}_{m_k}(R)$ be a finite product of matrix algebras over R, with each $m_i \geq 2$. Then any set which generates A as an R-algebra also strongly generates A. This is a direct consequence of Lemma 2.1 and the remark that A has no nontrivial commutative quotients.

In this paper we decided to focus on unital algebras and we do not discuss strong generators. However most of our results can be easily modified to sets of strong generators and algebras which are not necessarily unital. One can also reduce questions about strong generators to generators using the following observation. Recall that if A is an R-algebra (unital or not) we can construct a unital algebra $A^{(1)}$ which is $R \oplus A$ as an R-module with multiplication defined by $(r, a)(s, b) = (rs, ab + rb + sa)$. We have the following lemma.

Lemma 2.3. *Let $a_1, \ldots, a_k \in A$. Then the following conditions are equivalent*:

(1) *$a_1, \ldots, a_k$ strongly generate A as an R-algebra.*

(2) *$(r_1, a_1), \ldots, (r_k, a_k)$ generate $A^{(1)}$ as an R-algebra for any elements $r_1, \ldots, r_k \in R$.*

(3) *$(r_1, a_1), \ldots, (r_k, a_k)$ generate $A^{(1)}$ as an R-algebra for some elements $r_1, \ldots, r_k \in R$.*

Proof. We identify A with the ideal $\{0\} \oplus A$ in $A^{(1)}$. Assume (1) and let $r_1, \ldots, r_k$ be in R. Since $(0, a_i) = (r_i, a_i) - r_i(1, 0)$, the R-subalgebra B of $A^{(1)}$ generated by $(r_1, a_1), \ldots, (r_k, a_k)$ contains all monomials in $(0, a_1), \ldots, (0, a_k)$, hence it contains A. Since B also contains $R \oplus \{0\}$, we see that $A^{(1)} = B$. Thus condition (1) indeed implies (2). Condition (3) is clearly a consequence of (2). Assume (3) and let C be the subalgebra of A strongly generated by $a_1, \ldots, a_k$. Note that

any monomial of positive degree in $(r_1, a_1), \ldots, (r_k, a_k)$ is of the form (r, c) for some $r \in R$ and $c \in C$. By the assumption in (3), for any $a \in A$ there is $r \in R$ such that (r, a) is an R-linear combination of monomials of positive degree in $(r_1, a_1), \ldots, (r_k, a_k)$. It follows that $a \in C$. Thus $C = A$, which shows that (1) follows from (3). □

The following observation is straightforward.

Lemma 2.4. *Let A be an R-algebra. For any ideal I of R we have*

$$A^{(1)}/IA^{(1)} = (A/IA)^{(1)},$$

where the adjunction of unity on the right is in the category of R/I-algebras.

Definition 2.5. For an R-algebra A and positive integer k we denote by $\mathrm{Gen}_k(A, R)$ the set of all k-tuples $(a_1, \ldots, a_k) \in A^k$ which generate A as an R-algebra. When there is no danger of confusion, we write $\mathrm{Gen}_k(A)$ for $\mathrm{Gen}_k(A, R)$.

Lemma 2.6. *The elements $a_1, \ldots, a_k$ generate A as an R-algebra if and only if for every maximal ideal $\mathfrak{m}$ of R the images of $a_1, \ldots, a_k$ in $A \otimes_R R/\mathfrak{m} = A/\mathfrak{m}A$ generate $A/\mathfrak{m}A$ as an $R/\mathfrak{m}$-algebra.*

Proof. Let J be the R submodule of A generated by all the (noncommutative) monomials in $a_1, \ldots, a_k$. By [Matsumura 1986, Theorem 4.8], $A = J$ if and only if $A/J \otimes_R R/\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ of R. The result follows from the simple remark that $A/J \otimes_R R/\mathfrak{m} = 0$ if and only if the images of $a_1, \ldots, a_k$ in $A/\mathfrak{m}A$ generate it as an $R/\mathfrak{m}$-algebra. □

Lemma 2.7. *Let R be a field and let A be an R-algebra of dimension m. The elements $a_1, \ldots, a_k$ generate A as an R-algebra if and only if the (noncommutative) monomials in $a_1, \ldots, a_k$ of degree $< m$ span A as an R-vector space.*

Proof. Let A_i be the subspace of A spanned by all the monomials in $a_1, \ldots, a_k$ of degree $\leq i$. Clearly $A_0 \subseteq A_1 \subseteq A_2 \subseteq \ldots$. We also see that

$$A_{i+1} = A_i + a_1 A_i + a_2 A_i + \cdots + a_k A_i,$$

for any i. It follows that if $A_i = A_{i+1}$ for some i, then $A_j = A_i$ for all $j \geq i$. Since $\dim_R A_m \leq m$, we must have $A_i = A_{i+1}$ for some $i < m$. Thus $A_i = A_{m-1}$ for all $i \geq m$. This proves that $a_1, \ldots, a_k$ generate A as an R-algebra if and only if $A = A_{m-1}$. □

Lemma 2.8. *Suppose that A can be generated by m elements as an R-module. The elements $a_1, \ldots, a_k$ generate A as an R-algebra if and only if the (noncommutative) monomials in $a_1, \ldots, a_k$ of degree $< m$ generate A as an R-module.*

Proof. Suppose that $a_1, \dots, a_k$ generate A as an R-algebra and let A_i be the R-submodule of A generated by all the monomials in $a_1, \dots, a_k$ of degree $\leq i$. For any maximal ideal $\mathfrak{m}$ of R the dimension of $A/\mathfrak{m}A$ over $R/\mathfrak{m}$ does not exceed m. Thus $A/A_{m-1} \otimes_R R/\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ of R by Lemma 2.7. Hence $A = A_{m-1}$ by [Matsumura 1986, Theorem 4.8]. □

Recall that Spec R is the set of all prime ideals of R equipped with the Zariski topology and m-Spec R is the subspace of Spec R consisting of all maximal ideals. For $\mathfrak{p} \in \operatorname{Spec} R$ we denote by $R_\mathfrak{p}$ the localization of R at the prime ideal $\mathfrak{p}$ and we set $A_\mathfrak{p} = R_\mathfrak{p} \otimes_R A$. The residue field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is denoted by $\kappa(\mathfrak{p})$. Recall that $\kappa(\mathfrak{p})$ coincides with the field of fractions of $R/\mathfrak{p}$.

Definition 2.9. We say that the elements $a_1, \dots, a_k$ generate A at a prime ideal $\mathfrak{p}$ of R if their images in $\kappa(\mathfrak{p}) \otimes_R A$ generate $\kappa(\mathfrak{p}) \otimes_R A$ as a $\kappa(\mathfrak{p})$-algebra. Equivalently, $a_1, \dots, a_k$ generate A at $\mathfrak{p}$ if their images in $A_\mathfrak{p}$ generate $A_\mathfrak{p}$ as an $R_\mathfrak{p}$-algebra.

Lemma 2.10. *Let $a_1, \dots, a_k \in A$. The set of all prime ideals $\mathfrak{p}$ such that $a_1, \dots, a_k$ generate A at $\mathfrak{p}$ is open.*

Proof. Let B be the R submodule of A generated by all monomials in $a_1, \dots, a_k$ of degree $< m$, where m is such that A can be generated by m elements as an R-module. By Lemma 2.8, the images of $a_1, \dots, a_k$ in $A_\mathfrak{p}$ generate $A_\mathfrak{p}$ as an $R_\mathfrak{p}$-algebra if and only if $(A/B)_\mathfrak{p} = 0$. Since the support of a finitely generated R-module is closed, the result follows. □

Corollary 2.11. *For any positive integer k the set*

$$U_k = \{\mathfrak{p} \in \operatorname{Spec} R : A_\mathfrak{p} \textit{ can be generated by } k \textit{ elements as an } R_\mathfrak{p}\textit{-algebra}\}$$

is open.

Proof. Suppose that $A_\mathfrak{p}$ is generated by k elements as an $R_\mathfrak{p}$-algebra. We may choose elements $a_1, \dots, a_k$ in A which generate A at $\mathfrak{p}$. By Lemma 2.10, there is an open neighborhood of $\mathfrak{p}$ such that $a_1, \dots, a_k$ generate A at $\mathfrak{q}$ for each $\mathfrak{q}$ in this neighborhood. This shows that U_k is open. □

Proposition 2.12. *Suppose that $A = \prod_{i=1}^s A_i$ is a product of R-algebras $A_1, \dots, A_s$ such that for any maximal ideal $\mathfrak{m}$ of R and any $i \neq j$ the $R/\mathfrak{m}$-algebras $A_i \otimes_R R/\mathfrak{m}$ and $A_j \otimes_R R/\mathfrak{m}$ do not have isomorphic quotients. Then $\operatorname{Gen}_k(A) = \prod_{i=1}^s \operatorname{Gen}_k(A_i)$ under the natural identifications.*

Proof. The proposition says that a sequence $a_1, \dots, a_k$ of elements in A generates A as an R-algebra if and only if for every i the projection of these sequence to A_i generates A_i as an R-algebra. The implication to the right is clear. Since $A \otimes_R R/\mathfrak{m} = \prod_{i=1}^s (A_i \otimes_R R/\mathfrak{m})$, Lemma 2.6 reduces the proof to the case when R is a field. Suppose that a sequence $a_1, \dots, a_k$ of elements in A has the property

that for every i the projection of these sequence to A_i generates A_i as an R-algebra. Let B be the R-subalgebra of A generated by $a_1, \ldots, a_k$. By our assumption, the projection $\pi_i : B \to A_i$ is surjective. Let $J_i = \ker \pi_i$. Since A_i and A_j have no isomorphic quotients for $i \neq j$, we conclude that $J_i + J_j = B$ for $i \neq j$ (for otherwise, $J = J_i + J_j$ would be a proper ideal of B and B/J would be isomorphic to a quotient of A_i and a quotient of A_j). The Chinese remainder theorem implies now that $B = A$. □

Example 2.13. Let $A_i = \mathrm{M}_{n_i}(R)^{m_i}$ be the product of m_i copies of the $n_i \times n_i$ matrix ring over R, where $n_i \neq n_j$ for $i \neq j$. Then for any maximal ideal $\mathfrak{m}$ of R we have $A_i \otimes_R R/\mathfrak{m} = \mathrm{M}_{n_i}(R/\mathfrak{m})^{m_i}$. Consider two distinct indices i, j. If the $R/\mathfrak{m}$-algebras $A_i \otimes_R R/\mathfrak{m}$ and $A_j \otimes_R R/\mathfrak{m}$ had isomorphic quotients, they would have isomorphic quotients which are simple $R/\mathfrak{m}$-algebras. Clearly any simple quotient of $\mathrm{M}_{n_i}(R/\mathfrak{m})^{m_i}$ is isomorphic to $\mathrm{M}_{n_i}(R/\mathfrak{m})$. Since $\mathrm{M}_{n_i}(R/\mathfrak{m})$ and $\mathrm{M}_{n_j}(R/\mathfrak{m})$ are not isomorphic (they have different dimensions over $R/\mathfrak{m}$), we see that the $R/\mathfrak{m}$-algebras $A_i \otimes_R R/\mathfrak{m}$ and $A_j \otimes_R R/\mathfrak{m}$ do not have isomorphic quotients. Therefore the assumptions of Proposition 2.12 are satisfied and

$$\mathrm{Gen}_k\Big(\prod_{i=1}^{s} \mathrm{M}_{n_i}(R)^{m_i}\Big) = \prod_{i=1}^{s} \mathrm{Gen}_k\big(\mathrm{M}_{n_i}(R)^{m_i}\big).$$

Recall that in Definition 1.3 we defined $\mathrm{gen}_m(A, R)$ as the largest k such that A^k admits m generators as an R-algebra. The following proposition implies that if $\mathrm{gen}_m(A, R)$ is finite then $\mathrm{gen}_{m+1}(A, R) > \mathrm{gen}_m(A, R)$.

Proposition 2.14. *Let A be an R-algebra and let n be a positive integer. If A^n can be generated by m elements as an R-algebra then A^{n+1} can be generated by $m+1$ elements.*

Proof. Let $a_i = (a_{i,1}, \ldots, a_{i,n})$, with $i = 1, \ldots, m$, generate A^n. Let $b_i = (a_{i,1}, \ldots, a_{i,n}, a_{i,1})$, $i = 1, \ldots, m$, and set $b_{m+1} = (0, \ldots, 0, 1)$. For any $w = (w_1, \ldots, w_n) \in A^n$ there is a noncommutative polynomial $p(x_1, \ldots, x_m)$ with coefficients in R such that $w = p(a_1, \ldots, a_m)$. Then $p(b_1, \ldots, b_m) = (w_1, \ldots, w_m, w_1)$. It follows that $b_{m+1}p(b_1, \ldots, b_m) = (0, \ldots, 0, w_1)$ and $p(b_1, \ldots, b_m) - b_{m+1}p(b_1, \ldots, b_m) = (w_1, \ldots, w_m, 0)$. Thus the algebra generated by $b_1, \ldots, b_{m+1}$ coincides with A^{n+1}. □

Corollary 2.15. *Let A be an R-algebra. If $\mathrm{gen}_m(A, R)$ is finite then*

$$r(A^{1+\mathrm{gen}_m(A,R)}, R) = m + 1.$$

We end this section with a discussion of an effective method of checking if given elements generate an R-algebra A. The key observation is contained in the following simple lemma:

Lemma 2.16. *Let A be an R-algebra generated as an R-module by elements $u_1, \dots, u_m$ and let $k \geq 1$ be an integer. For every monomial $M = M(x_1, \dots, x_k)$ in k noncommuting variables $x_1, \dots, x_k$ there are polynomials $p_j^M(x_{1,1}, \dots, x_{k,m}) \in R[x_{1,1}, \dots, x_{k,m}]$, $j = 1, \dots, m$, such that the degree of each p_j^M does not exceed the degree of M and*

$$M(a_1, \dots, a_k) = \sum_{i=1}^{m} p_i^M(a_{1,1}, \dots, a_{k,m})u_i$$

whenever $a_{i,j} \in R$ satisfy $a_i = \sum_{j=1}^m a_{i,j}u_j$.

Proof. There exist elements $c_{i,j,s} \in R$, $1 \leq i, j, s \leq m$, such that $u_i u_j = \sum_{s=1}^m c_{i,j,s}u_s$. Note that these elements are not unique, unless A is a free R-module with basis $u_1, \dots, u_m$ (this is the case we are mainly interested in). We fix some choice of elements $c_{i,j,s}$ and call them the structure constants for A. Furthermore, choose and fix $r_i \in R$, $i = 1, \dots, m$, such that $1 = \sum r_i u_i$. We prove the lemma by induction on the degree of M. If degree of M is 0 then $M = 1$ and we can choose constant polynomials $p_i^M = r_i$. Suppose that the lemma holds for all monomials of degree less than n and let M be a monomial of degree n. Then $M = Nx_t$ for some monomial N of degree $n-1$ and some $t \in \{1, \dots, k\}$. If $a_i = \sum_{j=1}^m a_{i,j}u_j$, with $a_{i,j} \in R$, $1 \leq i \leq k$, then

$$\begin{aligned}
M(a_1, \dots, a_k) &= N(a_1, \dots, a_k) \sum_{j=1}^{m} a_{t,j}u_j \\
&= \Big(\sum_{i=1}^{m} p_i^N(a_{1,1}, \dots, a_{m,k})u_i\Big)\Big(\sum_{j=1}^{m} a_{t,j}u_j\Big) \\
&= \sum_{i=1}^{m}\sum_{j=1}^{m} p_i^N(a_{1,1}, \dots, a_{m,k})a_{t,j} \sum_{s=1}^{m} c_{i,j,s}u_s \\
&= \sum_{s=1}^{m}\Big(\sum_{i=1}^{m}\sum_{j=1}^{m} p_i^N(a_{1,1}, \dots, a_{m,k})a_{t,j}c_{i,j,s}\Big)u_s.
\end{aligned}$$

This proves that the polynomials

$$p_s^M = \sum_{i=1}^{m}\sum_{j=1}^{m} c_{i,j,s}p_i^N x_{t,j}, \quad s = 1, \dots, m,$$

have the required properties. □

Lemma 2.17. *Let A be an R-algebra which is a free R-module with a basis $u_1, \dots, u_m$ and let $k \geq 1$ be an integer. There is a finite set $T \subseteq R[x_{1,1}, \dots, x_{k,m}]$ of polynomials of degree not exceeding m^2 such that for any commutative R-algebra S the following two conditions are equivalent*:

(i) *The elements* $a_i = \sum_{j=1}^{m} a_{i,j} \otimes u_j$, $1 \le i \le k$, *of* $S \otimes_R A$, *where* $a_{i,j} \in S$, *generate* $S \otimes_R A$ *as an* S*-algebra.*

(ii) *The ideal of* S *generated by all the values* $f(a_{1,1}, \dots, a_{k,m})$, *where* $f \in T$, *coincides with* S.

Proof. Consider polynomials p_j^M described in Lemma 2.16. It is clear that the same polynomials (or rather their images in $S[x_{1,1}, \dots, x_{k,m}]$) work for the S algebra $S \otimes_R A$ and its generators $1 \otimes u_1, \dots, 1 \otimes u_m$. Let $\mathcal{M} = \mathcal{M}(x_{i,j})$ be the matrix whose rows are labeled in some way by the monomials M of degree $< m$ in noncommuting variables $x_1, \dots, x_k$, and whose row with label M is

$$\big(p_1^M(x_{1,1}, \dots, x_{k,m}), \dots, p_m^M(x_{1,1}, \dots, x_{k,m})\big).$$

The $m \times m$ minors of $\mathcal{M}$ are polynomials in $R[x_{1,1}, \dots, x_{k,m}]$ of degree $\le m^2$. Consider the set T of all these minors. Consider elements $a_i = \sum_{j=1}^{m} a_{i,j} \otimes u_j$ in $S \otimes_R A$, where $a_{i,j} \in S$ and $1 \le i \le k$. Let B be the set of all elements of the form $M(a_1, \dots, a_k)$, where M is a monomial of degree $< m$. By Lemmas 2.8 and 2.6, the elements $a_1, \dots, a_k$ generate $S \otimes_R A$ as an S-algebra if and only if for every maximal ideal $\mathfrak{m}$ of S, the image of the set B in $S \otimes_R A/\mathfrak{m}(S \otimes_R A)$ spans the $S/\mathfrak{m}$-vector space $S \otimes_R A/\mathfrak{m}(S \otimes_R A)$. This is equivalent to saying that the reduction modulo $\mathfrak{m}$ of the matrix $\mathcal{M}(a_{i,j})$ has rank m, which in turn is equivalent to the condition that at least one of the $m \times m$ minors of $\mathcal{M}(a_{i,j})$ does not belong to $\mathfrak{m}$. Thus the set T of all the $m \times m$ minors of $\mathcal{M}(x_{i,j})$ has the required property. □

3. The density of the set of ordered k-tuples which generate an algebra

The results of this section arose from our attempt to answer the following question: what is the probability that k random elements of a ring A, whose additive group is free of finite rank, generate A as a ring. Before we answer this question, we need to make it more precise. We will discuss it in a slightly more general context.

Throughout this section K will be a number field of degree d over $\mathbb{Q}$, with the ring of integers O_K. We work with an order R in K, that is, R is a subring of K which is free of rank d as a $\mathbb{Z}$-module. We fix an integral basis $w_1, \dots, w_d$ of R over $\mathbb{Z}$. Any element r of R can be uniquely written as $r = \sum r_i w_i$ with $r_i \in \mathbb{Z}$. For a positive integer N we denote by $R(N)$ the set of all $r \in R$ such that $|r_i| \le N$ for all i. Clearly $|R(N)| = (2N+1)^d$.

Let A be an R-algebra which is free of finite rank m as an R-module. Fix a basis $e_1, \dots, e_m$ of A over R. This choice allows us to identify A and R^m. Using this identification we define $A(N)$ as $R^m(N)$, so $|A(N)| = (2N+1)^{dm}$. We define the density $\mathrm{den}_k(A)$ of the set of k generators of A as an R-algebra as follows.

Definition 3.1. $$\mathrm{den}_k(A) = \lim_{N \to \infty} \frac{|\mathrm{Gen}_k(A) \cap A(N)^k|}{(2N+1)^{dmk}}.$$

At the moment it is not clear whether the limit on the right in the last formula exists. We will show, however, that it exists and is independent of the choice of an integral basis of R and the choice of a basis of A over R.

Consider a maximal ideal $\mathfrak{p}$ of R. We denote by $\mathbb{F}_\mathfrak{p}$ the field $R/\mathfrak{p}$ and by $\mathrm{N}(\mathfrak{p})$ its cardinality. Recall that we say that elements $a_1, \ldots, a_k$ of A generate A at $\mathfrak{p}$ if their images in $A \otimes_R \mathbb{F}_\mathfrak{p}$ generate $A \otimes_R \mathbb{F}_\mathfrak{p}$ as an $\mathbb{F}_\mathfrak{p}$-algebra. Let $g_k(\mathfrak{p}, A)$ be the cardinality of the set $\mathrm{Gen}_k(A \otimes_R \mathbb{F}_\mathfrak{p})$. In other words, $g_k(\mathfrak{p}, A)$ is the number of k-tuples of elements of $A \otimes_R \mathbb{F}_\mathfrak{p}$ which generate $A \otimes_R \mathbb{F}_\mathfrak{p}$ as an $\mathbb{F}_\mathfrak{p}$-algebra. It is not hard to see that the density of the set $\mathrm{Gen}_k(\mathfrak{p}, A)$ of all k-tuples in A^k which generate A at $\mathfrak{p}$ is

$$\lim_{N\to\infty} \frac{|\mathrm{Gen}_k(\mathfrak{p}, A) \cap A(N)^k|}{(2N+1)^{dmk}} = \frac{g_k(\mathfrak{p}, A)}{N(\mathfrak{p})^{mk}}.$$

Note that by Lemma 2.6, a given k-tuple of elements of A generates it as an R-algebra if and only if it generates A at $\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of R. Suppose now that the events "generate at $\mathfrak{p}$" are independent for different maximal ideals (we use this notion in a very intuitive sense here, just to motivate our result). It would mean that the probability that random k elements of A generate it as an R-algebra is the product of the numbers $g_k(\mathfrak{p}, A)/\mathrm{N}(\mathfrak{p})^{mk}$ over all maximal ideals $\mathfrak{p}$ of R. One of the main results of this section is a rigorous proof that this is indeed true. In other words, we prove the following theorem.

Theorem 3.2. *Let A be an R-algebra which is free of rank m as an R-module and let $k > 0$ be an integer. For a maximal ideal $\mathfrak{p}$ of R denote by $g_k(\mathfrak{p}, A)$ the number of k-tuples of elements of $A \otimes_R \mathbb{F}_\mathfrak{p}$ which generate $A \otimes_R \mathbb{F}_\mathfrak{p}$ as an $\mathbb{F}_\mathfrak{p}$-algebra. Then*

$$\mathrm{den}_k(A) = \prod_{\mathfrak{p}\in \text{m-Spec } R} \frac{g_k(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{mk}}. \tag{2}$$

This result establishes in particular the existence and independence of all the choices of the limit defining the quantity $\mathrm{den}_k(A)$.

We will derive Theorem 3.2 as a consequence of a more general result. To this end consider the set $T = \{f_1, \ldots, f_s\}$ of polynomials in $R[x_{1,1}, \ldots, x_{k,m}]$ established in Lemma 2.17 (under our choice of a basis of A over R). We identify A^k with the set R^{mk} so that a tuple $(a_1, \ldots, a_k) \in A^k$ corresponds to $(a_{i,j}) \in R^{mk}$ if and only if $a_i = \sum_{j=1}^m a_{i,j} e_j$. Note that according to Lemma 2.17, the element $a = (a_{i,j}) \in R^{mk}$ corresponds to a k-tuple in $\mathrm{Gen}_k(A)$ if and only if the ideal of R generated by the elements $f_1(a), \ldots, f_s(a)$ coincides with R. Moreover, a corresponds to a k-tuple which generates A at $\mathfrak{p}$ if and only if $f_i(a) \notin \mathfrak{p}$ for some i. It follows that $g_k(\mathfrak{p}, A) = \mathrm{N}(\mathfrak{p})^{mk} - t_\mathfrak{p}$, where $t_\mathfrak{p}$ is the number of solutions to $f_1 = \cdots = f_s = 0$ over the finite field $\mathbb{F}_\mathfrak{p}$. It is clear now that Theorem 3.2 is a consequence of the following result.

Theorem 3.3. *Let R be an order in a number field K and let $T = \{f_1, \dots, f_s\} \subset R[x_1, \dots, x_n]$ be a finite set of polynomials. Define*

$$S = S(T) = \{x = (x_1, \dots, x_n) \in R^n : \text{the ideal generated by } f_1(x), \dots, f_s(x) \text{ is } R\}.$$

For each maximal ideal $\mathfrak{p}$ of R let $t_\mathfrak{p}$ be the number of solutions to $f_1 = \cdots = f_s = 0$ over the finite field $\mathbb{F}_\mathfrak{p} = R/\mathfrak{p}$. For a positive integer N let $S_N = S_N(T) = \{x \in S : x_i \in R(N), i = 1, 2, \dots, n\}$. Then

$$\lim_{N\to\infty} \frac{|S_N|}{(2N+1)^{dn}} = \prod_{\mathfrak{p}\in \text{m-Spec } R} \left(1 - \frac{t_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n}\right). \tag{3}$$

A proof of Theorem 3.3 is given in the next section. Note that for $s = 2$, $R = \mathbb{Z}$, and polynomials f_1 and f_2 that do not have a nonconstant common factor this result was proved in [Poonen 2003] in a slightly more general form (there the limit is taken over boxes whose sides all increase to infinity; here we only deal with boxes which are cubes). Poonen's result was inspired by [Ekedahl 1991], where a similar result has been established. Arnold [2009] considers the set of pairs of relatively prime integers as a subset of $\mathbb{Z}^2$ and proves that its density can be computed by using sets of the form nG, where G is any polygon (so our case corresponds to G being the square $|x| \le 1$, $|y| \le 1$). He calls subsets of $\mathbb{Z}^2$ (or, more generally, of $\mathbb{Z}^n$) which have this property *uniformly distributed*. In a subsequent paper we will discuss uniform distribution of sets of the type $S(T)$.

We end this section with an application of our theorems.

3A. *The probability that k random elements generate the group $\mathbb{Z}^n$.* In his work on generic properties of one-relator groups Ilya Kapovich was led to the following question: what is the probability that several randomly chosen elements generate the group $\mathbb{Z}^n$. Even though there is a fairly simple heuristic argument which leads to an answer, neither Kapovich nor we have been able to find a reference containing a proof. The techniques developed in this paper allow us, in particular, to give a rigorous answer to Kapovich's question. The key observation is contained in the following lemma.

Lemma 3.4. *Let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$. The number $\alpha_{m,n} = \alpha_{m,n}(q)$ of m-tuples of elements in V that span V is equal to $\prod_{i=0}^{n-1}(q^m - q^i)$.*

Proof. For $m < n$ the formula is obviously true as it yields 0 and there are no m-tuples which span V. The number $\alpha_{n,n}$ equals the number of bases of V, which is well known to be equal to $|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$. This establishes the result for $m = n$. Note now that $v_1, \dots, v_m$ span V if and only if the images of $v_2, \dots, v_m$ in $V/\langle v_1\rangle$ span $V/\langle v_1\rangle$. Given $v \in V$, we count the number of m-tuples

which span V and start with $v_1 = v$. If $v = 0$ this number is clearly $\alpha_{m-1,n}$. If $v \neq 0$, then there are $\alpha_{m-1,n-1}$ $(m-1)$-tuples which span $V/\langle v\rangle$ and each such tuple lifts to q^{m-1} $(m-1)$-tuples from V. Thus we get $q^{m-1}\alpha_{m-1,n-1}$ m-tuples which span V and start at v. Since there are $q^n - 1$ nonzero elements in V, we get the following recursive formula:

$$\alpha_{m,n} = \alpha_{m-1,n} + q^{m-1}(q^n - 1)\alpha_{m-1,n-1}.$$

The recursive formula and a straightforward induction on $m+n$ finish the proof. □

Theorem 3.5. *Let R be an order in a number field. Define*

$$\zeta_R(s) = \prod_{\mathfrak{p}\in \text{m-Spec}(R)} (1 - |R/\mathfrak{p}|^{-s})^{-1}.$$

For any $k \geq n$ the density of the set of k-tuples that generate the R-module R^n is equal to

$$\prod_{m=k-n+1}^{k} \zeta_R(m)^{-1}.$$

Proof. Consider R^n as an R-algebra with trivial multiplication and let A be obtained from R^n by the construction of adjunction of unity (in the category of R-algebras). By Lemma 2.3 we see that the density of the set of k-tuples which generate the R-module R^n is the same as the density $\text{den}_k(A)$ of the set of k-tuples which generate the R-algebra A. By Lemmas 2.3 and 2.4, we have $g_k(\mathfrak{p}, A) = \text{N}(\mathfrak{p})^k \alpha_{k,n}(\text{N}(\mathfrak{p}))$. By Theorem 3.2 and Lemma 3.4 we obtain the formula

$$\text{den}_k(A) = \prod_{\mathfrak{p}\in \text{m-Spec } R} \frac{\prod_{i=0}^{n-1}(\text{N}(\mathfrak{p})^k - \text{N}(\mathfrak{p})^i)}{\text{N}(\mathfrak{p})^{nk}} = \prod_{m=k-n+1}^{k} \zeta_R(m)^{-1}. \qquad \square$$

The answer to Ilya Kapovich's question is therefore given by the following corollary.

Corollary 3.6. *The probability that k randomly chosen elements generate the group $\mathbb{Z}^n$ is equal to $\prod_{m=k-n+1}^{k} \zeta(m)^{-1}$, where ζ is the Riemann zeta function.*

This corollary can also be derived directly from Theorem 3.3.

4. Proof of Theorem 3.3

Let us start by recalling some of the notation set down in the previous section. R is an order in a number field K. The degree of K over $\mathbb{Q}$ is d and O_K is the ring of integers of K (that is, the integral closure of R in K). We fix an integral basis $w_1, \ldots, w_d$ of R over $\mathbb{Z}$. Any element r of R can be uniquely written as $r = \sum_{i=1}^{d} r_i w_i$ with $r_i \in \mathbb{Z}$. For a positive integer N we denote by $R(N)$ the set of all $r \in R$ such that $|r_i| \leq N$ for all i. Clearly $|R(N)| = (2N+1)^d$. The norm

map from K to $\mathbb{Q}$ is denoted by $\mathrm{N}_{K/\mathbb{Q}}$. For an ideal I of R we set $\mathrm{N}_{K/\mathbb{Q}}(I)$ for the nonnegative integer which is the greatest common divisor of the norms of all elements in I. We write $\mathrm{N}(I)$ for the cardinality of R/I. If $\mathfrak{p}$ is a maximal ideal of R then we write $\mathbb{F}_{\mathfrak{p}}$ for the field $R/\mathfrak{p}$.

The following lemma is well known but for the readers convenience we include a short proof.

Lemma 4.1. *Let F be a finite field with q elements and let $f(x_1, \ldots, x_n)$ be a nonzero polynomial in $F[x_1, \ldots, x_n]$. Then the number of solutions of the equation $f(x_1, \ldots, x_n) = 0$ in F^n does not exceed* $(\deg f)q^{n-1}$.

Proof. We proceed by induction on n. For $n = 1$ this is just the statement that a polynomial f in one variable over a field has at most $\deg f$ roots. Suppose now that the result holds for polynomials in less than n variables and let $f(x_1, \ldots, x_n) = \sum_{i=0}^{d} f_i(x_1, \ldots, x_{n-1})x_n^i$ be a polynomial in n variables with $f_d \neq 0$. By the inductive assumption, the number of solutions to $f_d = 0$ in F^n does not exceed $(\deg f_d) \cdot q^{n-2} \cdot q = (\deg f_d)q^{n-1}$. For each $(a_1, \ldots, a_{n-1}) \in F^{n-1}$ such that $f_d(a_1, \ldots, a_{n-1}) \neq 0$ there are at most d solutions to $f(a_1, \ldots, a_{n-1}, x_n) = 0$. Thus we have at most $(\deg f_d)q^{n-1} + dq^{n-1} \leq (\deg f)q^{n-1}$ solutions to $f = 0$. □

Proposition 4.2. *Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a nonzero polynomial. Set*

$$Z(f, N) = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : |x_i| \leq N \text{ and } f(x_1, \ldots, x_n) = 0\}.$$

Then $|Z(f, N)| \leq (\deg f)(2N + 1)^{n-1}$.

Proof. We proceed by induction on n. For $n = 1$ the result is straightforward. Now assume the results for polynomials in less than n variables and consider a polynomial $f(x_1, \ldots, x_n) = \sum_{i=0}^{d} f_i(x_1, \ldots, x_{n-1})x_n^i$ in n variables with $f_d \neq 0$. By the inductive assumption, the number of elements in $Z(f, N)$ for which $f_d = 0$ does not exceed $(\deg f_d) \cdot (2N + 1)^{n-2} \cdot (2N + 1)$. For each $(a_1, \ldots, a_{n-1})$ such that $f_d(a_1, \ldots, a_{n-1}) \neq 0$ there are at most d solutions to $f(a_1, \ldots, a_{n-1}, x_n) = 0$. Thus we have at most $(\deg f_d)(2N+1)^{n-1} + d(2N+1)^{n-1} \leq (\deg f)(2N+1)^{n-1}$ elements in $Z(f, N)$. □

Corollary 4.3. *Let $f \in R[x_1, \ldots, x_n]$ be a polynomial of positive degree* $\deg f > 0$. *For a nonzero ideal J of R define*

$$I(f, J, N) = \{(x_1, \ldots, x_n) \in R(N)^n : J \subseteq f(x_1, \ldots, x_n)R\}.$$

Then $|I(f, J, N)| \leq \delta(J)d(\deg f)(2N + 1)^{dn-1}$, where $\delta(J)$ is the number of integral divisors of the norm $\mathrm{N}_{K/\mathbb{Q}}(J)$.

Proof. Write $x_i = \sum_{j=1}^{d} y_{i,j} w_j$. If $J \subseteq f(x_1, \ldots, x_n)R$ then $\mathrm{N}_{K/\mathbb{Q}}(f(x_1, \ldots, x_n))$ divides $\mathrm{N}_{K/\mathbb{Q}}(J)$. There is a polynomial $g(y_{i,j}) \in \mathbb{Z}[y_{1,1}, y_{1,2}, \ldots, y_{n,d}]$ of degree $(\deg f)d$ in dn variables such that

$$\mathrm{N}_{K/\mathbb{Q}}\big(f(x_1, \ldots, x_n)\big) = g(y_{i,j}).$$

The result follows now from Proposition 4.2 applied to each of the polynomials $g - k$, where k varies over all divisors of $\mathrm{N}_{K/\mathbb{Q}}(J)$. □

Theorem 4.4. *Let $f \in R[x_1, \ldots, x_n]$ be a polynomial of positive degree. For each maximal ideal $\mathfrak{p}$ of R let $f_\mathfrak{p}$ be the number of solutions to $f = 0$ over the finite field $\mathbb{F}_\mathfrak{p}$. Then the series $\sum_{\mathfrak{p} \in \text{m-Spec } R} f_\mathfrak{p}/\,\mathrm{N}(\mathfrak{p})^n$ diverges.*

Proof. Replacing R by O_K changes only a finite number of terms in the sum $\sum_\mathfrak{p} f_\mathfrak{p}/\,\mathrm{N}(\mathfrak{p})^n$. It suffices then to prove the theorem under the additional assumption that $R = O_K$.

Let L be a number field containing K, with ring of integers S, and such that f has an absolutely irreducible divisor $g \in S[x_1, \ldots, x_n]$ of positive degree (so $f/g \in L[x_1, \ldots, x_n]$). It is known that the reduction of g modulo all but a finite number of prime ideals of S is absolutely irreducible (see [Schmidt 1976, V.2]). For a maximal ideal P of S let g_P be the number of solutions to $g = 0$ in $(S/P)^n$. By [Schmidt 1976, V, Theorem 5A], we have

$$g_P \geq \tfrac{1}{2}\,|S/P|^{n-1} = \tfrac{1}{2}\,\mathrm{N}(P)^{n-1}$$

provided the reduction of g modulo P is absolutely irreducible and $\mathrm{N}(P)$ is sufficiently large, which holds for all but a finite number of maximal ideals of S.

Let Φ be the set of maximal ideals of S which have inertia degree one over R and let Ψ be the set of all prime ideals of R which lie under the ideals of Φ. Let $P \in \Phi$ be a prime ideal of S over $\mathfrak{p} \in \Psi$. Then $S/P = \mathbb{F}_\mathfrak{p}$. It follows that $f_\mathfrak{p} \geq g_P$ except possibly for a finite number of P for which f/g is not P-integral. Since each maximal ideal of R lies under at most $[L : K]$ prime ideals of S we get that

$$\sum_{\mathfrak{p} \in \text{m-Spec } R} \frac{f_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n} \geq \sum_{\mathfrak{p} \in \Psi} \frac{f_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n} \geq \frac{1}{[L : K]} \sum_{\substack{P \in \Phi \\ \mathrm{N}(P) \gg 0}} \frac{g_P}{\mathrm{N}(P)^n} \geq \frac{1}{2[L : K]} \sum_{\substack{P \in \Phi \\ \mathrm{N}(P) \gg 0}} \frac{1}{\mathrm{N}(P)}.$$

It is well known that the set Φ has Dirichlet density equal to 1 [Narkiewicz 1990, 7.2, Corollary 3]; in particular $\sum_{P \in \Phi} 1/\,\mathrm{N}(P)$ diverges. □

Corollary 4.5. *Under the assumptions of Theorem 3.3, if the polynomials in T have a common divisor of positive degree in $K[x_1, \ldots, x_n]$ then both sides of* (3) *are* 0*. In particular, Theorem 3.3 is true in this case.*

Proof. Let $f \in R[x_1, \ldots, x_n]$ be a polynomial of positive degree which divides all f_i in the ring $K[x_1, \ldots, x_n]$. There is a nonzero a in R such that af_i/f is in $R[x_1, \ldots, x_n]$ for all i. It follows that $S_N(T) \subseteq I(f, aR, N)$. By Corollary 4.3,

$$\frac{|S_N|}{(2N+1)^{dn}} \leq \frac{|I(f, aR, N)|}{(2N+1)^{dn}} \leq \frac{\delta(aR)d(\deg f)}{2N+1},$$

so the left-hand side of (3) is 0.

For any maximal ideal $\mathfrak{p}$ of R which does not divide a we have $t_\mathfrak{p} \geq f_\mathfrak{p}$. It follows from Theorem 4.4 that $\sum_{\mathfrak{p} \in \text{m-Spec } R} t_\mathfrak{p}/\,\mathrm{N}(\mathfrak{p})^n$ diverges. This is equivalent to the right-hand side of (3) being 0. □

Lemma 4.6. *Let $\mathfrak{p}$ be a maximal ideal of R with $\mathrm{N}(\mathfrak{p}) = p^s$, where p is the characteristic of $\mathbb{F}_\mathfrak{p}$. Then any element of $\mathbb{F}_\mathfrak{p}$ lifts to at most $(2N+1)^{d-s}(1+2N/p)^s$ elements in $R(N)$.*

Proof. We may assume (after renumbering, if necessary) that $w_1, \ldots, w_s$ is a basis of $\mathbb{F}_\mathfrak{p}$ over $\mathbb{F}_p$. Consider a residue class $a \in \mathbb{F}_\mathfrak{p}$. To get an element $\sum_{i=1}^d y_i w_i \in R(N)$ in the given residue class a we may choose arbitrarily integers $y_{s+1}, \ldots, y_d$ in $[-N, N]$ and then the residue classes of $y_1, \ldots, y_s$ modulo p are uniquely determined. Thus each y_i, $i \leq s$, can be chosen in at most $1 + 2N/p$ ways. □

Lemma 4.7. *Let $f \in R[x_1, \ldots, x_{n-1}]$, $g = g_0 x_n^k + \cdots + g_k \in R[x_1, \ldots, x_n]$, where $g_0, \ldots, g_k \in R[x_1, \ldots, x_{n-1}]$ and $g_0 \neq 0$. Consider the set*

$$D(N) = \big\{(x_1, \ldots, x_n) \in R(N)^n : f(x_1, \ldots, x_{n-1}) \neq 0 \text{ and there exists a maximal ideal } \mathfrak{p} \text{ with } \mathrm{N}(\mathfrak{p}) > N \text{ and such that } f(x_1, \ldots, x_{n-1}) \in \mathfrak{p}, \; g(x_1, \ldots, x_n) \in \mathfrak{p}, \text{ and } g_0(x_1, \ldots, x_{n-1}) \notin \mathfrak{p}\big\}.$$

Then there is a constant c such that $|D(N)| \leq c(2N+1)^{dn-1}$ for all N.

Proof. There are positive integers w and c_1 such that

$$|\mathrm{N}_{K/\mathbb{Q}}\, f(x_1, \ldots, x_{n-1})| \leq c_1 N^w,$$

for any $N \geq 1$ and any $x_i \in R(N)$, $i = 1, \ldots, n-1$. If $N > c_1$ and $f(x_1, \ldots, x_{n-1})$ is nonzero, then $f(x_1, \ldots, x_{n-1})$ belongs to at most w maximal ideals $\mathfrak{p}$ such that $\mathrm{N}(\mathfrak{p}) > N$. In fact, if there were more than w maximal ideals in R with norm exceeding N which contain $f(x_1, \ldots, x_{n-1})$ then $f(x_1, \ldots, x_{n-1})$ would belong to at least $w+1$ maximal ideals of O_K of norm exceeding N and this would imply that $|\mathrm{N}_{K/\mathbb{Q}}\, f(x_1, \ldots, x_{n-1})| > N^{w+1}$, which is not possible. Let

$$G(N, \mathfrak{p}) = \big\{(x_1, \ldots, x_{n-1}) \in R(N)^{n-1} : f(x_1, \ldots, x_{n-1}) \in \mathfrak{p} - \{0\}\big\}.$$

Thus, if $N > c_1$ and $(x_1, \ldots, x_{n-1}) \in R(N)^{n-1}$, then there are at most w maximal ideals $\mathfrak{p}$ such that $\mathrm{N}(\mathfrak{p}) > N$ and $(x_1, \ldots, x_{n-1}) \in G(N, \mathfrak{p})$. Let $N > c_1$. Fix a

point $(x_1, \dots, x_{n-1}) \in R(N)^{n-1}$ and let $\mathfrak{p}$ be a maximal ideal such that $\mathrm{N}(\mathfrak{p}) > N$ and $(x_1, \dots, x_{n-1}) \in G(N, \mathfrak{p})$. We want to find an upper bound for the number of $x_n \in R(N)$ such that $g(x_1, \dots, x_n) \in \mathfrak{p}$ and $g_0(x_1, \dots, x_{n-1}) \notin \mathfrak{p}$. All such x_n split into at most k residue classes modulo $\mathfrak{p}$ (which correspond to the roots of $g(x_1, \dots, x_{n-1}, x) = 0$ in $\mathbb{F}_{\mathfrak{p}}$). Let $\mathrm{N}(\mathfrak{p}) = p^s$, where $p = \mathrm{char}\, F_{\mathfrak{p}}$. By Lemma 4.6, the number of $x_n \in R(N)$ which belong to a given residue class modulo $\mathfrak{p}$ is at most

$$\begin{aligned}(2N+1)^{d-s} \max\bigl(2, 2(2N+1)/p\bigr)^s &\le \max\bigl(2^s(2N+1)^{d-s}, 2^s(2N+1)^s/p^s\bigr)\\ &\le 3 \cdot 2^s \cdot (2N+1)^{d-1}\end{aligned}$$

(we have used the inequalities $1 + 2N/p \le \max(2, 2(2N+1)/p)$ and $p^s > N \ge (2N+1)/3$). It follows that there are at most $w \cdot k \cdot 3 \cdot 2^s (2N+1)^{d-1}$ values of $x_n \in R(N)$ such that $(x_1, \dots, x_n) \in D(N)$. Hence, if $N > c_1$, then

$$|D(N)| \le (2N+1)^{d(n-1)} \cdot w \cdot k \cdot 3 \cdot 2^s \cdot (2N+1)^{d-1} \le c(2N+1)^{dn-1},$$

where $c = 3 \cdot 2^s \cdot w \cdot k$. We can increase c if necessary so that the inequality $|D(N)| \le c(2N+1)^{dn-1}$ holds for all N. □

Lemma 4.8. *Let f be a nonzero polynomial in $R[x_1, \dots, x_{n-1}]$ and let*

$$g = g_0 x_n^k + \cdots + g_k \in R[x_1, \dots, x_n],$$

where $g_0, \dots, g_k \in R[x_1, \dots, x_{n-1}]$, $g_0 \ne 0$. For a maximal ideal $\mathfrak{p}$ of R consider the set

$$\begin{aligned}D_{\mathfrak{p}}(N) = \{(x_1, \dots, x_n) \in R(N)^n : f(x_1, \dots, x_{n-1}) \in \mathfrak{p},\\ g(x_1, \dots, x_n) \in \mathfrak{p},\ \textit{and}\ g_0(x_1, \dots, x_{n-1}) \notin \mathfrak{p}\}.\end{aligned}$$

Then, if $\mathrm{N}(\mathfrak{p}) \le N$ and the reduction of f modulo $\mathfrak{p}$ is not zero, we have

$$|D_{\mathfrak{p}}(N)| \le 2^{nd} (\deg f) k (2N+1)^{nd} / \mathrm{N}(\mathfrak{p})^2.$$

Proof. The image $Z_{\mathfrak{p}}$ of $D_{\mathfrak{p}}(N)$ in $\mathbb{F}_{\mathfrak{p}}^n$ consists of (some) solutions to $f = 0 = g$ in $\mathbb{F}_{\mathfrak{p}}^n$ (we use the same notation for a polynomial and its reduction modulo $\mathfrak{p}$). Now $f = 0$ has at most $(\deg f)\, \mathrm{N}(\mathfrak{p})^{n-2}$ solutions in $\mathbb{F}_p^{n-1}$ (Lemma 4.1) and each such solution extends to at most k solutions of $g = 0$, $g_0 \ne 0$ in $\mathbb{F}_{\mathfrak{p}}^n$. Thus $|Z_{\mathfrak{p}}| \le (\deg f) k\, \mathrm{N}(\mathfrak{p})^{n-2}$. Each element of $Z_{\mathfrak{p}}$ lifts to no more that $[(2N+1)^{d-s}(1 + 2N/p)^s]^n$ elements of $D_{\mathfrak{p}}(N)$ by Lemma 4.6, where $\mathrm{N}(\mathfrak{p}) = p^s$. Thus

$$\begin{aligned}|D_{\mathfrak{p}}(N)| &\le (\deg f) k\, \mathrm{N}(\mathfrak{p})^{n-2} [(2N+1)^{d-s}(1 + 2N/p)^s]^n\\ &\le (\deg f) k\, \mathrm{N}(\mathfrak{p})^{n-2} (2N+1)^{n(d-s)} [2^s (2N+1)^s / p^s]^n\\ &\le 2^{nd} (\deg f) k\, \mathrm{N}(\mathfrak{p})^{n-2} (2N+1)^{nd} / \mathrm{N}(\mathfrak{p})^n\\ &= 2^{nd} (\deg f) k (2N+1)^{nd} / \mathrm{N}(\mathfrak{p})^2.\end{aligned}$$

□

Proposition 4.9. *Let $f, g \in R[x_1, \ldots, x_n]$ be polynomials which are relatively prime as polynomials in $K[x_1, \ldots, x_n]$. Define*

$$W_M = W_M(f, g) = \{\mathbf{r} = (r_1, \ldots, r_n) \in R^n : \text{there is a maximal ideal } \mathfrak{p} \text{ of } R, \text{ with } \mathrm{N}(\mathfrak{p}) > M \text{ and such that } f(\mathbf{r}) \in \mathfrak{p} \text{ and } g(\mathbf{r}) \in \mathfrak{p}\}.$$

There is a constant $c > 0$ such that

$$|W_M \cap R(N)^n| \leq c\frac{(2N+1)^{nd}}{M}$$

for any integers $N > M \geq 1$.

Proof. We use induction on the number n of variables. Note that if f and g are polynomials in n variables for which the result holds, then it also holds for f and g considered as polynomials in $n+1$ variables. When $n = 0$ the result is clear. Suppose the result is true for less than $n \geq 1$ variables. Consider two relatively prime (in $K[x_1, \ldots, x_n]$) polynomials $f, g \in R[x_1, \ldots, x_n]$.

The first step is to establish the proposition under the additional assumption that f is irreducible in $K[x_1, \ldots, x_n]$ and does not depend on x_n (that is, f is in $R[x_1, \ldots, x_{n-1}]$). Let $g = g_0 x_n^k + \cdots + g_k$, where $g_0, \ldots, g_k \in R[x_1, \ldots, x_{n-1}]$, $g_0 \neq 0$. We fix f and proceed by induction on the degree k of g in x_n. If $k = 0$ then $g \in R[x_1, \ldots, x_{n-1}]$ and the result follows by our inductive assumption that the proposition holds for polynomials in $n-1$ variables. Suppose that $k > 0$ and the result holds for all polynomials g whose degree in x_n is less than k (and which are relatively prime to f). We may write $ag = \prod h_i$ for some nonzero a in R and polynomials $h_i \in R[x_1, \ldots, x_n]$ which are irreducible in $K[x_1, \ldots, x_n]$. Note that $W_M(f, g) \subseteq \bigcup W_M(f, h_i)$. Thus, if we show the proposition for each pair f, h_i, then it will also hold for the pair f, g. In other words, we may assume that g is irreducible in $K[x_1, \ldots, x_n]$. If $f \,|\, g_0$ in $K[x_1, \ldots, x_{n-1}]$, then there is a nonzero $u \in R$ such that $f \,|\, ug_0$ in $R[x_1, \ldots, x_{n-1}]$. It follows that

$$W_M(f, g) \subseteq W_M(f, u(g - g_0 x_n^k))$$

for all M. Since $u(g - g_0 x_n^k)$ has degree in x_n smaller than k, the result holds for $f, u(g - g_0 x_n^k)$ by our inductive assumption and therefore it also holds for the pair f, g. Thus we may assume that f does not divide g_0 in $K[x_1, \ldots, x_{n-1}]$. Since f is irreducible, f and g_0 are relatively prime in $K[x_1, \ldots, x_{n-1}]$. For $N > M$ we have

$$W_M(f, g) \cap R(N)^n \subseteq (W_M(f, g_0) \cap R(N)^n) \cup Z(f, N) \cup D(N) \cup \bigcup_{\mathfrak{p}: M < \mathrm{N}(\mathfrak{p}) \leq N} D_{\mathfrak{p}}(N),$$

where

$$Z(f, N) = \{\mathbf{r} = (r_1, \ldots, r_n) \in R(N)^n : f(\mathbf{r}) = 0\},$$

$$D(N) = \big\{\mathbf{r} \in R(N)^n : \text{ there is a maximal ideal } \mathfrak{p} \text{ such that } \mathrm{N}(\mathfrak{p}) > N, \\ f(\mathbf{r}) \in \mathfrak{p} - \{0\},\, g(\mathbf{r}) \in \mathfrak{p}, \text{ and } g_0(\mathbf{r}) \notin \mathfrak{p}\big\},$$

$$D_{\mathfrak{p}}(N) = \{\mathbf{r} \in R(N)^n : f(\mathbf{r}) \in \mathfrak{p},\, g(\mathbf{r}) \in \mathfrak{p},\, g_0(\mathbf{r}) \notin \mathfrak{p}\}.$$

By our inductive assumption that the proposition holds for polynomials in $n-1$ variables, there is $c_1 > 0$ such that $|W_M(f, g_0) \cap R(N)^n| \le c_1(2N+1)^{dn}/M$ for any integers $N > M \ge 1$. Note that if $f(\mathbf{r}) = 0$ then $(f-1)(\mathbf{r})R = R$. It follows by Corollary 4.3 applied to the polynomial $f-1$ and the ideal $J = R$ that

$$|Z(f, N)| \le \delta(R) d(\deg f)(2N+1)^{dn-1} \le c_2 \frac{(2N+1)^{dn}}{M}$$

for some $c_2 > 0$ and all $N > M \ge 1$. Lemma 4.7 assures the existence of $c_3 > 0$ such that $|D(N)| \le c_3(2N+1)^{dn-1} \le c_3(2N+1)^{dn}/M$. Finally, by Lemma 4.8, there are constants $c_4 > 0$, $c_5 > 0$ such that

$$\Big|\bigcup_{\mathfrak{p}:M<\mathrm{N}(\mathfrak{p})\le N} D_{\mathfrak{p}}(N)\Big| \le \sum_{\mathfrak{p}:M<\mathrm{N}(\mathfrak{p})\le N} |D_{\mathfrak{p}}(N)| \le \sum_{\mathfrak{p}:M<\mathrm{N}(\mathfrak{p})\le N} 2^{nd}(\deg f) d \frac{(2N+1)^{nd}}{\mathrm{N}(\mathfrak{p})^2}$$

$$\le c_4(2N+1)^{nd} \sum_{\mathfrak{p}:M<\mathrm{N}(\mathfrak{p})} \mathrm{N}(\mathfrak{p})^{-2} \le c_4(2N+1)^{nd} d \sum_{m>M} \frac{1}{m^2} \le c_5 \frac{(2N+1)^{nd}}{M}.$$

It follows that $|W_M(f, g) \cap R(N)^n| \le c(2N+1)^{nd}/M$, where $c = c_1 + c_2 + c_3 + c_5$. This completes our first step, that is, establishes the proposition under the additional assumption that f is irreducible in $K[x_1, \ldots, x_n]$ and does not depend on x_n.

Our second step is to prove the proposition when both f and g are irreducible in $K[x_1, \ldots, x_n]$. Consider f and g as polynomials in x_n with coefficients in $R[x_1, \ldots, x_{n-1}]$. If one of these polynomials does not depend on x_n, the proposition holds by our first step. Suppose that the degrees with respect to x_n of both f and g are positive. Let $r = \mathrm{Res}(f, g)$ be the resultant of f and g, so r is a nonzero polynomial in $R[x_1, \ldots, x_{n-1}]$. Recall that $r = af + bg$ for some polynomials $a, b \in R[x_1, \ldots, x_n]$ (see [Cox et al. 2005, §3.1] for a nice account of properties of resultants). It follows that $W_M(f, g) \subseteq W_M(f, r) \cap W_M(g, r)$. Since f and g are irreducible, g and r have no common factor in $K[x_1, \ldots, x_n]$ (otherwise g would not depend on x_n). We may write $ar = \prod r_i$, where $r_i \in R[x_1, \ldots, x_{n-1}]$ are irreducible in $K[x_1, \ldots, x_{n-1}]$ and $a \in R$ is nonzero. Clearly $W_M(f, g) \subseteq W_M(r, g) \subseteq \bigcup W_M(r_i, g)$. Since the proposition holds for each pair r_i, g by the first step, it also holds for the pair f, g.

Finally, without any additional assumptions, we may write $af = \prod f_i$, $bg = \prod g_i$, where $f_i, g_j \in R[x_1, \ldots, x_n]$ are irreducible in $K[x_1, \ldots, x_n]$ and $a, b \in R - \{0\}$. Clearly $W_M(f, g) \subseteq \bigcup W_M(f_i, g_j)$. Since the result holds for each pair f_i, g_j, it also holds for f, g. □

Corollary 4.10. *Let $T=\{f_1, \ldots, f_s\}$ be a finite set of polynomials in $R[x_1, \ldots, x_n]$ which do not have any common nonconstant divisor in $K[x_1, \ldots, x_n]$. Define*

$$W_M = W_M(T) = \{\mathbf{r} = (r_1, \ldots, r_n) \in R^n : \text{ there is a maximal ideal } \mathfrak{p} \text{ of } R \text{ with } \mathrm{N}(\mathfrak{p}) > M \text{ and such that } f(\mathbf{r}) \in \mathfrak{p} \text{ for every } f \in T\}.$$

There is a constant $c > 0$ such that $|W_M \cap R(N)^n| \leq c(2N+1)^{nd}/M$ for any integers $N > M \geq 1$.

Proof. We may write $d_i f_i = \prod f_{i,j}$, where $f_{i,j} \in R[x_1, \ldots, x_n]$ are irreducible in $K[x_1, \ldots, x_n]$ and $d_i \in R$ are nonzero. Then

$$W_M \subseteq \bigcup W_M(f, g),$$

where the union is over all pairs f, g such that f and g are among the polynomials $f_{i,j}$ and are relatively prime. Thus the result follows by Proposition 4.9. □

Corollary 4.10 is the main ingredient in our proof of Theorem 3.3. In fact, the proof now reduces to a fairly straightforward application of the inclusion-exclusion formula and the Chinese remainder theorem. For the benefit of the reader we provide a detailed argument.

Lemma 4.11. *Let I be a nonzero ideal of R. If m is a positive integer such that $mR \subseteq I$ then*

$$\frac{(2N-m)^d}{\mathrm{N}(I)} \leq |(a+I) \cap R(N)| \leq \frac{(2N+m)^d}{\mathrm{N}(I)}$$

for any $a \in R$ and any N such that $2N \geq m$.

Proof. The ideal I is a union of $m^d/\mathrm{N}(I)$ cosets of mR. Thus any coset of I is also a union of $m^d/\mathrm{N}(I)$ cosets of mR. Any coset H of mR is of the form

$$\sum_{i=1}^{d} a_i w_i + mR,$$

where $0 \leq a_i < m$. The elements of $H \cap R(N)$ are exactly those of the form $\sum_{i=1}^{d}(a_i + mb_i)w_i$ with $|a_i + mb_i| \leq N$. Thus $(-N - a_i)/m \leq b_i \leq (N - a_i)/m$. Recall now that an interval of length l has at least $l-1$ and at most $l+1$ integers in it. It follows that $(2N/m - 1)^d \leq |H \cap R(N)| \leq (2N/m + 1)^d$. Since $a + I$ is a disjoint union of $m^d/\mathrm{N}(I)$ cosets of mR, the result follows. □

Lemma 4.12. *Let I be a nonzero ideal of R. If V is a subset of $(R/I)^n$ and $V(N)$ is the set of elements of $R(N)^n$ whose image in $(R/I)^n$ belongs to V then*

$$\lim_{N\to\infty} \frac{|V(N)|}{(2N+1)^{nd}} = \frac{|V|}{\mathrm{N}(I)^n}.$$

Proof. Since both sides of the equality are additive for disjoint unions, it suffices to prove the lemma for sets V which contain only one element. In this case, there are cosets $a_1 + I, \ldots, a_n + I$ of I such that

$$V(N) = \big((a_1 + I) \cap R(N)\big) \times \cdots \times \big((a_n + I) \cap R(N)\big).$$

There is a positive integer m such that $mR \subseteq I$. By Lemma 4.11, we have

$$\frac{(2N - m)^{dn}}{\mathrm{N}(I)^n} \leq |V(N)| \leq \frac{(2N + m)^{dn}}{\mathrm{N}(I)^n}$$

provided $2N \geq m$. Dividing by $(2N+1)^{dn}$ and passing to the limit when $N \to \infty$, we get the result. □

Proof of Theorem 3.3. If the polynomials in T have a common divisor in $K[x_1, \ldots, x_n]$ the theorem holds by Corollary 4.5. Thus we may assume that elements of T do not have any common nonconstant divisor in $K[x_1, \ldots, x_n]$. For a prime ideal $\mathfrak{p}$ of R define

$$D_{\mathfrak{p}} = \{\mathbf{r} = (r_1, \ldots, r_n) \in R^n : f(\mathbf{r}) \in \mathfrak{p} \text{ for every } f \in T\}.$$

Let Φ be a finite set of maximal ideals of R. For any subset Ψ of Φ we denote by $I(\Psi)$ the intersection of all the ideals in Ψ. Note that

$$D_\Psi := \bigcap_{\mathfrak{p} \in \Psi} D_{\mathfrak{p}} = \{\mathbf{r} = (r_1, \ldots, r_n) \in R^n : f(\mathbf{r}) \in I(\Psi) \text{ for every } f \in T\}.$$

Let V_Ψ be the image of D_Ψ in $(R/I(\Psi))^n$. Thus V_Ψ is simply the set of all common zeros in $(R/I(\Psi))^n$ of the polynomials in T. By the Chinese remainder theorem, we have $R/I(\Psi) \cong \prod_{\mathfrak{p} \in \Psi} R/\mathfrak{p}$ and under this identification we have $V_\Psi = \prod_{\mathfrak{p} \in \Psi} V_{\mathfrak{p}}$. It follows that $|V_\Psi| = \prod_{\mathfrak{p} \in \Psi} t_{\mathfrak{p}}$. Applying Lemma 4.12 to the set V_Ψ and observing that $V_\Psi(N) = D_\Psi \cap R(N)^n$ we get

$$\lim_{N \to \infty} \frac{|D_\Psi \cap R(N)^n|}{(2N+1)^{nd}} = \frac{\prod_{\mathfrak{p} \in \Psi} t_{\mathfrak{p}}}{\mathrm{N}(I(\Psi))^n} = \prod_{\mathfrak{p} \in \Psi} \frac{t_{\mathfrak{p}}}{\mathrm{N}(\mathfrak{p})^n}.$$

Let W_Φ be the complement of the union $\bigcup_{\mathfrak{p} \in \Phi} D_{\mathfrak{p}}$ in R^n. The inclusion-exclusion principle yields the following formula:

$$|W_\Phi \cap R(N)^n| = \sum_{\Psi \subseteq \Phi} (-1)^{|\Psi|} |D_\Psi \cap R(N)^n|$$

(where $D_\varnothing = R^n$), from which we immediately conclude that

$$\lim_{N \to \infty} \frac{|W_\Phi \cap R(N)^n|}{(2N+1)^{nd}} = \sum_{\Psi \subseteq \Phi} (-1)^{|\Psi|} \prod_{\mathfrak{p} \in \Psi} \frac{t_{\mathfrak{p}}}{\mathrm{N}(\mathfrak{p})^n} = \prod_{\mathfrak{p} \in \Phi} \left(1 - \frac{t_{\mathfrak{p}}}{\mathrm{N}(\mathfrak{p})^n}\right).$$

Suppose now that Φ is the set of all prime ideals of norm $\leq M$. Note that

$$S(T) \subseteq W_\Phi \subseteq S(T) \cup W_M(T),$$

where $W_M(T)$ is defined in Corollary 4.10 and $S(T)$ in Theorem 3.3. Thus

$$|W_\Phi \cap R(N)^n| - |W_M(T) \cap R(N)^n| \leq |S(T) \cap R(N)^n| \leq |W_\Phi \cap R(N)^n|.$$

Note that Corollary 4.10 implies that

$$0 \leq \liminf_{N\to\infty} \frac{|W_M(T) \cap R(N)^n|}{(2N+1)^{dn}} \leq \limsup_{N\to\infty} \frac{|W_M(T) \cap R(N)^n|}{(2N+1)^{dn}} \leq \frac{c}{M}.$$

This yields

$$\prod_{\mathfrak{p}:\mathrm{N}(\mathfrak{p})\leq M} \left(1 - \frac{t_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n}\right) - \frac{c}{M} \leq \liminf_{N\to\infty} \frac{|S(T) \cap R(N)^n|}{(2N+1)^{dn}}$$
$$\leq \limsup_{N\to\infty} \frac{|S(T) \cap R(N)^n|}{(2N+1)^{dn}} \leq \prod_{\mathfrak{p}:\mathrm{N}(\mathfrak{p})\leq M} \left(1 - \frac{t_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n}\right).$$

Letting M go to infinity we see that

$$\lim_{N\to\infty} \frac{|S(T) \cap R(N)^n|}{(2N+1)^{dn}} = \prod_{\mathfrak{p}\in \text{m-Spec } R} \left(1 - \frac{t_\mathfrak{p}}{\mathrm{N}(\mathfrak{p})^n}\right). \qquad \square$$

5. The smallest number of generators

Let us return to our discussion of generators of algebras. We first show an application of Theorem 3.2. Let A be an algebra over a commutative ring R, which is finitely generated as an R-module.

Definition 5.1. We denote by $r = r(A) = r(A, R)$ the smallest number of elements which are needed to generate A as an R-algebra.

For a prime ideal $\mathfrak{p}$ of R define

$$r_\mathfrak{p} = r_\mathfrak{p}(A) = r\big(A \otimes_R \kappa(\mathfrak{p}), \kappa(\mathfrak{p})\big),$$

where $\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is the field of fractions of $R/\mathfrak{p}$.

Note that $r_\mathfrak{p}$ is the smallest number of generators of $A_\mathfrak{p}$ as an $R_\mathfrak{p}$-algebra by Lemma 2.6. Clearly $r_\mathfrak{p} \leq r$ for every $\mathfrak{p} \in \operatorname{Spec} R$ and $r_\mathfrak{p} \leq r_\mathfrak{q}$ whenever $\mathfrak{p} \subseteq \mathfrak{q}$ by Corollary 2.11. The first main result of this section is the following theorem.

Theorem 5.2. *Let R be an order in a number field K and let A be an R-algebra which is free as an R-module. Suppose that $k \geq r_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of R and $k \geq 1 + r_0$. Then* $\operatorname{den}_k(A) > 0$. *In particular, $k \geq r$.*

Our proof of Theorem 5.2 will use the following nice result, often called the Loomis–Whitney inequality [Loomis and Whitney 1949].

Lemma 5.3. *Let T be a finite set, D a subset of T^s, and let D_i be the projection of D to T^{s-1} along the i-th coordinate. Then $|D|^{s-1} \le \prod_{i=1}^{s} |D_i|$.*

As a corollary we get the following lemma.

Lemma 5.4. *Let $\mathbb{F}$ be a finite field with q elements. Suppose that an m-dimensional $\mathbb{F}$-algebra A can be generated by r elements as an $\mathbb{F}$-algebra. For $k \ge r$ let ng_k be the number of k-tuples in A^k which do not generate A as an $\mathbb{F}$-algebra. Then $\mathrm{ng}_k \le m^{2k/r} q^{mk-k/r}$ for any $k > r$.*

Proof. Let $D(k) \subseteq A^k$ be the set of all k-tuples which do not generate A as an $\mathbb{F}$-algebra. For each i the projection $D(k)_i \subseteq A^{k-1}$ of $D(k)$ along the i-th coordinate is contained in $D(k-1)$. By the Loomis–Whitney inequality (Lemma 5.3) we have

$$\mathrm{ng}_k^{k-1} \le \mathrm{ng}_{k-1}^{k}.$$

A straightforward induction yields now the inequality

$$\mathrm{ng}_k \le \mathrm{ng}_r^{k/r}.$$

The set $D(r)$ is contained in the set of all zeros of some nonzero polynomial of degree $\le m^2$ in rm variables by Lemma 2.17. It follows that $|D(r)| = \mathrm{ng}_r \le m^2 q^{mr-1}$ by Lemma 4.1. Consequently,

$$\mathrm{ng}_k \le \mathrm{ng}_r^{k/r} \le m^{2k/r} q^{km-k/r}. \qquad \square$$

Proof of Theorem 5.2. Recall that by Theorem 3.2 we have

$$\mathrm{den}_k(A) = \prod_{\mathfrak{p} \in \text{m-Spec } R} \frac{g_k(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{mk}},$$

where m is the rank of the free R-module A. Since $k \ge r_{\mathfrak{p}}$, we see that $g_k(\mathfrak{p}, A) > 0$ for all maximal ideals $\mathfrak{p}$. It suffices therefore to show that

$$\prod \frac{g_k(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{mk}} > 0,$$

where the product is over all maximal ideals with sufficiently large norm. Since the set of all prime ideals $\mathfrak{p}$ of R such that $r_{\mathfrak{p}} = r_0$ is open and contains the zero ideal, we have $r_{\mathfrak{p}} = r_0$ for all but a finite number of maximal ideals $\mathfrak{p}$. Since $k \ge r_0 + 1$, Lemma 5.4 implies that $g_k(\mathfrak{p}, A) \ge \mathrm{N}(\mathfrak{p})^{km} - m^{2k/r_0}\,\mathrm{N}(\mathfrak{p})^{km-k/r_0}$ for every $\mathfrak{p} \in \text{m-Spec } R$ such that $r_0 = r_{\mathfrak{p}}$. It follows that

$$\frac{g_k(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{mk}} \ge 1 - \frac{m^{2k/r_0}}{\mathrm{N}(\mathfrak{p})^{k/r_0}}$$

for all but a finite number of maximal ideals $\mathfrak{p}$. It suffices therefore to show that

$$\prod \left(1 - \frac{m^{2k/r_0}}{\mathrm{N}(\mathfrak{p})^{k/r_0}}\right) > 0,$$

where the product is over all maximal ideals with sufficiently large norm. This in turn is equivalent to showing that the series

$$\sum_{\mathfrak{p} \in \text{m-Spec } R} \frac{m^{2k/r_0}}{\mathrm{N}(\mathfrak{p})^{k/r_0}}$$

converges, which is indeed true since $k/r_0 > 1$. □

As an immediate corollary of Theorem 5.2 we get the following.

Theorem 5.5. *Let R be an order in a number field K and let A be an R-algebra which is free as an R-module. If $r_0 < r_{\mathfrak{p}}$ for some maximal ideal $\mathfrak{p}$ of R then $r = \max\{r_{\mathfrak{p}} : \mathfrak{p} \in \text{m-Spec } R\}$. If $r_0 = r_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{p}$ then $r_0 \le r \le 1 + r_0$.*

A special case of Theorem 5.5 when $R = \mathbb{Z}$ was shown to us by H. W. Lenstra (private communication, 2007). His proof of this result is purely algebraic and does not provide any way to handle the ambiguity for r when $r_0 = r_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{p}$. It is known that in this case both $r = r_0$ and $r = r_0 + 1$ are possible. For example, there are infinitely many number fields in which the ring of integers A considered as a $\mathbb{Z}$-algebra has $r_{\mathfrak{p}} = 1$ for all prime ideals $\mathfrak{p}$ but $r = 2$. As an explicit example one can take the ring of integers in the cubic field $\mathbb{Q}(\sqrt[3]{198})$ [Pleasants 1974, p. 167]. Later, we will see examples where $\mathrm{den}_{r_0}(A) > 0$, hence $r = r_0$, even though we are unable to find generators.

Question 5.6. Let R be an order in a number field. Suppose that A is an R-algebra which is finitely generated and projective as an R-module. The right-hand side of the formula in Theorem 3.2 makes perfect sense for A and we will continue to denote it by $\mathrm{den}_k A$. Is it true that if $\mathrm{den}_k A > 0$ then A can be generated by k elements as an R-algebra? We believe that the answer is positive. Perhaps there is a notion of density in this case which makes Theorem 3.2 valid?

We have the following generalization of the original result of Lenstra.

Theorem 5.7. *Let R be a commutative ring of dimension ≤ 1 such that* m-Spec R *is Noetherian and let A be an R-algebra finitely generated as an R-module. Let h be the smallest nonnegative integer such that $h \ge r_{\mathfrak{p}}$ for all but a finite number of maximal ideals $\mathfrak{p}$ of R. Suppose that $k \ge r_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{p}$ and $k \ge 1 + h$. Then A can be generated by k elements as an R-algebra.*

Proof. Since m-Spec R is Noetherian, it has a finite number of irreducible components. Note that if an irreducible component of m-Spec R is finite then it consists of a single maximal ideal. Otherwise it contains infinitely many maximal ideals

and the intersection of all these ideals is a prime ideal which we call the generic ideal of the component. Let T be the set of all prime ideals which are generic ideals of some infinite irreducible component of m-Spec R. Thus T is a finite set of minimal prime ideals of R (it can be empty). Note that if $\mathfrak{p} \in T$ then $r_{\mathfrak{p}} \leq r_{\mathfrak{q}}$ for any maximal ideal $\mathfrak{q}$ containing $\mathfrak{p}$ and the equality holds for all but a finite number of such maximal ideals by Corollary 2.11. It follows that $h = \max\{r_{\mathfrak{p}} : \mathfrak{p} \in T\}$. For each prime $\mathfrak{p} \in T$ choose a maximal ideal $\mathfrak{q} \supseteq \mathfrak{p}$ such that $r_{\mathfrak{p}} = r_{\mathfrak{q}}$ and denote this set of chosen maximal ideals by M.

We call a sequence $a_1, \ldots, a_m$ of elements of A *M-generic* if it generates A at $\mathfrak{p}$ for every $\mathfrak{p} \in M$. Note that an M-generic sequence generates A at $\mathfrak{p}$ for all but a finite number of maximal ideals $\mathfrak{p}$. We claim that there is an M-generic sequence of length h. Indeed, for each $\mathfrak{q} \in M$ there are h elements in A which generate A at $\mathfrak{q}$. By the Chinese remainder theorem for modules, we may find elements $a_1, \ldots, a_h$ in A which generate A at $\mathfrak{q}$ for all $\mathfrak{q} \in M$. Thus $a_1, \ldots, a_h$ is M-generic.

We will now show that for every $i \leq h$ there is an M-generic sequence $b_1, \ldots, b_h$ such that for every maximal ideal $\mathfrak{q}$ the elements $b_1, \ldots, b_i$ can be completed to a set of k elements which generate A at $\mathfrak{q}$. Our argument is by induction on i. It is clearly true for $i = 0$ (any M-generic sequence of length h works). Suppose that $b_1, \ldots, b_h$ is a generic sequence which works for some i. We seek a generic sequence working for $i + 1$ which is of the form $b_1, \ldots, b_i, b, b_{i+2}, \ldots, b_h$ for some $b \in A$. Note that if b is such that $b - b_{i+1} \in \mathfrak{q}A$ for all $\mathfrak{q} \in M$ then $b_1, \ldots, b_i, b, b_{i+2}, \ldots, b_h$ is M-generic. Also, there is a finite set W of maximal ideals, disjoint from M, such that for any maximal ideal $\mathfrak{q} \notin W$ and any $b \in A$, the sequence $b_1, \ldots, b_i, b, b_{i+1}, \ldots, b_h$ generates A at $\mathfrak{q}$. Since $k > h$, for any $\mathfrak{q} \notin W$ and any $b \in A$, the elements $b_1, \ldots, b_i, b$ can be completed to a set of k elements which generate A at $\mathfrak{q}$. So in our choice of b we only need to worry about maximal ideals in W. For every $\mathfrak{q} \in W$ there is $b_{\mathfrak{q}} \in A$ such that $b_1, \ldots, b_i, b_{\mathfrak{q}}$ extends to a set of k elements which generate A at $\mathfrak{q}$. By the Chinese remainder theorem for modules, we may choose $b \in A$ such that $b - b_{i+1} \in \mathfrak{q}A$ for all $\mathfrak{q} \in M$ and $b - b_{\mathfrak{q}} \in \mathfrak{q}A$ for all $\mathfrak{q} \in W$. For any such b the sequence $b_1, \ldots, b_i, b, b_{i+2}, \ldots, b_h$ has the required properties for $i + 1$.

Let $a_1, \ldots, a_h$ be an M-generic sequence good for $i = h$. Thus, for any maximal ideal $\mathfrak{q}$ outside some finite set U the elements $a_1, \ldots, a_h$ generate A at $\mathfrak{q}$. For each $\mathfrak{q} \in U$, there are elements $a_{h+1}(\mathfrak{q}), \ldots, a_k(\mathfrak{q})$ in A such that $a_1, \ldots, a_h, a_{h+1}(\mathfrak{q}), \ldots, a_k(\mathfrak{q})$ generate A at $\mathfrak{q}$. By the Chinese remainder theorem for modules, there are elements $a_{h+1}, \ldots, a_k$ in A such that $a_i - a_i(\mathfrak{q}) \in \mathfrak{q}A$ for all $\mathfrak{q} \in U$ and all $i = h + 1, \ldots, k$. Thus the elements $a_1, \ldots, a_k$ generate A at $\mathfrak{q}$ for every maximal ideal $\mathfrak{q}$, hence they generate A as an R-algebra by Lemma 2.6. □

The reader familiar with the results of Forster and Swan on the number of generators of modules over Noetherian commutative rings should recognize the

similarities between Theorem 5.7 and Swan's theorem [Matsumura 1986, Theorem 5.8]. Unlike the result of Swan, Theorem 5.7 only treats the case of rings of dimension ≤ 1. So far we have not been able to get similar results for rings of higher dimension but we believe that the following conjectural generalization should be true. In order to state it we need to recall briefly some notions (see [Matsumura 1986, p. 35–37] for more details). We denote by j-Spec R the subspace of Spec R which consists of those prime ideals which are intersections of some set of maximal ideals of R. We assume that m-Spec R is a Noetherian space. It turns out that this is equivalent to j-Spec R being Noetherian, and then both spaces have the same combinatorial dimension. When $\mathfrak{p} \in$ j-Spec R, we write j-dim $\mathfrak{p}$ for the combinatorial dimension of the closure of $\{\mathfrak{p}\}$ in j-Spec R. For $\mathfrak{p} \in$ j-Spec R define

$$b(\mathfrak{p}, A) = \begin{cases} 0 & \text{if } A_{\mathfrak{p}} = 0, \\ \text{j-dim}\, \mathfrak{p} + r_{\mathfrak{p}}(A) & \text{if } A_{\mathfrak{p}} \neq 0. \end{cases}$$

Conjecture 5.8. *Suppose that R is a commutative ring such that* m-Spec R *is a Noetherian space. Let A be an R-algebra finitely generated as an R-module. If* $\sup\{b(\mathfrak{p}, A) : \mathfrak{p} \in \text{m-Spec } R\} = n < \infty$ *then A can be generated as an R-algebra by n elements.*

6. Generators of matrix algebras over finite fields

It is clear from the results of Section 3 that the key step towards understanding the smallest number of generators of an algebra over a commutative ring is to handle the case of algebras over fields. Among the finite-dimensional algebras over fields the best understood class is the class of separable algebras. It was proved in [Mazur and Petrenko 2009] that any separable algebra over an infinite field is two-generated. This is no longer true over finite fields. In this case, separable algebras coincide with finite products of matrix algebras.

By Proposition 2.12, understanding the structure of generators of a semisimple F-algebra reduces to algebras of the form A^m, where A is a simple F-algebra. We have the following result:

Theorem 6.1. *Let F be a field, A a finite-dimensional simple F-algebra, and k, m, n positive integers. Then k elements of A^m, say $a_1 = (a_{11}, \ldots, a_{1m})$, $\ldots$, $a_k = (a_{k1}, \ldots, a_{km})$, generate A^m as an F-algebra if and only if the following two conditions are satisfied*:

(1) *For any $i = 1, \ldots, m$, the elements $a_{1i}, \ldots, a_{ki}$ generate A as an F-algebra.*

(2) *There does not exist a pair of different indices i, j for which there is an automorphism Ψ of the F-algebra A such that*

$$a_{1i} = \Psi(a_{1j}), \ldots, a_{ki} = \Psi(a_{kj}).$$

Proof. Let B denote the subalgebra of A^m generated by $a_1, \ldots, a_k$. Recall that there is a unique (up to isomorphism) simple A-module M and it is faithful. Let M_i be the pull-back of M via the projection $\pi_i : B \to A$ on the i-th coordinate. Thus M_i is a B-module which coincides with M as an F-vector space, and for $b \in B$ and $m \in M_i = M$ we have $bm = \pi_i(b)m$. Since π_i is surjective by (1), each M_i is a simple B module. We claim that these B-modules are pairwise nonisomorphic. Indeed, suppose that for some $i \neq j$ the B-modules M_i and M_j are isomorphic and let $\Phi : M_i \to M_j$ be an isomorphism of these B-modules. For any $a \in A$ there is $b \in B$ such that $\pi_i(b) = a$. Set $\Psi(a) = \pi_j(b)$. We claim that Ψ is well-defined and an automorphism of the F-algebra A. Indeed, if $b_1 \in B$ is another element such that $\pi_i(b_1) = a$ then for any $m \in M_i$ we have $bm = b_1 m$. Applying Φ to this equality, we see that $b\Phi(m) = b_1\Phi(m)$ for any $m \in M_i$. Since Φ is an isomorphism, we conclude that $bn = b_1 n$ for any $n \in M_j$, that is, $\pi_j(b)m = \pi_j(b_1)m$ for every $m \in M$. Since M is a faithful A-module, we conclude that $\pi_j(b) = \pi_j(b_1)$. This shows that Ψ is well-defined. It is now straightforward to see that Ψ respects addition and multiplication and that it is F-linear. It follows that Ψ is an isomorphism of F-algebras. This however is in contradiction with our assumption (2). It follows that M_i and M_j are not isomorphic as B-modules for $i \neq j$. Note that $\bigoplus_{i=1}^m M_i$ is a semisimple, faithful B-module. It follows that B is semisimple and every simple B-module is isomorphic to one of the M_i's. By Wedderburn–Artin theory, B is isomorphic to the product $\prod_{i=1}^m B_i$, where $B_i = \mathrm{M}_{n_i}(D_i)$, $D_i = \mathrm{End}_B(M_i)$, and $n_i \dim_F(D_i) = \dim_F(M_i) = \dim_F M$. Note that $D_i = \mathrm{End}_B(M_i) = \mathrm{End}_A(M)$ and therefore A is isomorphic to B_i for each i, again by Wedderburn–Artin theory. This proves that $\dim_F A^m = \dim_F B$, and consequently $A^m = B$. □

As a simple corollary we get the following.

Proposition 6.2. *Let A be a simple finite-dimensional algebra over a field F. For any $k > 0$ the group $\mathrm{Aut}_F(A)$ of F-algebra automorphisms of A acts freely on the set $\mathrm{Gen}_k(A, F)$. The algebra A^m can be generated by k elements as an F-algebra if and only if there are at least m different orbits of the action of $\mathrm{Aut}_F(A)$ on $\mathrm{Gen}_k(A, F)$.*

Proof. The action of $\mathrm{Aut}_F(A)$ on $\mathrm{Gen}_k(A, F)$ is the restriction of the coordinate-wise action of $\mathrm{Aut}_F(A)$ on A^k. If $\Psi \in \mathrm{Aut}_F(A)$ fixes an element of $\mathrm{Gen}_k(A, F)$, then it fixes each member of a set of generators of A as an F-algebra, so Ψ is the identity. This explains why the action is free. Theorem 6.1 says that elements $a_1 = (a_{11}, \ldots, a_{1m}), \ldots, a_k = (a_{k1}, \ldots, a_{km})$ generate A^m as an F-algebra if and only if the elements $(a_{11}, \ldots, a_{k1}), \ldots, (a_{1m}, \ldots, a_{km})$ belong to different orbits of the action of $\mathrm{Aut}_F(A)$ on $\mathrm{Gen}_k(A, F)$. □

Suppose now that $F = \mathbb{F}_q$ is a finite field with q elements. Then simple finite-dimensional $\mathbb{F}_q$-algebras are exactly algebras of the form $\mathrm{M}_n(\mathbb{F}_{q^s})$ for some positive

integers n, s. Now, by the Skolem–Noether theorem, the group of automorphisms of the $\mathbb{F}_q$-algebra $\mathrm{M}_n(\mathbb{F}_{q^s})$ is the semidirect product of the group $\mathrm{PGL}_n(\mathbb{F}_{q^s})$ and the Galois group $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$. Thus we get the following.

Theorem 6.3. *Let $A = \mathrm{M}_n(\mathbb{F}_{q^s})$. Then A^m can be generated by k elements as an $\mathbb{F}_q$-algebra if and only if*

$$m \le \frac{|\mathrm{Gen}_k(A, \mathbb{F}_q)|}{s|\mathrm{PGL}_n(\mathbb{F}_{q^s})|}.$$

Furthermore, $|\mathrm{Gen}_k(A^m, \mathbb{F}_q)| = \prod_{i=0}^{m-1} \big(|\mathrm{Gen}_k(A, \mathbb{F}_q)| - i \cdot s \cdot |\mathrm{PGL}_n(\mathbb{F}_{q^s})|\big)$.

Proof. As we noted above, $\mathrm{Aut}_{\mathbb{F}_q}(A)$ has $s|\mathrm{PGL}_n(\mathbb{F}_{q^s})|$ elements. Since $\mathrm{Aut}_{\mathbb{F}_q}(A)$ acts freely on $\mathrm{Gen}_k(A, \mathbb{F}_q)$, the number of orbits of this action is equal to

$$\frac{|\mathrm{Gen}_k(A, \mathbb{F}_q)|}{s|\mathrm{PGL}_n(\mathbb{F}_{q^s})|}.$$

The first part of the theorem is now an immediate consequence of Proposition 6.2.

To prove the second part note that according to Proposition 6.2 the elements of $\mathrm{Gen}_k(A^m, \mathbb{F}_q)$ are in bijective correspondence with sequences of length m of elements from $\mathrm{Gen}_k(A, \mathbb{F}_q)$, with no two elements in the same orbit of $\mathrm{Aut}_{\mathbb{F}_q}(A)$. In order to count these sequences, let o be the number of orbits of the action of $\mathrm{Aut}_{\mathbb{F}_q}(A)$ on $\mathrm{Gen}_k(A, \mathbb{F}_q)$ and let t be the size of each orbit. We can choose a sequence of m different orbits $O_1, \dots, O_m$ in $m!\binom{o}{m}$ ways and the number of sequences $g_1, \dots, g_m$ such that $g_i \in O_i$ for $i = 1, \dots, m$ is t^m. Thus

$$|\mathrm{Gen}_k(A^m, \mathbb{F}_q)| = m!\binom{o}{m} t^m = \prod_{i=0}^{m-1} (ot - it).$$

The second part of the theorem follows now immediately from the equalities $ot = |\mathrm{Gen}_k(A, \mathbb{F}_q)|$ and $t = s|\mathrm{PGL}_n(\mathbb{F}_{q^s})|$. □

For a simple separable algebra A over any field F the sets $\mathrm{Gen}_k(A, F)$ are nonempty for any $k \ge 2$. In other words, we have the following.

Theorem 6.4. *Let A be a simple separable algebra over a field F. Then A can be generated by two elements as an F-algebra.*

Proof. For infinite fields F the result has been proved in [Mazur and Petrenko 2009]. When $F = \mathbb{F}_q$ is a finite field with q elements then A is isomorphic to $\mathrm{M}_n(\mathbb{F}_{q^s})$ for some positive integers n and s. Let u be a generator of the multiplicative group of $\mathbb{F}_{q^s}$, so in particular $\mathbb{F}_{q^s} = \mathbb{F}_q[u]$. For $1 \le i, j \le n$ let E_{ij} denote the matrix whose (i, j) entry is 1 and all other entries are 0. Let $A = uE_{11}$ and $B = E_{1n} + \sum_{i=1}^{n-1} E_{i+1,i}$. Then $u^k E_{ij} = B^{i-1} A^k B^{n+1-j}$ for all $1 \le i, j \le n$ and all $k \ge 0$. It follows that A and B generate the $\mathbb{F}_q$-algebra $\mathrm{M}_n(\mathbb{F}_{q^s})$. □

7. The numbers $|\mathrm{Gen}_k(\mathrm{M}_n(\mathbb{F}_q), \mathbb{F}_q)|$

In this section we will study the numbers $|\mathrm{Gen}_k(\mathrm{M}_n(\mathbb{F}_q), \mathbb{F}_q)|$. In particular, we will compute them when $n \leq 3$. To simplify the notation, we make the following definition.

Definition 7.1. Let m and n be positive integers and let q be a prime power. We introduce the following notation:

(i) $\mathrm{G}_{m,n}(\mathbb{F}_q) = \mathrm{Gen}_m(\mathrm{M}_n(\mathbb{F}_q), \mathbb{F}_q)$.

(ii) $\mathrm{g}_{m,n}(q) = |\mathrm{G}_{m,n}(\mathbb{F}_q)|$.

(iii) $\mathrm{gen}_{m,n}(q) = \dfrac{\mathrm{g}_{m,n}(q)}{|\mathrm{PGL}_n(\mathbb{F}_q)|}$.

Note that by Theorem 6.3, the number $\mathrm{gen}_{m,n}(q)$ is equal to the largest $k \in \mathbb{Z}$ such that $r(\mathrm{M}_n(\mathbb{F}_q)^k, \mathbb{F}_q) \leq m$. Thus our notation agrees with that introduced in Definition 1.3.

When $n = 1$, an m-tuple generates $\mathbb{F}_q$ if and only if it contains a nonzero element. It follows that $\mathrm{g}_{m,1}(q) = q^m - 1$. From now on in this section we assume that $n \geq 2$, unless stated otherwise.

Our attempt at computing the numbers $\mathrm{g}_{m,n}(q)$ is based on the following simple observation: a set of matrices does not generate the whole algebra $\mathrm{M}_n(\mathbb{F}_q)$ if and only if there is a maximal subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ that contains this set. Thus the following is true:

$$\mathrm{G}_{m,n}(\mathbb{F}_q) = \mathrm{M}_n(\mathbb{F}_q)^m - \bigcup \{\mathscr{A}^m : \mathscr{A} \text{ is a maximal subalgebra of } \mathrm{M}_n(\mathbb{F}_q)\}. \quad (4)$$

Let $\mathscr{D}$ be the subalgebra of scalar matrices of $\mathrm{M}_n(\mathbb{F}_q)$. Since any subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ contains $\mathscr{D}$, we can subtract $\mathscr{D}^m$ in the above formula and get that $G_{m,n}(\mathbb{F}_q)$ is equal to

$$\mathrm{M}_n(\mathbb{F}_q)^m - \mathscr{D}^m - \bigcup \{\mathscr{A}^m - \mathscr{D}^m : \mathscr{A} \text{ is a maximal subalgebra of } \mathrm{M}_n(\mathbb{F}_q)\}.$$

Since $|\mathrm{M}_n(\mathbb{F}_q)| = q^{n^2}$ and $|\mathscr{D}| = q$, the inclusion-exclusion formula yields

$$\mathrm{g}_{m,n}(q) = q^{mn^2} - q^m + \sum (-1)^k |(\mathscr{A}_{i_1}^m - \mathscr{D}^m) \cap \cdots \cap (\mathscr{A}_{i_k}^m - \mathscr{D}^m)|,$$

where the sum is taken over all nonempty subsets $\{\mathscr{A}_{i_1}, \ldots, \mathscr{A}_{i_k}\}$ of the set of all maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$. Since $\mathscr{D}$ is contained in every subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$, we have

$$(\mathscr{A}_{i_1}^m - \mathscr{D}^m) \cap \cdots \cap (\mathscr{A}_{i_k}^m - \mathscr{D}^m) = \mathscr{A}_{i_1}^m \cap \cdots \cap \mathscr{A}_{i_k}^m - \mathscr{D}^m = (\mathscr{A}_{i_1} \cap \cdots \cap \mathscr{A}_{i_k})^m - \mathscr{D}^m,$$

and therefore

$$\mathrm{g}_{m,n}(q) = q^{mn^2} - q^m + \sum (-1)^k \big(|\mathscr{A}_{i_1} \cap \cdots \cap \mathscr{A}_{i_k}|^m - q^m\big), \quad (5)$$

where the sum is taken over all nonempty subsets $\{\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_k}\}$ of the set of all maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$.

In order to evaluate the right-hand side of (5), it is necessary to have a description of all maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$. It is quite easy to produce one type of maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$. In fact, we have the following result.

Lemma 7.2. *For a proper nontrivial vector subspace U of $\mathbb{F}_q^n$ let $\mathcal{A}_U$ be the set of all matrices from $\mathrm{M}_n(\mathbb{F}_q)$ that leave U invariant. Then $\mathcal{A}_U$ is a maximal subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$. Moreover, each $\mathcal{A}_U$ is uniquely determined by U, that is, if $\mathcal{A}_U = \mathcal{A}_{U'}$ then $U = U'$.*

Proof. First note that the center of $\mathcal{A}_U$ consists of scalar matrices. In fact, if a matrix A is in the center of $\mathcal{A}_U$ then it acts as a scalar λ on U. The matrix $B = A - \lambda I$ annihilates U and is in the center of $\mathcal{A}_U$. Suppose that $Bv \neq 0$ for some v. Then there is a projection Π onto U such that $\Pi(Bv) \neq 0$. Since $\Pi \in \mathcal{A}_U$, we have $0 \neq \Pi Bv = B\Pi v = 0$, a contradiction. Thus $B = 0$ and A is a scalar matrix.

Now note that if $U \neq U'$ then there is $A \in \mathcal{A}_U - \mathcal{A}_{U'}$. In fact, if $U' \subsetneq U$ then such an A clearly exists since $\mathcal{A}_U$ is transitive on U. If there exists $v \in U' - U$ then for any w there is an $A \in \mathcal{A}_U$ such that $Av = w$. Taking $w \notin U'$ yields the required A. This, in particular, proves the second assertion.

Take any matrix A not in $\mathcal{A}_U$ and let $\mathcal{A}'$ be the algebra generated by A and $\mathcal{A}_U$. Note that $\mathcal{A}'$ cannot fix any nontrivial subspace V of $\mathbb{F}_q^n$. In fact, if $V \neq U$ then, as we have seen above, $\mathcal{A}_U$ is not contained in $\mathcal{A}_V$ and A does not take U into U. Thus $\mathbb{F}_q^n$ is a simple and faithful $\mathcal{A}'$-module. It follows that $\mathcal{A}'$ is a simple central $\mathbb{F}_q$-algebra with a simple module of dimension n over $\mathbb{F}_q$, hence it must be isomorphic to $\mathrm{M}_n(\mathbb{F}_q)$. It follows that $\mathcal{A}_U$ is maximal. □

The following lemma describes a second type of maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$.

Lemma 7.3. *Let s be a prime divisor of n and let $m = n/s$. Any $\mathbb{F}_q$-subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$ is maximal. Any two such subalgebras are conjugate in $\mathrm{M}_n(\mathbb{F}_q)$ and their number is equal to*

$$s^{-1} \prod_{s \nmid i, 1 \leq i < n} (q^n - q^i).$$

Proof. Let $\mathcal{A}$ be a $\mathbb{F}_q$-subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$. Thus $\mathbb{F}_q^n$ is an $\mathcal{A}$-module of dimension m over the center of $\mathcal{A}$ (which is isomorphic to $\mathbb{F}_{q^s}$). It follows that $\mathbb{F}_q^n$ is a simple $\mathcal{A}$-module. Suppose that $\mathcal{A}'$ is a $\mathbb{F}_q$-subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ containing $\mathcal{A}$. Then $\mathbb{F}_q^n$ is a simple and faithful $\mathcal{A}'$-module. It follows that $\mathcal{A}'$ is simple, hence it is isomorphic to $\mathrm{M}_k(\mathbb{F}_{q^r})$, where $kr = n$ and r is the dimension of the center of $\mathcal{A}'$ over $\mathbb{F}_q$. Clearly, the center of $\mathcal{A}'$ is contained in the center of $\mathcal{A}$. It follows that $r \mid s$, and therefore $r = 1$ or $r = s$ (recall that s is

a prime). In the former case we get $\mathscr{A}' = \mathrm{M}_n(\mathbb{F}_q)$ and in the latter case we have $\mathscr{A}' = \mathscr{A}$. This shows that $\mathscr{A}$ is maximal.

For the existence of an $\mathbb{F}_q$-subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$ consider the (unique up to isomorphism) simple $\mathrm{M}_m(\mathbb{F}_{q^s})$-module V. It has dimension m as a vector space over $\mathbb{F}_{q^s}$, so as a $\mathbb{F}_q$-vector space it is isomorphic to $\mathbb{F}_q^n$. Thus the action of $\mathrm{M}_m(\mathbb{F}_{q^s})$ on V induces an $\mathbb{F}_q$-algebra embedding of $\mathrm{M}_m(\mathbb{F}_{q^s})$ into $\mathrm{M}_n(\mathbb{F}_q)$.

Fix now a $\mathbb{F}_q$-subalgebra $\mathscr{A}$ of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$. By the Noether–Skolem theorem, any $\mathbb{F}_q$-algebra homomorphism of $\mathscr{A}$ into $\mathrm{M}_n(\mathbb{F}_q)$ is given by conjugation with some invertible element of $\mathrm{M}_n(\mathbb{F}_q)$. This means that the group $\mathrm{GL}_n(\mathbb{F}_q)$ acts transitively on the set of subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$ which are isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$. Since $\mathscr{A}$ is maximal, the subgroup C of elements which act trivially on $\mathscr{A}$ coincides with the multiplicative group of the center of $\mathscr{A}$. The quotient of the stabilizer of $\mathscr{A}$ by C is, again by the Noether–Skolem theorem, isomorphic to the group of all automorphisms of the $\mathbb{F}_q$-subalgebra $\mathscr{A}$. We have seen earlier that the group of $\mathbb{F}_q$-algebra automorphisms of $\mathrm{M}_m(\mathbb{F}_{q^s})$ has $s|\mathrm{PGL}_m(\mathbb{F}_{q^s})|$ elements (see the discussion directly before Theorem 6.3). Therefore the stabilizer of $\mathscr{A}$ has $|C| \cdot s \cdot |\mathrm{PGL}_m(\mathbb{F}_{q^s})| = s|\mathrm{GL}_m(\mathbb{F}_{q^s})|$ elements. Consequently, the number of $\mathbb{F}_q$-subalgebras $\mathscr{A}$ of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$ is equal to

$$\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{s|\mathrm{GL}_m(\mathbb{F}_{q^s})|} = s^{-1} \prod_{s \nmid i, 1 \le i < n} (q^n - q^i). \qquad \square$$

It turns out that the maximal subalgebras described in Lemmas 7.2 and 7.3 exhaust all possible maximal subalgebras. In other words, we have the following result.

Proposition 7.4. *Let $\mathscr{A}$ be a maximal $\mathbb{F}_q$-subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$. Then either $\mathscr{A} = \mathscr{A}_U$ for some subspace U of $\mathbb{F}_q^n$ or $\mathscr{A}$ is isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$ for some prime divisor s of $n = ms$.*

Proof. Suppose that $\mathscr{A}$ fixes some proper nontrivial subspace U of $\mathbb{F}_q^n$. Then $\mathscr{A}$ is contained in $\mathscr{A}_U$, hence $\mathscr{A} = \mathscr{A}_U$. If no proper nontrivial subspace of $\mathbb{F}_q^n$ is fixed by $\mathscr{A}$ then $\mathbb{F}_q^n$ is a simple and faithful $\mathscr{A}$-module. It follows that $\mathscr{A}$ is simple and therefore it is isomorphic to $\mathrm{M}_k(\mathbb{F}_{q^r})$, where $kr = n$. Let s be a prime divisor of r. The center of $\mathscr{A}$ contains a subfield F isomorphic to $\mathbb{F}_{q^s}$. The centralizer of F in $\mathrm{M}_n(\mathbb{F}_q)$ consists exactly of those linear transformations of $\mathbb{F}_q^n$ which are F-linear. Thus it is a subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_m(\mathbb{F}_{q^s})$, where $ms = n$. On the other hand, this subalgebra contains $\mathscr{A}$, hence it must be equal to $\mathscr{A}$. $\square$

In order to carry out our strategy to compute the numbers $\mathrm{g}_{m,n}(q)$ we need to understand the intersections of maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$. This appears to be a very challenging combinatorial problem and so far we have only succeeded in completing the computations for $n \le 3$. One of the complications in the general

case is that the maximal subalgebras are of two different types. This difficulty disappears when n is a prime by the following observation.

Lemma 7.5. *Let n be a prime number. If $\mathscr{A}$ is a maximal subalgebra of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathbb{F}_{q^n}$, then its intersection with any other maximal subalgebra is equal to $\mathscr{D}$, the algebra of scalar matrices.*

Proof. Since n is prime, $\mathbb{F}_{q^n}$ has only two subfields, itself and $\mathbb{F}_q$. In other words, $\mathscr{A}$ has only two subalgebras, $\mathscr{A}$ and $\mathscr{D}$. Since the intersection cannot be equal to $\mathscr{A}$, it is equal to $\mathscr{D}$. □

For the rest of this section we assume that n is a prime number. Thus Lemma 7.5 tells us that if the set $\{\mathscr{A}_{i_1}, \ldots, \mathscr{A}_{i_k}\}$ of maximal subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$ includes a subalgebra isomorphic to $\mathbb{F}_{q^n}$, and $k \geq 2$, then the intersection of the subalgebras in this set is equal to $\mathscr{D}$, and so the corresponding term in (5), $|\mathscr{A}_{i_1} \cap \cdots \cap \mathscr{A}_{i_k}|^m - q^m$, is equal to 0. It follows that we can rewrite (5) in the following way:

$$\mathrm{g}_{m,n}(q) = q^{mn^2} - q^m - \sum_{\mathscr{A} \cong \mathbb{F}_{q^n}} (|\mathscr{A}|^m - q^m) + \sum (-1)^k (|\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k}|^m - q^m),$$

where the second sum is over all nonempty sets $\{U_1, \ldots, U_k\}$ of nontrivial proper subspaces of $\mathbb{F}_q^n$. By Lemma 7.3, the first sum consists of $n^{-1} \prod_{i=1}^{n-1} (q^n - q^i)$ terms, each term being $q^{mn} - q^m$. Thus we get the following formula:

$$\mathrm{g}_{m,n}(q) = q^{mn^2} - q^m - n^{-1}(q^{mn} - q^m) \prod_{i=1}^{n-1} (q^n - q^i) + \sum (-1)^k (|\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k}|^m - q^m), \quad (6)$$

where the sum is over all nonempty sets $\{U_1, \ldots, U_k\}$ of nontrivial proper subspaces of $\mathbb{F}_q^n$.

Let $\mathscr{F}$ be the set of all subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$ which are intersections of some of the maximal algebras of the form $\mathscr{A}_U$. For each $\mathscr{A} \in \mathscr{F}$, define the degree $\mathrm{d}(\mathscr{A})$ of $\mathscr{A}$ by

$$\mathrm{d}(\mathscr{A}) = \sum (-1)^k, \quad (7)$$

where the sum is over all sets $\{U_1, \ldots, U_k\}$ of nontrivial proper subspaces of $\mathbb{F}_q^n$ such that $\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k} = \mathscr{A}$. Thus (6) can be stated as

$$\mathrm{g}_{m,n}(q) = q^{mn^2} - q^m - n^{-1}(q^{mn} - q^m) \prod_{i=1}^{n-1} (q^n - q^i) + \sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m). \quad (8)$$

The following simple lemma will be useful for our analysis of elements of $\mathscr{F}$.

Lemma 7.6. *Let F be a field, V be a vector space over F, and let $v_1, \ldots, v_k \in V$ be a minimal linearly dependent collection of vectors (so any $k-1$ of them are*

linearly independent). *Then any linear endomorphism of V that scales $v_1, \dots, v_k$ is a scalar operator when restricted to the linear span of $v_1, \dots, v_k$.*

Proof. Let f be a linear endomorphism of V such that $f(v_i) = \alpha_i v_i$ for some $\alpha_i \in F$ and $i = 1, \dots, k$. The assumptions of the lemma imply that

$$v_k = \beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1}$$

for some nonzero $\beta_1, \dots, \beta_{k-1} \in F$. By expressing $f(v_k)$ in two ways, as $\beta_1\alpha_1 v_1 + \cdots + \beta_{k-1}\alpha_{k-1} v_{k-1}$ and as $\alpha_k v_k$, we obtain $\beta_i\alpha_i = \beta_i\alpha_k$ for all i. Since none of the β_i's is 0, we have $\alpha_i = \alpha_k$ for $i = 1, \dots, k$. □

7A. ***The case n = 2.*** In this subsection we evaluate (8) in the case $n = 2$. Any element $\mathscr{A} \in \mathscr{F}$ is of the form $\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k}$, where $k \geq 1$ and $U_1, \dots, U_k$ are distinct lines in $\mathbb{F}_q^2$. Note that by Lemma 7.6, $\mathscr{A} = \mathscr{D}$ if $k \geq 3$ and in this case $\mathscr{A}$ does not contribute anything to (8). It follows that if $\mathscr{A}$ is an element of $\mathscr{F}$ different from $\mathscr{D}$, then it can be expressed as the intersection of maximal subalgebras in a unique way and it is either of the form $\mathscr{A}_U$ or of the form $\mathscr{A}_{U_1} \cap \mathscr{A}_{U_2}$. In the former case, we have $|\mathscr{A}| = q^3$ and $\mathrm{d}(\mathscr{A}) = -1$. In the latter case, $|\mathscr{A}| = q^2$ and $\mathrm{d}(\mathscr{A}) = 1$. Since the number of lines in $\mathbb{F}_q^2$ is $q + 1$, (8) takes the following form:

$$\mathrm{g}_{m,2}(q) = q^{4m} - q^m - 2^{-1}(q^{2m} - q^m)(q^2 - q) \\ -(q+1)(q^{3m} - q^m) + 2^{-1}(q+1)q(q^{2m} - q^m),$$

which simplifies to

$$\mathrm{g}_{m,2}(q) = q^{2m+1}(q^{m-1} - 1)(q^m - 1). \tag{9}$$

7B. ***The case n = 3.*** In this subsection we evaluate (8) for $n = 3$. This is substantially more difficult than the case $n = 2$, but we are still able to analyze all elements of $\mathscr{F}$. The following combinatorial lemma will help us evaluate the degree of some of the algebras in $\mathscr{F}$.

Lemma 7.7. *Let X be a finite set. Consider a family $\mathcal{S}$ of subsets of X such that if $Y \in \mathcal{S}$ and $Y \subseteq Y' \subseteq X$, then Y' also belongs to $\mathcal{S}$. Suppose furthermore that one of the following two conditions is true.*

(1) *There is $x \in X$ such that $X' - \{x\} \in \mathcal{S}$ for any $X' \in \mathcal{S}$.*

(2) *There are $x, y \in X$ such that if $X' \in \mathcal{S}$ and $X' - \{x\} \notin \mathcal{S}$ then*
   (a) *$X' - \{y\} \in \mathcal{S}$ and*
   (b) *$(X' \cup \{y\}) - \{x\} \notin \mathcal{S}$.*

Then $\sum_{Y \in \mathcal{S}} (-1)^{|Y|} = 0.$

Proof. Let $\mathcal{S}_0$ be the family of those subsets from $\mathcal{S}$ that do not contain x and let $\mathcal{S}_1$ be the family of those subsets that contain x. The map $t : Y \mapsto Y \cup \{x\}$ is an injection from $\mathcal{S}_0$ to $\mathcal{S}_1$. Let $\mathcal{S}_2 = \mathcal{S}_1 - t(\mathcal{S}_0)$. We have

$$\sum_{Y\in\mathcal{S}}(-1)^{|Y|} = \sum_{Y\in\mathcal{S}_0}(-1)^{|Y|} + \sum_{Y\in t(\mathcal{S}_0)}(-1)^{|Y|} + \sum_{Y\in\mathcal{S}_2}(-1)^{|Y|}.$$

Since $|t(Y)| = 1 + |Y|$, the first two sums on the right annihilate each other, and so

$$\sum_{Y\in\mathcal{S}}(-1)^{|Y|} = \sum_{Y\in\mathcal{S}_2}(-1)^{|Y|}.$$

Condition (1) exactly means that $\mathcal{S}_2$ is empty, hence $\sum_{Y\in\mathcal{S}}(-1)^{|Y|} = 0$. If condition (2) holds, we write $\mathcal{S}_2$ as a disjoint union $\mathcal{S}_2 = \mathcal{S}_{20} \cup \mathcal{S}_{21}$, where $\mathcal{S}_{20}$ consists of those elements of $\mathcal{S}_2$ which do not contain y. By (b), the map $s : Y \mapsto Y \cup \{y\}$ maps $\mathcal{S}_{20}$ into $\mathcal{S}_{21}$ and (a) implies that s is onto. Thus $s : \mathcal{S}_{20} \to \mathcal{S}_{21}$ is a bijection and

$$\sum_{Y\in\mathcal{S}_2}(-1)^{|Y|} = \sum_{Y\in\mathcal{S}_{20}}(-1)^{|Y|} + \sum_{Y\in\mathcal{S}_{21}}(-1)^{|Y|} = \sum_{Y\in\mathcal{S}_{20}}\left((-1)^{|Y|} + (-1)^{|s(Y)|}\right) = 0. \square$$

We apply Lemma 7.7 as follows. Given $\mathscr{A} \in \mathcal{F}$, the set $X = X_{\mathscr{A}}$ will consists of all proper nontrivial subspaces of $\mathbb{F}_q^3$ fixed by $\mathscr{A}$ and the family $\mathcal{S} = \mathcal{S}_{\mathscr{A}}$ will consist of all subsets $\{U_1, \ldots, U_k\}$ of X such that $\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k} = \mathscr{A}$. If conditions (1) or (2) hold for $\mathcal{S}_{\mathscr{A}}$, then Lemma 7.7 tells us that $\mathrm{d}(\mathscr{A}) = 0$.

Before we start the analysis of elements in $\mathcal{F}$ let us recall that the dot product $v \cdot w = v_1w_1 + v_2w_2 + v_2w_3$ is a nondegenerate symmetric bilinear form on $\mathbb{F}_q^3$. The adjoint operator with respect to this bilinear form is the transposition. It follows that if $\mathscr{A}_{U_1} \cap \cdots \cap \mathscr{A}_{U_k} = \mathscr{A} \in \mathcal{F}$ then

$$\mathscr{A}_{U_1^\perp} \cap \cdots \cap \mathscr{A}_{U_k^\perp} = \mathscr{A}^t := \{A^t : A \in \mathscr{A}\} \in \mathcal{F},$$

where A^t is the transpose of A and $U^\perp$ is the subspace orthogonal to U with respect to the dot product. We will often call $\mathscr{A}^t$ the dual of $\mathscr{A}$. It is clear that $\mathscr{A}$ and $\mathscr{A}^t$ have the same number of elements and the same degree.

Definition 7.8. Let $\mathscr{A} \in \mathcal{F}$. Then

$$\mathrm{L}_{\mathscr{A}} = \{U : \dim U = 1 \text{ and } \mathscr{A} \subseteq \mathscr{A}_U\}$$

is the set of all lines fixed by $\mathscr{A}$ and

$$\mathrm{P}_{\mathscr{A}} = \{U : \dim U = 2 \text{ and } \mathscr{A} \subseteq \mathscr{A}_U\}$$

is the set of all planes fixed by $\mathscr{A}$.

Note that $\mathrm{L}_{\mathscr{A}^t} = \{\pi^\perp : \pi \in \mathrm{P}_{\mathscr{A}}\}$ and $\mathrm{P}_{\mathscr{A}^t} = \{l^\perp : l \in \mathrm{L}_{\mathscr{A}}\}$. Also, $X_{\mathscr{A}} = \mathrm{L}_{\mathscr{A}} \cup \mathrm{P}_{\mathscr{A}}$.

Consider an algebra $\mathscr{A} \in \mathscr{F}$, $\mathscr{A} \neq \mathscr{D}$. Then $\mathscr{A}$ falls into exactly one of the following cases.

Case I: $\mathrm{L}_{\mathscr{A}}$ *contains three lines in general position.* Recall that we say that three lines in $\mathbb{F}_q^3$ are in general position if they are not contained in any plane. Dually, three planes are in general position if they do not share any common line. Let $l_1, l_2, l_3 \in \mathrm{L}_{\mathscr{A}}$ be three lines in general position. Let π_i be the plane spanned by l_j and l_k, where $\{i, j, k\} = \{1, 2, 3\}$.

Subcase Ia: $\mathrm{L}_{\mathscr{A}} = \{l_1, l_2, l_3\}$. In this case $\mathrm{P}_{\mathscr{A}} = \{\pi_1, \pi_2, \pi_3\}$. The algebra $\mathscr{A}$ is conjugate to the algebra of all diagonal matrices. In particular, $|\mathscr{A}| = q^3$. Furthermore, $X_{\mathscr{A}} = \mathrm{L}_{\mathscr{A}} \cup \mathrm{P}_{\mathscr{A}}$ and a subset of $X_{\mathscr{A}}$ belongs to $\mathscr{S}_{\mathscr{A}}$ if and only if it contains one of the following sets: $\{l_1, l_2, l_3\}$, $\{\pi_1, \pi_2, \pi_3\}$, $\{l_1, l_2, \pi_1, \pi_2\}$, $\{l_1, l_3, \pi_1, \pi_3\}$, or $\{l_2, l_3, \pi_2, \pi_3\}$. Thus $\mathscr{S}_{\mathscr{A}}$ has two members of cardinality 3, nine members of cardinality 4, six members of cardinality 5 and one element of cardinality 6. Therefore, $\mathrm{d}(\mathscr{A}) = -2 + 9 - 6 + 1 = 2$.

Note that the algebras in this subcase are in bijective correspondence with sets of three lines in general position. Recall that $\mathbb{F}_q^3$ has q^2+q+1 lines, and each plane has $q + 1$ lines. It follows that the number of ordered triples of lines in general position is $(q^2 + q + 1)(q^2 + q)q^2$. Thus, the number of algebras in this subcase is $q^3(q + 1)(q^2 + q + 1)/6$. Consequently, the algebras in this subcase contribute the quantity

$$3^{-1}q^{m+3}(q + 1)(q^2 + q + 1)(q^{2m} - 1)$$

to the sum $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Subcase Ib: $\mathrm{L}_{\mathscr{A}} \supseteq \{l_1, l_2, l_3, l_4\}$*, where* l_4 *is a line not contained in any of the planes* π_1, π_2, π_3. In this case, by Lemma 7.6, we have $\mathscr{A} = \mathscr{D}$, and $\mathscr{A}$ does not contribute anything to the sum $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

It remains to consider the case when $\mathrm{L}_{\mathscr{A}}$ contains a line l_4 which is contained in one of the planes π_1, π_2, π_3. Changing the numbering if necessary, we may assume that l_4 belongs to π_1. If there is a line l_5 (different from $l_1, \ldots, l_4$) which is contained in π_2, the planes through l_4, l_1 and through l_5, l_2 intersect along a line l_6 which does not belong to any of the planes π_1, π_2, π_3. Thus we are in Subcase Ib. The same argument shows that there is no line in $\mathrm{L}_{\mathscr{A}}$ different from $l_1, \ldots, l_4$ and contained in π_3. Since $\mathscr{A}$ fixes three different lines in π_1, it acts as a scalar on π_1 by Lemma 7.6. In particular, $\mathrm{L}_{\mathscr{A}}$ contains all the lines in π_1. We will write π for π_1 and l for l_1. We see that all the remaining algebras in Case I fall in the following subcase.

Subcase Ic: $\mathrm{L}_{\mathscr{A}} = \{l\} \cup \{$*all lines in* $\pi\}$. It is easy to see that in this case $\mathrm{P}_{\mathscr{A}} = \{\pi\} \cup \{$all planes through $l\}$. We will show that $\mathrm{d}(\mathscr{A}) = 0$ by applying Lemma 7.7

to $X = X_{\mathcal{A}}$, $\mathcal{S} = \mathcal{S}_{\mathcal{A}}$. We need to verify that $x = l$, $y = \pi$ satisfy condition (2). Suppose that $X' \in \mathcal{S}_{\mathcal{A}}$ and $X' - \{l\} \notin \mathcal{S}_{\mathcal{A}}$. We claim that X' contains at most one plane through l. For suppose otherwise, that there are two planes containing l in X'. Their intersection is l. Thus a matrix fixes all elements of $X' - \{l\}$ if and only if it fixes all elements of X', that is, $X' - \{l\} \in \mathcal{S}_{\mathcal{A}}$, a contradiction. This proves that indeed X' contains at most one plane different from π. We claim that X' contains at least two lines contained in π. Otherwise, there would be at most one such line in X', so X' would be a subset of a set of the form $\{l, l', \pi, \pi'\}$ for some line l' contained in π and some plane π' containing l. Thus $\mathcal{A}$ would contain the algebra $\mathcal{A}' = \mathcal{A}_l \cap \mathcal{A}_{l'} \cap \mathcal{A}_\pi \cap \mathcal{A}_{\pi'}$. This is, however, not possible, since $\mathcal{A}'$ has an element which is not a scalar on π and all elements of $\mathcal{A}$ act as scalars on π. Indeed, if the line $l'' = \pi \cap \pi'$ is different from l' then $\mathcal{A}'$ equals $\mathcal{A}_l \cap \mathcal{A}_{l'} \cap \mathcal{A}_{l''}$ and contains the matrix which is the identity on l and l' and is 0 on l''. If $l'' = l'$ then $\mathcal{A}' = \mathcal{A}_l \cap \mathcal{A}_{l'} \cap \mathcal{A}_\pi$ contains the algebra $\mathcal{A}_l \cap \mathcal{A}_{l'} \cap \mathcal{A}_{l'_1}$ for any line l'_1 in π which is different from l'.

Thus there are two lines in X' which are contained in π. These two lines span π, so $X' - \{\pi\} \in \mathcal{S}_{\mathcal{A}}$. Also, $(X' \cup \{\pi\}) - \{l\}$ and $X' - \{l\}$ are fixed by the same set of matrices, so $(X' \cup \{\pi\}) - \{l\} \notin \mathcal{S}_{\mathcal{A}}$. This verifies condition (2) of Lemma 7.7, so $\mathrm{d}(\mathcal{A}) = 0$. Consequently, the algebras of Subcase Ic do not contribute anything to the sum $\sum_{\mathcal{A} \in \mathcal{F}} \mathrm{d}(\mathcal{A})(|\mathcal{A}|^m - q^m)$.

Note that if $\mathrm{P}_{\mathcal{A}}$ contains three planes in general position, then the three lines obtained by intersecting pairs of these planes are in general position and belong to $\mathrm{L}_{\mathcal{A}}$. Thus from now on we assume that $\mathrm{L}_{\mathcal{A}}$ does not contain three lines in general position and that $\mathrm{P}_{\mathcal{A}}$ does not contain three planes in general position. If $\mathrm{L}_{\mathcal{A}}$ contains more than two elements, then all of the lines in $\mathrm{L}_{\mathcal{A}}$ must be contained in some plane π and then, by Lemma 7.6, $\mathrm{L}_{\mathcal{A}} = \{\text{all lines in } \pi\}$. Similarly, by duality, if $\mathrm{P}_{\mathcal{A}}$ contains more than two elements, then all the planes in $\mathrm{P}_{\mathcal{A}}$ share a common line l and $\mathrm{P}_{\mathcal{A}} = \{\text{all planes which contain } l\}$. This leads to the following two cases.

Case II: There is a plane π such that $\mathrm{L}_{\mathcal{A}} = \{$*all lines in* $\pi\}$. By Lemma 7.6, every element of $\mathcal{A}$ acts as a scalar on π. In particular, $\pi \in \mathrm{P}_{\mathcal{A}}$. Note that all the planes in $\mathrm{P}_{\mathcal{A}}$ must share a common line l (if $\mathrm{P}_{\mathcal{A}} = \{\pi\}$, pick any line in π for l). In fact, suppose that there are $\pi_1, \pi_2 \in \mathrm{P}_{\mathcal{A}}$ such that the lines $\pi \cap \pi_1$ and $\pi \cap \pi_2$ are different. Then the line $\pi_1 \cap \pi_2$ belongs to $\mathrm{L}_{\mathcal{A}}$ and is not contained in π, which is not possible. Thus, $\mathrm{P}_{\mathcal{A}} \subseteq \{\text{all planes which contain } l\}$. We claim that any $X \in \mathcal{S}_{\mathcal{A}}$ contains at least two lines in π different from l. In fact, if the lines in X are contained in $\{l, l_1\}$ then consider a plane π_1 which does not contain l but contains l_1. There is a matrix A which is 0 on l and is the identity on π_1 and this matrix fixes every plane passing through l. Thus A fixes all elements of X, yet A is not a scalar on π. This means

that $A \notin \mathscr{A}$, and consequently $X \notin S_{\mathscr{A}}$, a contradiction. Now any two lines in X span π. It follows that any matrix which fixes all elements of $X - \{\pi\}$ also fixes π, that is, $X - \{\pi\} \in S_{\mathscr{A}}$. This means that the family $\mathscr{S}_{\mathscr{A}}$ of subsets of $X_{\mathscr{A}}$ satisfies the assumptions of Lemma 7.7, condition (1), with $x = \pi$. It follows that $\mathrm{d}(\mathscr{A}) = 0$ and the algebras in this case do not contribute anything to $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case III: There is a lane l such that $\mathrm{P}_{\mathscr{A}} = \{$*all planes through* $l\}$. Any algebra in this case is dual to an algebra in Case II, hence it has degree 0. Thus algebras in this case do not contribute anything to $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

It remains to analyze algebras $\mathscr{A}$ such that both $\mathrm{L}_{\mathscr{A}}$ and $\mathrm{P}_{\mathscr{A}}$ have at most two elements.

Case IV: $|\mathrm{L}_{\mathscr{A}}| = 2 = |\mathrm{P}_{\mathscr{A}}|$. We may assume that $\mathrm{L}_{\mathscr{A}} = \{l, l'\}$ and $\mathrm{P}_{\mathscr{A}} = \{\pi, \pi'\}$, where π' is spanned by l, l' and $\pi \cap \pi' = l$. It is easy to see that the family $\mathscr{S}_{\mathscr{A}}$ has three elements: $\{l, l', \pi\}$, $\{l', \pi, \pi'\}$, and $\{l, l', \pi, \pi'\}$. Thus $\mathrm{d}(\mathscr{A}) = -2 + 1 = -1$. Choosing nonzero vectors $v_1 \in l'$, $v_2 \in l$, and $v_3 \in \pi - l$ we get a basis of $\mathbb{F}_q^3$ and $A \in \mathscr{A}$ if and only if the matrix of the linear transformation given by A, expressed in the basis v_1, v_2, v_3, has the form

$$\begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}.$$

In other words, $\mathscr{A}$ is conjugate to the algebra of all the matrices of the form

$$\begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}.$$

In particular, $|\mathscr{A}| = q^4$. To count the number of algebras in Case IV, note that these algebras are in bijective correspondence with triples l, l', π, where π is a plane and l and l' are lines such that $l \subset \pi$ and $l' \not\subset \pi$. There are $q^2 + q + 1$ choices for π and for each π we have $q + 1$ choices of l and q^2 choices of l'. Thus the number of algebras in Case IV is $q^2(q+1)(q^2+q+1)$. Consequently, the algebras in this case contribute

$$-q^{m+2}(q+1)(q^2+q+1)(q^{3m}-1)$$

to $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case V: $|\mathrm{L}_{\mathscr{A}}| = 2$ *and* $|\mathrm{P}_{\mathscr{A}}| = 1$. Thus $\mathrm{L}_{\mathscr{A}} = \{l, l'\}$ and $\mathrm{P}_{\mathscr{A}} = \{\pi\}$, where π is spanned by l, l'. It is straightforward to see that $\mathscr{S}_{\mathscr{A}}$ has two elements: $\{l, l'\}$ and $\{l, l', \pi\}$. It follows that $\mathrm{d}(\mathscr{A}) = 0$ and therefore algebras in this case contribute nothing to $\sum_{\mathscr{A} \in \mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case V$^{\perp}$: $|\mathrm{L}_{\mathscr{A}}| = 1$ *and* $|\mathrm{P}_{\mathscr{A}}| = 2$. Algebras in this case are dual to algebras in Case V, so they have degree 0 and contribute nothing to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case VI: $\mathrm{L}_{\mathscr{A}} = \{l\}$ *and* $\mathrm{P}_{\mathscr{A}} = \{\pi\}$, *where* $l \not\subset \pi$. It is clear that $\mathscr{S}_{\mathscr{A}}$ has exactly one element: $\{l, \pi\}$. Thus $\mathrm{d}(\mathscr{A}) = 1$. Choosing a basis v_1 of l and v_2, v_3 of π we easily see that $\mathscr{A}$ is conjugate to the algebra of all the matrices of the form

$$\begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

In particular, $|\mathscr{A}| = q^5$. To count the number of algebras in Case VI, note that these algebras are in bijective correspondence with pairs l, π, where π is a plane and l is a line not contained in π. There are q^2+q+1 choices for π and for each π we have q^2 choices of l. Thus the number of algebras in Case VI is $q^2(q^2+q+1)$. Consequently, the algebras in this case contribute

$$q^{m+2}(q^2+q+1)(q^{4m}-1)$$

to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case VII: $\mathrm{L}_{\mathscr{A}} = \{l\}$ *and* $\mathrm{P}_{\mathscr{A}} = \{\pi\}$, *where* $l \subset \pi$. It is clear that $\mathscr{S}_{\mathscr{A}}$ has exactly one element: $\{l, \pi\}$. Thus $\mathrm{d}(\mathscr{A}) = 1$. Choosing a basis v_1 of l, v_1, v_2 of π, and a vector $v_3 \notin \pi$, we easily see that $\mathscr{A}$ is conjugate to the algebra of all the matrices of the form

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}.$$

In particular, $|\mathscr{A}| = q^6$. To count the number of algebras in Case VII, note that these algebras are in bijective correspondence with pairs l, π, where π is a plane and l is a line contained in π. There are q^2+q+1 choices for π and for each π we have $q+1$ choices of l. Thus the number of algebras in Case VII is $(q+1)(q^2+q+1)$. Consequently, the algebras in this case contribute

$$q^m(q+1)(q^2+q+1)(q^{5m}-1)$$

to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Case VIII: $\mathscr{A} = \mathscr{A}_l$ *for some line* l. The family $\mathscr{S}_{\mathscr{A}}$ has exactly one element: $\{l\}$, so $\mathrm{d}(\mathscr{A}) = -1$. It is easy to see that $\mathscr{A}$ is conjugate to the algebra of all the matrices of the form

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

In particular, $|\mathscr{A}| = q^7$. Algebras in this case are in bijection with lines, so we have q^2+q+1 such algebras. Thus the algebras in this case contribute

$$-q^m(q^2+q+1)(q^{6m}-1)$$

to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

The following case is the last to consider.

Case VIII$^\perp$: $\mathscr{A} = \mathscr{A}_\pi$ for some plane π. This case consists of algebras dual to algebras of Case VIII, so they also contribute

$$-q^m(q^2+q+1)(q^{6m}-1)$$

to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m)$.

Putting together all the contributions to $\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})\,(|\mathscr{A}|^m - q^m)$ we arrive at the formula

$$\begin{aligned}\sum_{\mathscr{A}\in\mathscr{F}} \mathrm{d}(\mathscr{A})(|\mathscr{A}|^m - q^m) &= 3^{-1}q^{m+3}(q+1)(q^2+q+1)(q^{2m}-1)\\ &\quad -q^{m+2}(q+1)(q^2+q+1)(q^{3m}-1) + q^{m+2}(q^2+q+1)(q^{4m}-1)\\ &\quad + q^m(q+1)(q^2+q+1)(q^{5m}-1) - 2q^m(q^2+q+1)(q^{6m}-1).\end{aligned}$$

After inserting this into (8) and simplifying we arrive at the following formula for $\mathrm{g}_{m,3}(q)$:

$$\begin{aligned}\mathrm{g}_{m,3}(q) &= q^{3m+4}(q^{m-1}-1)(q^{m-1}+1)(q^m-1)\\ &\quad \times (q^{3m-2}+q^{2m-2}-q^m-2q^{m-1}-q^{m-2}+q+1). \quad (10)\end{aligned}$$

7C. *Lower bound for $\mathrm{g}_{m,n}(q)$.* So far we have been unable to obtain exact formulas for $\mathrm{g}_{m,n}(q)$ for any $n \geq 4$. We have however the following lower bound.

Proposition 7.9. *Let m and n be positive integers and let q be a power of a prime number. Then*

$$\mathrm{g}_{m,n}(q) \geq q^{mn^2} - 2^{(n+6)/2}q^{n^2m-(m-1)(n-1)}. \quad (11)$$

Proof. By (4), we have the following inequality:

$$\mathrm{g}_{m,n}(q) \geq q^{mn^2} - \sum |\mathscr{A}|^m,$$

where the sum is taken over all maximal subalgebras $\mathscr{A}$ of $\mathrm{M}_n(\mathbb{F}_q)$. We use the description of maximal subalgebras given by Proposition 7.4. Let $1 \leq k < n$. The number of k-dimensional subspaces of $\mathbb{F}_q^n$ is

$$\prod_{i=0}^{k-1}(q^n - q^i)\prod_{i=0}^{k-1}(q^k - q^i)^{-1}.$$

For any such subspace V the algebra $\mathscr{A}_V$ has $q^{n^2-nk+k^2}$ elements. Let

$$S_k = \sum |\mathscr{A}_V|^m,$$

where the sum is taken over all k-dimensional subspaces V of $\mathbb{F}_q^n$. It follows that

$$S_k = q^{(n^2-nk+k^2)m} \prod_{i=0}^{k-1} (q^n - q^i) \prod_{i=0}^{k-1} (q^k - q^i)^{-1}.$$

Using the inequality $\dfrac{q^n - q^i}{q^k - q^i} \le q^{n-k} \dfrac{q}{q-1}$ we get

$$S_k \le q^{n^2m-(m-1)k(n-k)} \Big(\frac{q}{q-1}\Big)^k.$$

Note that $S_k = S_{n-k}$ (by duality). Since $\dfrac{q}{q-1} \le 2$ and $k(n-k) \ge n-1$, we have

$$\Sigma_a := \sum_{k=1}^{n-1} S_k \le 2 \sum_{k=1}^{\lfloor n/2 \rfloor} S_k \le 2^{(n+4)/2} q^{n^2m-(m-1)(n-1)}.$$

For a prime divisor s of n define T_s as the sum $\sum |\mathscr{A}|^m$, where the sum is over all subalgebras of $\mathrm{M}_n(\mathbb{F}_q)$ isomorphic to $\mathrm{M}_{n/s}(\mathbb{F}_{q^s})$. By Lemma 7.3, we have

$$\begin{aligned} T_s = q^{(n^2/s)m} \cdot s^{-1} \cdot \prod_{\substack{s \nmid i \\ 1 \le i < n}} (q^n - q^i) &\le s^{-1} \cdot q^{(n^2/s)m} \cdot q^{n(n-n/s)} \\ &\le s^{-1} \cdot q^{n^2(m+1)/2}. \end{aligned}$$

Let $\Sigma_b = \sum T_s$, where the sum is over all prime divisors s of n. It is easy to see that the sum $\sum s^{-1}$ of all reciprocals of prime divisors of n does not exceed $2^{(n+4)/2}$. Furthermore, $q^{n^2(m+1)/2} \le q^{n^2m-(m-1)(n-1)}$. It follows that

$$\Sigma_b \le 2^{(n+4)/2} q^{n^2m-(m-1)(n-1)}.$$

By Proposition 7.4 we have $\Sigma_a + \Sigma_b = \sum |\mathscr{A}|^m$, where the sum is taken over all maximal subalgebras $\mathscr{A}$ of $\mathrm{M}_n(\mathbb{F}_q)$. Thus,

$$\mathrm{g}_{m,n}(q) \ge q^{mn^2} - 2^{(n+6)/2} q^{n^2m-(m-1)(n-1)}. \qquad \square$$

As an immediate consequence of Proposition 7.9 we get the following corollary.

Corollary 7.10. *Let $m, n \ge 2$. The probability that m matrices in $\mathrm{M}_n(\mathbb{F}_q)$, chosen under the uniform distribution, generate the $\mathbb{F}_q$-algebra $\mathrm{M}_n(\mathbb{F}_q)$ tends to 1 as $q + m + n \to \infty$.*

Corollary 7.10 proves and vastly generalizes the conjectural formula [Petrenko and Sidki 2007, (17), p. 27].

8. Finite products of matrix algebras over rings of algebraic integers

Let R be the ring of integers in a number field K. In this final section we apply the techniques developed in our paper to investigate generators of R-algebras A which are products of a finite number of matrix algebras over R. Thus we have

$$A \cong \prod_{i=1}^{s} \mathrm{M}_{n_i}(R)^{m_i},$$

where $1 \leq n_1 < n_2 < \cdots < n_s$ and m_i are positive integers. As we have seen in Example 2.13, the algebra A is k-generated if and only if all the algebras $\mathrm{M}_{n_i}(R)^{m_i}$ are k-generated. Thus, we may and will focus on the case when $A \cong \mathrm{M}_n(R)^m$ for some positive integers n, m. We have the following theorem.

Theorem 8.1. *Let R be the ring of integers in a number field K. Suppose that either $n \geq 3$ or $k \geq 3$ and let $A = \mathrm{M}_n(R)^m$ for some positive integer m. Then the following conditions are equivalent.*

(i) *The R-algebra A admits k generators.*

(ii) *For every maximal ideal $\mathfrak{p}$ of R the $R/\mathfrak{p}$-algebra $\mathrm{M}_n(R/\mathfrak{p})^m$ admits k generators.*

(iii) *The density $\mathrm{den}_k(A)$ is positive.*

Furthermore, the following formulas, in which ζ_K denotes the Dedekind zeta function of K, hold for every $k \geq 2$:

(a) $\mathrm{den}_2(\mathrm{M}_2(R)^m) = 0$ *for every* m;

(b) $\mathrm{den}_k(\mathrm{M}_2(R)) = \dfrac{1}{\zeta_K(k-1)\zeta_K(k)}$;

(c) $\mathrm{den}_k(\mathrm{M}_3(R)) = \dfrac{1}{\zeta_K(2k-2)\zeta_K(k)} \displaystyle\prod_{\mathfrak{p} \in \text{m-Spec } R} \left(1 + \frac{\phi_k(\mathrm{N}(\mathfrak{p}))}{\mathrm{N}(\mathfrak{p})^{3k-2}}\right)$, *where* $\phi_k(x) = x^{2k-2} - x^k - 2x^{k-1} - x^{k-2} + x + 1$.

Proof. The implications (i) $\Rightarrow$ (ii) and (iii) $\Rightarrow$ (i) are clear. When $k \geq 3$, the implication (ii) $\Rightarrow$ (iii) is an immediate consequence of Theorem 5.2 and the fact that the K-algebra $\mathrm{M}_n(K)^m$ is 2-generated [Mazur and Petrenko 2009]. Suppose now that $k = 2$, $n \geq 3$, and (ii) holds. Consider a maximal ideal $\mathfrak{p}$ of R and let $q = \mathrm{N}(\mathfrak{p})$. By Theorem 6.3, the number $\mathrm{g}_2(\mathfrak{p}, A)$ of pairs of elements which generate $\mathrm{M}_n(R/\mathfrak{p})^m$ is given by

$$\mathrm{g}_2(\mathfrak{p}, A) = \prod_{i=0}^{m-1} \big(\mathrm{g}_{2,n}(q) - i \cdot |\mathrm{PGL}_n(\mathbb{F}_q)|\big).$$

By (ii), we have $g_2(\mathfrak{p}, A) > 0$. Note that $|\mathrm{PGL}_n(\mathbb{F}_q)| \le q^{n^2-1} \le q^{2n^2-n+1}$. Furthermore, we have $\mathrm{g}_{2,n}(q) \ge q^{2n^2} - 2^n q^{2n^2-n+1}$ by Proposition 7.9. Hence

$$\mathrm{g}_2(\mathfrak{p}, A) \ge \left(\mathrm{N}(\mathfrak{p})^{2n^2} - (2^n + m)\,\mathrm{N}(\mathfrak{p})^{2n^2-n+1}\right)^m,$$

provided $\mathrm{N}(\mathfrak{p}) > 2^n + m$. By Theorem 3.2, we have

$$\mathrm{den}_2(A) = \prod_{\mathfrak{p} \in \text{m-Spec } R} \frac{\mathrm{g}_2(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{2mn^2}}.$$

Since all the factors in the product on the right are positive and all but a finite number of them satisfy the inequality

$$\frac{\mathrm{g}_2(\mathfrak{p}, A)}{\mathrm{N}(\mathfrak{p})^{2mn^2}} \ge \left(1 - \frac{m + 2^n}{\mathrm{N}(\mathfrak{p})^{n-1}}\right)^m,$$

the product converges to a positive number. In other words, $\mathrm{den}_2(A) > 0$. This completes the proof of the implication (ii) $\Rightarrow$ (iii).

In order to establish formulas (b) and (c) note that

$$\mathrm{den}_k\big(\mathrm{M}_n(R)\big) = \prod_{\mathfrak{p} \in \text{m-Spec } R} \frac{\mathrm{g}_{k,n}(\mathrm{N}(\mathfrak{p}))}{\mathrm{N}(\mathfrak{p})^{kn^2}}$$

by Theorem 3.2. Formulas (b) and (c) follow now from (9) and (10), respectively. To justify (a) note that $\mathrm{g}_2(\mathfrak{p}, \mathrm{M}_2(R)^m) \le \mathrm{g}_{2,2}(\mathrm{N}(\mathfrak{p}))^m$ for every maximal ideal $\mathfrak{p}$. It follows that $\mathrm{den}_2(\mathrm{M}_2(R)^m) \le \mathrm{den}_2(\mathrm{M}_2(R))^m$. Since by (b) with $k = 2$ we have $\mathrm{den}_2(\mathrm{M}_2(R)) = 0$, the equality in (a) follows. □

Recall now that by Theorem 6.3, the $R/\mathfrak{p}$-algebra $\mathrm{M}_n(R/\mathfrak{p})^m$ is k-generated if and only if $m \le \mathrm{gen}_{k,n}(\mathrm{N}(\mathfrak{q}))$, where $\mathrm{gen}_{k,n}(q) = \mathrm{g}_{k,n}(q)/|\mathrm{PGL}_n(\mathbb{F}_q)|$. Using (10) we get the following theorem.

Theorem 8.2. *Let R be the ring of integers in a number field and let $\mathfrak{p}$ be a maximal ideal of R with smallest norm. Define polynomials $f_k(x)$ by $f_1(x) = 0$ and*

$$f_k(x) = \frac{x^{3k+1}(x^{k-1}-1)(x^{k-1}+1)(x^k-1)}{(x^2+x+1)(x-1)^2(x+1)} \times (x^{3k-2} + x^{2k-2} - x^k - 2x^{k-1} - x^{k-2} + x + 1) \quad (12)$$

for any $k \ge 2$. Let $k \ge 2$ and m be positive integers. Then the following conditions are equivalent:

(i) $r(\mathrm{M}_3(R)^m, R) = k$;

(ii) $f_{k-1}(\mathrm{N}(\mathfrak{p})) < m \le f_k(\mathrm{N}(\mathfrak{p}))$.

In particular, the $\mathbb{Z}$-algebra $\mathrm{M}_3(\mathbb{Z})^m$ is 2-generated if and only if $m \le 768$.

Proof. By (10), we have $\mathrm{gen}_{k,3}(q) = f_k(q)$ for any $k \geq 2$. By Theorem 8.1, the R-algebra $\mathrm{M}_3(R)^m$ is k-generated if and only if $m \leq f_k(\mathrm{N}(\mathfrak{q}))$ for every maximal ideal $\mathfrak{q}$ of R. It is easy to see that $f_k(x)$ is increasing on $[2, \infty)$. It follows that $\mathrm{M}_3(R)^m$ is k-generated if and only if $m \leq f_k(\mathrm{N}(\mathfrak{p}))$. This establishes the equivalence of (i) and (ii). The last claim follows now from the fact that $f_2(2) = 768$. □

Even though in (9) we established a formula for $\mathrm{gen}_{k,2}(q)$, getting an analog of Theorem 8.2 for products of copies of $\mathrm{M}_2(R)$ is more complicated. The difficulty is that the density $\mathrm{den}_2(\mathrm{M}_2(R)^m)$ is 0 and we have to find a way to deal with the ambiguity in Theorem 5.5 when $k = 2$. So far we can overcome this difficulty only when R has a maximal ideal of norm 2. We have the following theorem.

Theorem 8.3. *Let R be the ring of integers in a number field and let $\mathfrak{p}$ be a maximal ideal of R with smallest norm. Define polynomials $h_k(x)$ by $h_1(x) = 0$ and*

$$h_k(x) = \frac{x^{2k}(x^{k-1} - 1)(x^k - 1)}{(x - 1)(x + 1)} \tag{13}$$

for any $k \geq 2$. Let $k > 3$ and m be positive integers. Then the following conditions are equivalent:

(i) $r(\mathrm{M}_2(R)^m, R) = k$;

(ii) $h_{k-1}(\mathrm{N}(\mathfrak{p})) < m \leq h_k(\mathrm{N}(\mathfrak{p}))$.

Furthermore, there exists an integer t such that $16 \leq t \leq h_2(\mathrm{N}(\mathfrak{p}))$, $\mathrm{M}_2(R)^m$ is 2-generated if and only if $m \leq t$, and $r(\mathrm{M}_2(R)^m, R) = 3$ if and only if $t < m \leq h_3(\mathrm{N}(\mathfrak{p}))$. In particular, if $\mathrm{N}(\mathfrak{p}) = 2$, then $t = 16$, so in this case (i) and (ii) are equivalent for all $k \geq 2$.

Proof. By (9), we have $\mathrm{gen}_{k,2}(q) = h_k(q)$ for any $k \geq 2$. Suppose that $k \geq 3$. By Theorem 8.1, the R-algebra $\mathrm{M}_2(R)^m$ is k-generated if and only if $m \leq h_k(\mathrm{N}(\mathfrak{q}))$ for every maximal ideal $\mathfrak{q}$ of R. It is easy to see that $h_k(x)$ is increasing on $[2, \infty)$. It follows that when $k \geq 3$ then $\mathrm{M}_2(R)^m$ is k-generated if and only if $m \leq h_k(\mathrm{N}(\mathfrak{p}))$. This, in particular, justifies the equivalence of (i) and (ii) when $k > 3$. It also implies the existence of t having all the required properties except possibly the estimate $t \geq 16$. In order to show that $t \geq 16$, we need to establish that $\mathrm{M}_2(R)^{16}$ is 2-generated as an R-algebra. It suffices to prove that $\mathrm{M}_2(\mathbb{Z})^{16}$ admits two generators as a $\mathbb{Z}$-algebra. This will be done in Proposition 8.9. Finally, the equality $t = 16$ when $\mathrm{N}(\mathfrak{p}) = 2$ follows from the fact that $h_2(2) = 16$. □

In order to improve on Theorem 8.3 and extend it to matrix algebras of size $n \geq 3$ the following two questions need to be answered.

Question 8.4. Is it true that $t = h_2(\mathrm{N}(\mathfrak{p}))$?

Question 8.5. Given positive integers k and n, is $\mathrm{gen}_{k,n}(q)$ an increasing function of q?

It order to complete our proof of Theorem 8.3 we have to show that $\mathrm{M}_2(\mathbb{Z})^{16}$ admits two generators. For that we need several observations, which seem of independent interest.

Proposition 8.6. *Let S be a commutative ring. Two matrices $A, B \in \mathrm{M}_2(S)$ generate $\mathrm{M}_2(S)$ as an S-algebra if and only if $\det(AB - BA)$ is invertible in S.*

Proof. First we prove the result under the additional assumption that S is a field. Let $N = AB - BA$ and let T be the subalgebra generated by A and B. If T is a proper subalgebra then its dimension is at most 3. It follows that $T/J(T)$ is a semisimple algebra of dimension ≤ 3 (recall that $J(T)$ denotes the Jacobson radical of T). Thus $T/J(T)$ is abelian and therefore $N \in J(T)$. Since the Jacobson radical is nilpotent, N is nilpotent, hence $\det N = 0$.

Conversely, suppose that $\det N = 0$. Recall that any 2×2 matrix X satisfies the identity $X^2 = t_X X - d_X I$, where t_X is the trace and d_X is the determinant of X. Since the trace of N is 0, we have $N^2 = 0$. If $N = 0$ then T is commutative, and hence a proper subalgebra of $\mathrm{M}_2(S)$. If $N \neq 0$, the null-space of N is one-dimensional. Using the identity $A^2 = t_A A - d_A I$ we easily see that $AN + NA = t_A N$. It follows that the null-space of N is A-invariant. Similarly, the null-space of N is B-invariant. It follows that the null-space of N is T-invariant, hence T is a proper subalgebra of $\mathrm{M}_2(S)$. This completes our proof in the case when S is a field.

If S is any commutative ring then, by Lemma 2.6, the matrices A and B generate $\mathrm{M}_2(S)$ if and only if for any maximal ideal M of S the S/M-algebra $\mathrm{M}_2(S/M)$ is generated by the images of A and B. By the just established field case of the result, this is equivalent to the condition that $\det(AB - BA) \notin M$ for all maximal ideals M, which in turn is equivalent to claiming that $\det(AB - BA)$ is invertible in S. □

The following observation is due to H. W. Lenstra.

Lemma 8.7. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be two matrices with all entries in $\{0, 1\}$. Then A, B generate $\mathrm{M}_2(\mathbb{Z})$ if and only if their reductions modulo 2 generate $\mathrm{M}_2(\mathbb{F}_2)$.*

Proof. By Proposition 8.6, we need to prove that $\det(AB - BA)$ is odd if and only if it is ± 1. The "if" part is clear. Suppose then that

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \text{ and } B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

are such that $a_i, b_j \in \{0, 1\}$ and $\det(AB - BA)$ is odd. Note that

$$AB - BA = \begin{pmatrix} a_2b_3 - a_3b_2 & a_2(b_4 - b_1) + b_2(a_1 - a_4) \\ a_3(b_1 - b_4) + b_3(a_4 - a_1) & a_3b_2 - a_2b_3 \end{pmatrix}.$$

The diagonal entries of this matrix are in $\{0, \pm 1\}$ and the off-diagonal entries are in the set $\{0, \pm 1, \pm 2\}$. If $a_2b_3 - a_3b_2 = 0$ then the off-diagonal entries must be

odd and hence are ± 1. It follows that $\det(AB - BA) = \pm 1$. The same conclusion holds if one of the off-diagonal entries is 0. Suppose now that $a_2b_3 - a_3b_2 = \pm 1$ and the off-diagonal entries are not 0. Then one of the off-diagonal entries, say $a_3(b_1 - b_4) + b_3(a_4 - a_1)$, must be even and nonzero (the other possibility is handled in the same way). This can only happen if $a_3 = b_3 = 1$ and $b_1 - b_4 = a_4 - a_1 = \pm 1$. It follows that one of a_2, b_2 is 0 and the other is 1. Thus $\det(AB - BA) = -1 - (\mp 1)(\pm 2) = 1$. □

Lemma 8.8. *Let $A, B, A', B' \in \mathrm{M}_2(\mathbb{Z})$ be matrices with all entries in $\{0, 1\}$ such that each pair A, B and A', B' generates $\mathrm{M}_2(\mathbb{Z})$. If there is an odd prime p such that the reductions modulo p of (A, B) and (A', B') are conjugate in $\mathrm{M}_2(\mathbb{F}_p)$ then the pairs (A, B) and (A', B') are conjugate in $\mathrm{M}_2(\mathbb{Z})$.*

Proof. For a pair of 2×2 matrices X and Y define

$$\mathrm{conj}(X, Y) = \big(\mathrm{tr}(X), \det(X), \mathrm{tr}(Y), \det(Y), \mathrm{tr}(XY)\big).$$

It follows from [Mazur and Petrenko 2009, Theorem 2] that for any principal ideal domain R and any two pairs (X, Y) and (X', Y') of elements in $\mathrm{M}_2(R)$ which generate $\mathrm{M}_2(R)$ as an R-algebra we have $\mathrm{conj}(X, Y) = \mathrm{conj}(X', Y')$ if and only if $X' = CXC^{-1}$ and $Y' = CYC^{-1}$ for some invertible matrix $C \in \mathrm{M}_2(R)$ (in [Mazur and Petrenko 2009] the fifth component of conj is $\det(X + Y)$ but it is equivalent to the version above by the following identity for 2×2 matrices:

$$\mathrm{tr}(X)\,\mathrm{tr}(Y) - \mathrm{tr}(XY) + \det(X) + \det(Y) - \det(X + Y) = 0.)$$

Under the assumptions of the lemma, the traces of A, B, A', B' are in $\{0, 1, 2\}$ and the determinants of these matrices are in $\{-1, 0, 1\}$. Our assumption that $\mathrm{conj}(A, B) \equiv \mathrm{conj}(A', B') \pmod p$ implies then that $\mathrm{tr}\,A = \mathrm{tr}\,A'$, $\det A = \det A'$, $\mathrm{tr}\,B = \mathrm{tr}\,B'$, and $\det B = \det B'$. It remains to prove that $\mathrm{tr}(AB) = \mathrm{tr}(A'B')$. Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \quad A' = \begin{pmatrix} a'_1 & a'_2 \\ a'_3 & a'_4 \end{pmatrix}, \quad B' = \begin{pmatrix} b'_1 & b'_2 \\ b'_3 & b'_4 \end{pmatrix}.$$

Then $\mathrm{tr}(AB) = a_1b_1 + a_2b_3 + a_3b_2 + a_4b_4$ and $\mathrm{tr}(A'B') = a'_1b'_1 + a'_2b'_3 + a'_3b'_2 + a'_4b'_4$. Both these numbers belong to $\{0, 1, 2, 3, 4\}$. Suppose that these numbers are different. Since they are congruent modulo p, we see that $p = 3$ and one of these numbers is in $\{0, 4\}$. If $\mathrm{tr}(AB) = 4$ then all the entries a_i and b_j must be 1 so $A = B$, which is not possible. Thus we may assume that $\mathrm{tr}(AB) = 0$ and then $\mathrm{tr}(A'B') = 3$. If $\mathrm{tr}(A) = 0$ then $\mathrm{tr}(A') = 0$, so $a'_1 = a'_4 = 0$ and therefore $\mathrm{tr}(A'B') \le 2$, a contradiction. Thus $\mathrm{tr}(A) \ne 0$ and in the same way we show that $\mathrm{tr}(B) \ne 0$. If $\mathrm{tr}(A) = 2$ then $a_1 = a_4 = 1$ so $b_1 = b_4 = 0$ and $\mathrm{tr}(B) = 0$, which we have just proved impossible. This shows that $\mathrm{tr}(A) = 1$ and a similar argument yields $\mathrm{tr}(B) = 1$. Thus $\mathrm{tr}(A') = 1 = \mathrm{tr}(B')$. It follows that one of a'_1 and a'_4 is

0. We may assume that $a'_1 = 0$ (the same argument works when $a'_4 = 0$). Then $a'_2 = a'_3 = a'_4 = b'_2 = b'_3 = b'_4 = 1$ and consequently $b'_1 = 0$ and $A' = B'$, a contradiction. □

We have now the following curious proposition.

Proposition 8.9. *Let x and y be two elements of $\mathrm{M}_2(\mathbb{Z})^k$ such that every component of x and y is a matrix whose all entries are in $\{0, 1\}$. Suppose that x, y, considered as elements of $\mathrm{M}_2(\mathbb{F}_2)^k$, generate the algebra $\mathrm{M}_2(\mathbb{F}_2)^k$. Then x, y generate $\mathrm{M}_2(\mathbb{Z})^k$ as a ring. In particular, the ring $\mathrm{M}_2(\mathbb{Z})^{16}$ admits two generators.*

Proof. Let $x = (X_1, \ldots, X_k)$, $y = (Y_1, \ldots, Y_k)$. By Lemma 8.7, each pair (X_i, Y_i) generates $\mathrm{M}_2(\mathbb{Z})$. According to Lemma 2.6 and Theorem 6.1, it suffices to prove that for any prime p and any $1 \leq i < j \leq k$, the pairs (X_i, Y_i) and (X_j, Y_j) are not conjugate modulo p. For $p = 2$ this follows from our assumptions and Theorem 6.1. Consequently, the pairs (X_i, Y_i) and (X_j, Y_j) are not conjugate in $\mathrm{M}_2(\mathbb{Z})$ whenever $i \neq j$. By Lemma 8.8, the pairs (X_i, Y_i) and (X_j, Y_j) are not conjugate modulo p for any odd prime p. This proves the first part of the proposition.

Since $\mathrm{gen}_{2,2}(2) = 16$ by (9), the algebra $\mathrm{M}_2(\mathbb{F}_2)^{16}$ is two-generated. It follows from the first part of the proposition that $\mathrm{M}_2(\mathbb{Z})^{16}$ admits two generators. □

Remark 8.10. We would like to point out that one should not expect any analogs of Proposition 8.9 for matrix rings of size larger than 2. For example, consider the matrices

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Considered as matrices over the field $\mathbb{F}_3$ with three elements they have a common eigenvector $(1, -1, 1)^t$. Thus these matrices do not generate $\mathrm{M}_3(\mathbb{F}_3)$, hence they do not generate $\mathrm{M}_3(\mathbb{Z})$. Consider now these matrices as matrices over $\mathbb{F}_2$. If they do not generate $\mathrm{M}_3(\mathbb{F}_2)$, then they are contained in a maximal subalgebra of $\mathrm{M}_3(\mathbb{F}_2)$. By Proposition 7.4, the maximal subalgebra is either a field or it fixes a nontrivial proper subspace. Since $A^2 = A$, the former case is not possible. In the latter case, A and B have a common eigenvector either in their action on column vectors or in their action on row vectors. It is however a straightforward verification to see that no such common eigenvector exists. Thus A and B generate the algebra $\mathrm{M}_3(\mathbb{F}_2)$. In fact, in the same way one can see that they generate $\mathrm{M}_3(\mathbb{F}_p)$ for any prime p different from 3. With a bit more work, one can see that the subalgebra of $\mathrm{M}_3(\mathbb{Z})$ generated by A and B has index 9. Note that by (10), there are 129024 ordered pairs of 3×3 matrices with entries in $\{0, 1\}$, which considered as elements of $\mathrm{M}_3(\mathbb{F}_2)$ generate the algebra $\mathrm{M}_3(\mathbb{F}_2)$. Tsvetomira Radeva, at our request, performed computations using Java and GAP and found that among them exactly 9132 pairs

do not generate $\mathrm{M}_3(\mathbb{Z})$. The computations are based on a result of [Paz 1984] and use the LLL algorithm [Lenstra et al. 1982; Pohst 1987].

We end with the following curious observation. In Theorem 8.1 we defined a family of polynomials $\phi_k(x)$, $k \geq 2$. The polynomial $x^{3k-2} + \phi_k(x)$ is a factor of the polynomial f_k defined in Theorem 8.2. Define polynomials $\psi_k(x)$ as follows:

$$\psi_k(x) = \begin{cases} \dfrac{x^{3k-2} + \phi_k(x)}{x-1} & \text{if } k \equiv 0, 4 \pmod 6, \\ \dfrac{x^{3k-2} + \phi_k(x)}{x^2-1} & \text{if } k \equiv 1, 3 \pmod 6, \\ \dfrac{x^{3k-2} + \phi_k(x)}{x^3-1} & \text{if } k \equiv 2 \pmod 6, \\ \dfrac{x^{3k-2} + \phi_k(x)}{(x+1)(x^3-1)} & \text{if } k \equiv 5 \pmod 6. \end{cases} \tag{14}$$

Computations with Maxima show that the polynomials ϕ_k and ψ_k are irreducible for $k \leq 250$. While the polynomials ϕ_k have only six nonzero coefficients, the polynomials ψ_k have complicated structure. For example,

$$\begin{aligned} \psi_{12}(x) = {} & x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} \\ & + 2x^{21} + 2x^{20} + 2x^{19} + 2x^{18} + 2x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + 2x^{12} \\ & + x^{11} - x^{10} - 2x^9 - 2x^8 - 2x^7 - 2x^6 - 2x^5 - 2x^4 - 2x^3 - 2x^2 - 2x - 1. \end{aligned}$$

Nevertheless, it seems that all the coefficients of ψ_k are in the set $\{-2, -1, 0, 1, 2\}$. Even though we do not have at present any conceptual reason for it, we propose the following intriguing conjecture.

Conjecture 8.11. *The polynomials ϕ_k and ψ_k are irreducible.*

Acknowledgments

It is our pleasure to thank Max Alekseyev, Nigel Boston, Evgeny Gordon, Rostislav Grigorchuk, Ilya Kapovich, Martin Kassabov, Hendrik Lenstra, Pieter Moree, Tsvetomira Radeva, Peter Sarnak, Said Sidki, John Tate, and Paula Tretkoff. The first author was supported by NSF Grant DMS-0456185. The third author thanks the Max Planck Institute for Mathematics for the warm hospitality, unique research opportunities, and financial support during his visit in July–August of 2009.

References

[Arnold 2009] V. I. Arnold, "Uniform distribution of indivisible vectors in the space of integers", *Izv. Ross. Akad. Nauk Ser. Mat.* **73**:1 (2009), 21–30. In Russian; translated in *Izv. Math.* **73**:1 (2009), 21–29. MR 2010h:60023

[Cox et al. 2005] D. A. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, 2nd ed., Graduate Texts in Mathematics **185**, Springer, New York, 2005. MR 2005i:13037 Zbl 1079.13017

[Ekedahl 1991] T. Ekedahl, "An infinite version of the Chinese remainder theorem", *Comment. Math. Univ. St. Paul.* **40**:1 (1991), 53–59. MR 92h:11027 Zbl 0749.11004

[Hall 1936] P. Hall, "The Eulerian functions of a group", *Q. J. Math* **7** (1936), 134–151. Zbl 0014.10402

[Kravchenko and Petrenko 2006] R. V. Kravchenko and B. V. Petrenko, "Some formulas for the smallest number of generators for finite direct sums of matrix algebras", preprint, 2006. arXiv math/0611674

[Lenstra et al. 1982] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.* **261**:4 (1982), 515–534. MR 84a:12002 Zbl 0488.12001

[Loomis and Whitney 1949] L. H. Loomis and H. Whitney, "An inequality related to the isoperimetric inequality", *Bull. Amer. Math. Soc* **55** (1949), 961–962. MR 11,166d Zbl 0035.38302

[Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1986. MR 88h:13001 Zbl 0603.13001

[Mazur and Petrenko 2009] M. Mazur and B. V. Petrenko, "Separable algebras over infinite fields are 2-generated and finitely presented", *Arch. Math.* (*Basel*) **93**:6 (2009), 521–529. MR 2011b:16066 Zbl 1190.16026

[Narkiewicz 1990] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Springer, Berlin, 1990. MR 91h:11107 Zbl 0717.11045

[Paz 1984] A. Paz, "An application of the Cayley-Hamilton theorem to matrix polynomials in several variables", *Linear and Multilinear Algebra* **15**:2 (1984), 161–170. MR 85h:15019 Zbl 0536.15007

[Petrenko and Sidki 2007] B. V. Petrenko and S. N. Sidki, "On pairs of matrices generating matrix rings and their presentations", *J. Algebra* **310**:1 (2007), 15–40. MR 2008j:16088 Zbl 1122.16017

[Pleasants 1974] P. A. B. Pleasants, "The number of generators of the integers of a number field", *Mathematika* **21** (1974), 160–167. MR 52 #3122 Zbl 0328.12008

[Pohst 1987] M. Pohst, "A modification of the LLL reduction algorithm", *J. Symbolic Comput.* **4**:1 (1987), 123–127. MR 89c:11183 Zbl 0629.10001

[Poonen 2003] B. Poonen, "Squarefree values of multivariable polynomials", *Duke Math. J.* **118**:2 (2003), 353–373. MR 2004d:11094 Zbl 1047.11021

[Schmidt 1976] W. M. Schmidt, *Equations over finite fields: an elementary approach*, Lecture Notes in Mathematics **536**, Springer, Berlin, 1976. MR 55 #2744 Zbl 0329.12001

Communicated by Hendrik W. Lenstra
Received 2010-05-09 Revised 2011-01-08 Accepted 2011-02-06

rkchenko@gmail.com *Laboratoire de Mathématique d'Orsay, Université Paris-Sud, 91405 Orsay Cedex, France*

mazur@math.binghamton.edu *Department of Mathematical Sciences, Binghamton University, Binghamton, NY 13902-6000, United States*

bpetrenk@brockport.edu *Department of Mathematics, SUNY College at Brockport, 350 New Campus Drive, Brockport, NY 14420, United States*

Algebra & Number Theory

msp.berkeley.edu/ant

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2012 is US $175/year for the electronic version, and $275/year (+$40 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

Algebra & Number Theory

Volume 6 No. 2 2012

1937-0652(2012)6:2;1-D